Trends Organ Crim
https://doi.org/10.1007/s12117-018-9342-y

Cyber-organised crime. A case of moral panic?

Anita Lavorgna[1]

Abstract A growing number of studies show that the advent of the Internet has transformed the organisational life of crime, with many academic and non-academic articles and reports describing various types of organisational structures involved in cybercrimes as "organised crime". Other researchers are more critical in applying the organised crime label to cybercrimes. These debates are not merely speculative and scholastic but have a real practical significance, as over-estimating organised crime involvement can attract more resources (which might end up being allocated in a less efficient way), additional legal powers, and support from the general public. This study aims to further this path of inquiry by investigating whether the advancement of the cyber-organised crime narrative in the UK can be identified also in the media discourse. More specifically, this study will analyse UK press to explore to what extent "moral panic" can be identified, how primary definers use particular tactics and rhetorical constructions, and what are the dominant consequences.

Keywords Organised crime · Cybercrime · Moral panic · Risk society · Media analysis

Introduction

A growing number of studies show that the advent of the Internet has transformed the organisational life of crime, with many academic and non-academic articles and reports describing various types of organisational structures involved in cybercrimes as "organised crime" (hereafter OC) (among others, Williams 2001; Grabosky 2007; Symantec 2008; McGuire 2012; Broadhurst et al. 2014). Other researchers are more critical in applying the OC label to cybercrimes (Wall 2008, 2015; Lusthaus 2013; Lavorgna 2015, 2016; Leukfeldt et al. 2016). In their view, enough consistent and solid evidence to make analogies between online criminal networks and OC groups is

✉ Anita Lavorgna
a.lavorgna@soton.ac.uk

[1] Department of Sociology, Social Policy and Criminology, University of Southampton, Murray Building, 58 Salisbury Rd, Southampton SO17 1BJ, UK

Published online: 16 May 2018

missing, especially keeping in mind the recommendations of OC scholars on the fact that we need something "more" than an organisational structure to have OC (von Lampe 2008).

These debates on the use of the OC label are not merely speculative and scholastic but have a real practical significance. As effectively summarised by Ashby (2016), over-estimating OC involvement in a crime can attract more resources and additional legal powers, and can make it easier to attract support from politicians, the general public and the media. For a tendency towards causal reductionism in thinking about crime, the involvement of OC in complex crimes can simply provide a more appealing explanation for a crime problem; however, this can also entail that resources might end up being allocated in a less efficient way, disproportionate interference with suspects' rights might occur, and an erroneous focus on OC might deflect preventive measures and investigations from more effective activities (Ashby 2016). Recent research has already showed how European and international organisations and policy-makers have relied on pairing cybercrime with OC as a way to justify the prioritisation and expansion of intelligence and law-enforcement activities in the domain of counter-OC efforts (Lavorgna 2016), and to lift cybercrime into the national security agenda (in the UK) (Lavorgna and Sergi 2016).

This study aims to further this path of inquiry by investigating whether the advancement of the cyber-OC narrative can be identified also in the media discourse. More specifically, this study will analyse UK press to explore to what extent "moral panic" can be identified, how primary definers (or "moral entrepreneurs", in the moral panic jargon) use particular tactics and rhetorical constructions, and what are the dominant consequences.[1] The UK has been chosen as a relevant case study as it is a country where the conceptualisation of OC has been evolving and refining from both a policy and a legal point of view over the years in a process dominated by the juxtaposition between the concepts of "serious" and "organised", which led to the characterisation of OC as a national security issue (Campbell 2014; Sergi 2016). Over the last few years, as demonstrated in Lavorgna and Sergi (2016), an inverted parallelism between the characterisation of OC as a serious threat to national security and the developing characterisation of cybercrime as serious crime too – therefore organised "by default" – is triggering the securitisation of cybercrime in the country, with important consequences in terms of policing powers and approaches, and resources allocation. Media are a fundamental actor in understanding policy developments: everyday meanings of crime and threats, as well as public perceptions of control policies (and therefore the extent to which they can be "accepted" by the general public), depend on what people learn about them through the media (Ferrell and Sanders 1995). While the findings of this study cannot be generalised to other countries as media dynamics could be different, the issue investigated is likely to be relevant also beyond the UK, considering that the cyber-OC pairing has also been used in international and transnational policy making (Lavorgna 2016), and this use is in line with previously studied expansions of counter-OC efforts through policy constructions and securitisation attempts (Carrapico 2014).

A small caveat is needed. The expression "moral panic" has been criticised for its derogatory connotations: it suggests that the crime problem is somehow overblown by

[1] Please note that these questions are inspired by those suggested as relevant and necessary in moral panics research by Cohen (2011, p.237).

media exaggeration, leading to a disproportionate response. In doing so, however, it implies that public and official anxieties are without substance or justification (Waddington 1986; Thibodeaux 2014). This contribution does not intend to deny the criminogenic nature of cyberspace, nor minimise the understandable fears of the general public. Rather, it aims to call for rigour in media representations and in policy-making, as the undeniable crime and security threats present online should not be overblown for private interests, with the risk of shifting the delicate balance between privacy and security in surveillance and policing. As clarified by Cohen himself (2011), being "sceptical, debunking and deconstructive" does not imply not to be "interventionist and activist" (p. 239), there is not a contradiction between these two attitudes.

Before moving to the core of this contribution, the following sections provide a concise overview of the main empirical, legal and theoretical problems in the use of the cyber-OC rhetoric, and of the relevant moral panics literature.

Cyber-organised crimes: Problems within and beyond definitions

Empirical issues

As anticipated in the Introduction, over the last 15 years a number of academic studies and non-academic reports have described criminal networks operating in cyberspace as OC. While most academic studies focused on particularly serious forms of cybercrimes, such as those compromising data and financial security (Birk et al. 2007; Yip et al. 2013; Hutchings 2014; Formby et al. 2017), other studies and reports draw conclusion on cybercrime more in general (Choo & Smith 2008; McGuire 2012; Broadhurst et al. 2014; Europol 2017). Unfortunately, unequivocal evidence of the presence of OC online 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 OC (which has been consistently criticised over the years by OC researchers, see for instance Paoli 2002; Hobbs 2013; Sergi 2016) (see also Leukfeldt et al. 2016, 2017 for an updated and broader literature review on the use of the cyber-OC rhetoric in these studies). While the existing literature suggests that it is likely that the criminogenic features of cyberspace are attractive to OC, there is currently no sufficient evidence that OC groups are morphing into online criminal networks. Rather, evidence suggests that many OC groups operating offline still need to rely on their established system of (offline) socio-economic opportunities for their criminal activities, with cyberspace mostly used in specific situations to facilitate communications and protect anonymity (Lavorgna 2015; Leukfeldt et al. 2017). This is not to deny that some OC groups might be active also online, or that the situation might evolve and change in the near future. However, it should be emphasised that, at least for the moment being, there is no conclusive evidence to claims that OC moved online.

Many studies that used the OC rhetoric to describe criminal networks operating online expanded the notion of OC to cover a broad range of criminal phenomena occurring completely or partially in cyberspace. In doing so, they generally acknowledged that certain key characteristics of traditional OC groups need to be re-discussed when groups are operating in cyberspace. For instance, in the case of online criminal

networks, traditional continuity between group size, length of association and organisation tend to be different (McGuire 2012; Hutchings 2014). An additional problem is that many studies have been carried out by the cybercrime security industry, or are otherwise referring to data produced by it (see Lavorgna 2016). With the cybercrime security industry (rather than independent institutions) producing most of the available statistics and reports on cybercrime, however, there are fewer checks on the quality of the data gathered, which can result in misinformation and in the perpetration of false myths (Wall 2008; Steinmetz 2016).

As noted in prior research (Lusthaus 2013; Leukfeldt et al. 2016), many criminal networks operating in cyberspace cannot meet existing definitions of OC (for a more in-depth discussion, see Leukfeldt et al. 2016): they often lack a clear agenda and are loosely structured, with opportunistic rather than systematic connections. In addition, the fluidity of the networks entails that, even when a division of roles can be identified, members of the network are easily replaceable (should they be arrested). Other networks might be more structured but they lack any role of governance in cyberspace. Only a few groups have been showing some (more or less) successful attempts to take over roles played by traditional OC groups in regulating and controlling the production and distribution of products and services, first and foremost in certain online trading forums: administrators and moderators can provide a certain degree of third-party enforcement over transactions and regulate the access to the forum. However, contrary than in the physical world, they cannot prevent people to try, for example, to access the forum with another name (Lusthaus 2013). The broader academic empirical research (looking in particular at hacking, phishing and malware attacks) that examined network ties between actors involved in various forms of cybercrime is consistent with these findings, and suggests that criminal groups are well connected to one another but in a very fluid way: individuals often participate in multiple groups without a clear sense of affiliation or belonging, with their networks extending well beyond their crime associates; in addition, the circulation rate of members is very high (Holt et al. 2012; Décary-Hétu and Dupont 2012; Odabaş et al. 2017). Recent studies focusing on the origin, growth and criminal capabilities of cybercriminal networks (see, for instance, Leukfeldt et al. 2017) are confirming that the general composition of networks changes frequently.

As in the offline world, existing empirical evidence points in the direction that in cyberspace different networks with different degree of sophistications are involved. Assuming characteristics of the offenders involved as a proxy for the seriousness of the offence is always problematic (Sergi 2016). In the lack of sufficient empirical evidence, therefore, the alleged link between "cyber" and "OC" seems to serve the purpose to sensationalise statements and articles (Lusthaus 2013) by invoking imagery of mafia-type OC or, to borrow Wall's words, "cyberpunk meets The Godfather" (Wall 2008: 873). Of course, this caution in using the OC narrative does not intend to deny the seriousness of many cybercrimes, nor dispute the fact that certain OC groups have moved (or might increasingly move) into online businesses while new criminal groups with OC features are (or might increasingly be) active in cyberspace. Rather, as detailed in Lavorgna and Sergi (2016), this caution is due to the will of avoiding the deployment of the vague concept of "organised" as this is not a neutral adjective, but one that carries with it consequences in terms of resources allocation and implementation of security agendas.

Legal issues

Legal definitions of OC are very different from one another and generally depend on the characteristics of the criminal phenomena as experienced in different countries (Finckenauer 2005; Calderoni 2010; Lavorgna and Sergi 2014). In the UK, participation in a criminal organisation has been criminalised with the Serious Crime Act 2015, 45 ("Offence of participating in activities of organised crime group"): an "organised crime group" consists of three or more persons who act, or agree to act, together to further a criminal purpose. A person who takes part in any activity (constituting an offence in England and Wales punishable on conviction on indictment with imprisonment for a term of 7 years or more) knowing or reasonably suspecting it is a criminal activity of an OC group, or will help an OC group to carry on criminal activities, commits an offence. In line with Sergi's "Activity Model" (Sergi 2015) – which described how the conceptualisation of OC in England and Wales essentially overlaps with a set of crimes that are classified as posing high risks and high levels of harms for the country in various ways – the focus is on the criminal activity, identified as *serious* through the sentencing classification.

In this context, we should not forget that "cybercrime" actually spans a number of legal categories, ranging from fraud and harassment to forgery and counterfeiting; it includes both new types of crimes that would have been unthinkable without Information and Communication Technologies (e.g., malware attacks), and old crimes "revived" by new criminogenic opportunities (e.g., cyber-stalking). Many of these crimes do not meet the sentencing threshold of a minimum sentence requirement that must be met for a case to be labelled as OC (see also Leukfeldt et al. 2016).

Theoretical issues

The concept of OC has a long-standing history, and over the years many conceptualisations and interpretations have been used to explain this criminal phenomenon. To keep it brief and not exceed the scope of this study, this section summarises the discussion on the theoretical "paradoxes" of the conceptualisation of cyber-OC that the reader can find more in detail in (to be added after peer review 2016). For a long time, OC has been conceptualised as an ethnic-based criminal endeavour (such as in the case of the Italian and the Russian Mafias). This early conceptualisation is reflected in the so-called Alien Conspiracy Theory, which was developed in the multi-ethnic setting of the United States in the mid-1900s, resting on the premise that OC is native from a "foreign" culture forcing its way into a relatively unprotected society (Smith Jr 2016). This theory, largely criticised, still survives as a conceptual framework to explain the (alleged) ethnic homogeneity of certain OC groups (Antonopoulos 2009; Smith Jr 2016). Being dissatisfied with this explanation of OC, some scholars started focusing on the economic origin of OC and the dynamics of criminal marketplaces. The Enterprise Model proposed by D.C. Smith Jr. in the mid-1970s, for instance, has been one of the first contributions that tried to demystify the common understanding of OC as a secret criminal society and stated clearly how OC is based on the same assumptions of legitimate business organisations – that is, maintaining and extending their share of the market (Smith Jr 1975). In the following decades, the vision of a *Homo Economicus Criminalis* (McCarthy 2011: 22) as a metaphor to enlighten the understanding of OC has become increasingly common.

Author (details to be added after peer review) (2016) showed that this latter interpretation is prevalent in documents on cyber-OC produced by the major security and intelligence agencies and institutions at the European and international levels. It is "expected" for OC to adapt to cyberspace (as if it was a business company), in order to stay competitive and survive in the (criminal) market. The pairing among "cyber" and "organised", however, overlooks major differences between criminal and conventional criminal activities, with the risk of neglecting specific skills and motives – that are expected to depend on the nature of the specific crime in question – when investigating a specific cybercrime. In addition, if we maintain the crime-enterprise narrative, we should expect criminals to be rationally geared towards efficiency; this efficiency is to be reached by relying on a minimum degree of organisation as needless complexity is ineffective for offenders (Felson and Boba 2010; Ashby 2016). The ironic consequence would be that OC is bound to become marginalised in cyberspace, as less efficient.

Cyberspace and moral panic

There is a background anxiety on cyberspace that has been increasingly pointed as a causal factor for many dramatic crimes and events, if only because in our hyper-connected world it is becoming more and more hard to imagine a crime that does not involve an online component. Consequently, the term cybercrime – a fictional construction used to emphasise the criminogenic elements of cyberspace – has become a symbol of insecurities and risk: a real "mythology about cyberspace and cybercrime" (Wall 2008: 862), reinforcing public concerns, emerged from the increased awareness of technical scientific possibilities, with a number of cyber-related urban myths distorting our understanding of present and emerging issues. Myths, however, are dangerous. As stressed by Wall (2008), not only technological changes are very rapid and they can quickly mutate the reality of the problem, but they can also become self-perpetuating, hindering our understanding of change as it happens.

The notion of *moral panic*, a concept that roots in the radical interactionists' critique of social control (Garland 2008), was first introduced by Cohen (1972), and soon became part of the jargon of sociologists and criminologists to describe strategies and rhetoric in the media coverage of crime and deviancy. Moral panics are identifiable objects onto which social anxieties can be projected (Hier 2003). As clarified by Cohen himself (2011), new moral panics continuously emerge and adapt in our postmodern world. While moral panics can be driven bottom-up by local anxieties, they can be also deliberately elite-engineered for commercial or political gain (Hall et al. 1978; Goode and Ben-Yehuda 1994; McRobbie and Thornton 1995; Garland 2008; Hier 2008). Moral panics are in fact generally created by so-called "*moral entrepreneurs*" (Becker 1963), with the aim to propagate their viewpoint, creating or enforcing norms in line with their understanding of what is best. In order to do so, moral entrepreneurs define a social problem as "serious enough" to warrant attention and a desired social policy. Moral entrepreneurs can make a career out of spreading public alarm on a certain crime issue, advocating certain necessary reforms and measures to deal with it, and putting forward themselves as the right persons to deal with such an issue (Philips 2003). Moral entrepreneurs can be rule creators – trying to bring forward "moral" crusades to combat some type of social evil – or rule enforcers – i.e., experts or professionals who legitimise a moral crusade because it is their job (e.g., law enforcement officers).

Hidden and not-so-hidden political agendas are generally associated with moral panic (Cohen 2011), to the point that they have has been described as "a rhetorical move in cultural politics" (Garland 2008:9). In fact, while at the beginning moral panic served mainly to mark the connection between media and social control, it was soon recognised that media and political strategies are often strictly connected (McRobbie and Thornton 1995), as moral panics can serve to attract public attention on a specific issue and therefore force it onto the political agenda (Garland 2008). As emphasised by Garland (2008), moral panics matter because they "make things happen" (p.15). In particular, they can allow to build infrastructures of regulation and control that can have lasting effects. The vague concept of OC, as shown in previous research on the USA and the UK, has already been used by media and policy makers as a vehicle for passing new legislation to increase crime control powers and to promote specific types of crime control approaches (in terms of drug policies, for example) whose effectiveness is still debatable (see the historical analysis of Woodiwiss and Hobbs 2008).

Every moral panic has its own folk devil – i.e., a group of people or an episode onto whom or which public anxieties are projected (Cohen 1972; Hier 2008) – cyber-OC, in the hypothesis of this study. Goode and Ben-Yehuda (1994) identified some common features of moral panics: concern (a reported conduct or event create anxiety); hostility (the offenders are portrayed as folk devils); consensus (of the negative social reaction); disproportionality (the extent of/threat posed by the conduct is exaggerated); volatility (of the media's attention on the issue). Garland (2008) added to this list the moral dimension of the social reaction, and the idea that the deviant conduct is somehow symptomatic of a bigger problem.

Over the years, moral panic as an approach has been criticised – also harshly criticised as an academic cliché based on the idea of a consensus society (Thompston and Williams, 2013) – for its (apparent) inability to adapt to different moral viewpoints and, as such, to be of practical use in our modern and pluralistic societies (Waddington 1986; McRobbie and Thornton 1995; Thompston and Williams, 2013; Horsley 2017). In a way, the moral panic thesis has been accused to be trapped in an anachronistic critique of a "moral order" no longer existing (Horsley 2017), becoming a description for any widespread concern that is embraced by the media in a spiral of hyperbole to secure a significant audience (Jewkes 2015). Despite these criticisms, however, moral panic can still be praised as "a means of conceptualising the lines of power in society" (Jewkes 2015: 104), confirming its continuing practical and heuristical value once we widen and tighten the focus of analysis, redefining moral panics' traditional parameters (Hier 2016).

Methodology

Data gathering

This study focuses on newspaper articles published in the UK between January 1, 2010 and December 31, 2016. The dates were chosen to capture articles over a period sufficient to take into consideration possible changes in the representation of the issue. Particularly, the analysis starts 3 years before the creation of the National Crime Agency (NCA) (in 2013) and ends 3 years later, as it was expected that the new

Agency might have increased media attention to the issue (in line with the increase of documents from policy makers on cyber-OC in 2013, see Lavorgna and Sergi 2016).

Articles were extracted from the database *Lexis Nexis Academic*, which is useful for press analyses as it provides full text access and allows searches by period, language, and type of source. Trying to keep the search as comprehensive as possible, the following syntaxes was chosen for the keyword searches: "cyber [same sentence] organised" (anywhere in the text, 473 results). The search was entered based on the following criteria: timeframe (01/01/2010–31/12/2016); type of source (News, UK national newspapers). Duplicate options were automatically excluded "if high similarity" was to be found. Documents with less than 500 words and documents with high similarity (which suggests duplication of results) were automatically excluded (for a total of 351 results). The selected articles were then manually sorted out to exclude those non-relevant for the scope of this study. A total of 213 press items were identified as relevant for the analysis.

As already underlined by Weaver and Bimber (2008) among others, news aggregation databases such as Lexis Nexis have important limitations, which might hinder the accuracy of a study looking at the news distribution of a particular subject. In fact, they do not necessarily constitute archives of the whole content of news appearing, because of the exclusion of major wire services and major newspapers. Nonetheless, *Lexis Nexis Academic* was chosen as a proper news aggregator for this exploratory analysis because of its powerful search capability and extensive coverage (Center for Research Libraries 2013).

Data analysis

The software NVivo was used for the computer-assisted content analysis. Relevant passages in the text were categorised according to five ("year", "primary definers", "OC juxtaposition", "OC understanding", and "other") main codes (or "nodes", in the language of NVivo) and a total of 25 sub-codes, as summarised in Appendix Table 1. The use of NVivo allowed to obtain descriptive statistics of the different codes and sub-codes, offering comprehension of the recurrence of certain themes and topics in the press news analysed. Particularly, the number of references (i.e., the number of text fragments within our sampled articles that have been coded with any node) provided insights into the recurrence of a certain theme in the press (the number of references is reported in parenthesis in the following text). Moreover, the codes and sub-codes were used to assist the qualitative part of the analysis, whose results are presented in the following section.

Results and discussion

Year

Contrarily to what was expected, there was not a peak of news in 2013 (28 references), when the NCA – the UK's lead national agency against serious and organised crime – came into being with the Crime and Courts Act. Rather, the peak on news on cyber-OC was reached the following year (43 references). Overall, it can be noticed that

references to cyber-OC in the news augmented since 2010, but no clear trend can be identified (see Appendix Table 1).

Primary definers

This code identifies the actors whose voice framed a cybercrime problem as OC. The most active primary definers when it comes to cyber-OC are high-level policy makers (49 references) – e.g. ministries and members of Parliament – and cyber-security companies/consultants (42 references). Law enforcement representatives (21 references) and independent (non-academic) researchers and writers/bloggers on cybersecurity issues (11 references) follow. In this latter case, it should be noted that the discussion was generally not on a specific empirical case but on a recent book published by these researchers/authors and somehow dealing with cybercrime. Voice is given also to private companies (5 references) and trade associations (2 references) that might be affected by cybercrimes. Comments on cyber-OC by the directors of Europol and of the European Cybercrime Centre (EC3) are also reported (5 references), which is not surprising considering the role of these centres in framing the cyber-OC narrative (Lavorgna 2016). Finally, think-tanks (2 references) and one academic researcher (a cyber-psychologist, but presented in her role of consultant for the tv show *CSI: cyber*) (2 references) described cybercrime as OC. Interestingly, the same cyber-psychologist was criticised by Steinmetz (2016) for inflating the scope of cybercrime-related problems in the show (for instance suggesting connections with "violent organised crime and seemingly all-powerful hackers", Steinmetz 2016, p. 204).

As in the case of moral entrepreneurs in moral panics, the primary definers identified have hidden and not-so-hidden agendas and use media hyperboles to rally the support of society behind their specific scope. To borrow the words of van Duyne (2011), this can be interpreted as "fear management" creating gullibility, and is in line with findings on moral panic in the social construction of hackers (see Steinmetz 2016). However, while in traditional moral panics rule creators and rule enforcers socially construct "crime" by defining (perceived) deviant acts as (moral) threats, in the case of cyber-OC criminal activities are already recognised as security threats. Rather than trying to mobilise the general public against some types of social evil, these primary definers tend to mobilise respectively other policy makers, the legislator, and/or potential customers (in the case of cybersecurity companies). The general public seems to be addressed only to make it "accept" the new structures of social control as effective means to counter cyber-OC in all its seriousness (Hall et al. 1978).

As mentioned above, voices of cybersecurity consultants and companies are recurring in the news; in 5 cases this resulted in explicit *advertisements* for specific companies. Consider for instance:

> "At [company] for example, we know that our clients are going to get attacked, so it's about preparing traps, laying tracks and waiting for would-be attackers to fall into the snare. […] Instead of a software-only approach, the solution is to provide software and people. […] That's where we're going, and where I think I can see things going industry-wide" (*The Telegraph*, 5 October 2016).

As noted in Simon and Feeley (2013), media seem to have lost the front line as primary definers, leaving the main voice in framing reality to others; in their search for the (newsworthy) production of information, they are becoming reactive agents, increasingly accepting the narrative of those "governing through crime" (Simon 2007).

OC juxtaposition

Because cybercrimes are relatively new offences, and are often not well understood by the general public, public's perception of cybercrime can be heavily influenced by how the issue of cybercrime is framed, and by whether this framing attempts to integrate cybercrime into extant, and better known, threat frames. A tactic used to increase public support towards strategies to tackle a complicated crime problem (e.g., cybercrime) is to link it with one that is more familiar for the public to understand (Hill and Marion 2016) – OC, in our case. After all, as noticed already four decades ago, when two or more threats converge moral panics can become particularly powerful, as the threat potential for society is amplified (Hall et al. 1978). In an overwhelming majority of cases analysed (134 references), the association between OC and "cyber" occurred only in general terms: in line with what has been observed in policy-making documents (Lavorgna 2016; Lavorgna and Sergi 2016), the adjective "organised" was used *en passant* as an attribute of a criminal activity perceived as "serious" or of a criminal group perceived as sufficiently sophisticated. The media, unsurprisingly, are interested in visual symbols, and OC traditionally provides one (Levi 2009). Consider for instance the following snippets:

> "Cyber security experts have warned of a constant threat of organised cyber criminals on the financial sector" (*Financial Times*, 31 August 2014);
>
> "Cyber-security experts confirm that the virus is run by organised criminal gangs who make millions from it" (*Daily Mail*, 28 January 2015);
>
> "This is organised crime. Whilst the individual cases themselves may involve relatively limited amounts of money, this is being organised by well-equipped, often off-shore organised crime groups that are facilitating this activity" (*The Independent*, 30 November 2016).

In many other cases, a certain cybercrime is juxtaposed to OC via the association with an anti-OC agency (36 references), without further specification neither of the type of cybercrime at issue, nor its "seriousness". Most of these cases refer to the role of the NCA in tackling serious (and) organised crime. Consider for instance the following fragment:

> "In the fight against online fraudsters the biggest change on the horizon is the creation of the National Crime Agency. It will merge specialist cyber law enforcement expertise at Scotland Yard with the Serious Organised Crime

Agency's international criminal intelligence capabilities" (*The Telegraph*, 24 November 2011).

Sometimes, the juxtaposition between cyber and OC is explicitly related to the demand for new powers and/or resources to tackle cyber-related crime problems (13 references). These references concentrate around the so-called "Snooper's Charter" – i.e., two bills of the UK Parliament aiming (1) to require communication service providers to maintain data on their user's online activities, including browsing activities (the Draft Communications Data Bill, produced for consultation in 2012 but never introduced to Parliament after the criticisms it received) and (2) to expand the powers of the UK intelligence community by allowing, among other things, bulk interception of communications and their data and by requiring communication service providers to retain the Internet connections records of their users (the Investigatory Powers Act 2016 which, despite the concerns regarding the use of mass surveillance and intrusive powers, came into force). Consider, for instance:

"[The then] Home Secretary Theresa May stepped up her call for more powers to track email and internet use. She claimed people will "die" without more powers to track terrorists, paedophiles and criminals online. [She added:] "The people who say they're against this bill need to look victims of serious crime, terrorism and child sex offences in the eye and tell them why they're not prepared to give the police the powers they need to protect the public"" (*Daily Mail*, 4 December 2012).

"[…] Mrs May reiterated her support for the so-called Snoopers' Charter that would give law enforcement agencies the power to access and store details of an individual's online activity to see which websites they have been accessing. "It is a matter of national security"" (*Sunday Express*, 23 November 2014).

"The [then] Minister for the Cabinet Office Ben Gummer [explains] why the Government is today launching its five-years National Cyber Security Strategy. It is a bold vision to tackle the many threats our country faces in cyberspace and sets out our plan to make the UK confident, capable and resilient in a fast-moving digital world. The strategy will only be as good as the resources we deploy to make it happen" (*The Telegraph*, 31 October 2016).

If the "year" code was not very enlightening to understand the historical temporality of the cyber-OC narrative, the "OC juxtaposition" code can shed some light on why such a narrative has been used in specific moments in time. In line with the findings of Hill and Marion (2016) in their study of the (American) presidential rhetoric on cybercrime, it is not uncommon for high-level policy makers to attempt to put pressure on the legislator with their public speeches as a way to persuade them to take actions such as passing new legislation, or providing additional funding. Furthermore, the juxtaposition opens the way to treat cybercrimes as a national security issue. Without denying how certain cybercrimes could significantly affect national security (and so the rhetoric used does contain an element of truth – suffice it to think about the scale of the

recent WannaCry ransomware attack in May 2017, which also affected the Britain's National Health Service), we should bear in mind that many cybercrimes are merely instances of traditional crimes on the Internet. As already identified by Cohen in later revisions of his initial work, if it is plausible that a certain event will become a major threat (in our case, that an increasing number of cybercrimes and criminal actors online will achieve the "national security threat" level), the control culture we are part of mobilises in advance, with potential events being anticipated to justify increased repression (in our case, more pervasive security measures) (Cohen 1980).

OC understanding

In the majority of newspaper articles, it was not possible to identify a specific (even if implicit) theoretical understanding of OC. After all, press news are not expected to dwell on theorisations and explanations of crime phenomena. However, it is interesting to note that, while international policy-making documents and reports overwhelmingly suggested an understating of OC as an economic phenomenon in line with Smith's Crime Enterprise approach (Lavorgna 2016), only a limited number of press news were explicitly depicting cyber-OC as a profit driven activity (19 references, and in 2 additional references there was a tentative explanation of the rise of cybercrime in certain countries as a consequence of the economic crisis):

> "[…] it is not just that these organisations are getting large and sophisticated, it's that they run themselves like modern profit-oriented businesses, with weekly targets, commission-based remuneration and strategy meetings. And just like modern corporations, they're competitively minded and fearful of challenges to their marketshare" (*Financial Times*, 6 November 2015).

Rather, a significant higher number of press news relied on an Alien Conspiracy approach in associating cybercrime with OC (36 references), describing the criminal actors involved as based elsewhere and "launching cyber-attacks against Britain" (*Daily Mail*, 3 December 2012). "Organised cyber criminals, who are mainly based in Russia but also emerging in Africa" (*Daily Mail*, 2 November 2016) are reported as particularly dangerous, while "gangs in Eastern Europe and elsewhere routinely raid the bank accounts and personal data of British internet users, with little apparent fear of punishment" (*The Telegraph*, 24 November 2011). Conversely, only one reference referred to "British" manifestations of OC as active in cyberspace (*The Sunday Telegraph*, 3 October 2010). A very common OC-related moral panic argument can be fund here: there are forces outside "our" mainstream culture that threaten "our" otherwise sound and safe society. There is a form of globalisation that inspires fear, suggesting that alien forces create problems to righteous citizens and promoting a form of othering which is in line with certain right-thinking political and media players (Woodiwiss and Hobbs 2008). Economic forms of cybercrime in particular, as other problems connected to late capitalism, are considered to originate from another malevolent place rather than in "our" own backyard (Hall et al. 1978; Woodiwiss and Hobbs 2008).

In describing cyber-OC, explicit parallelisms with evocative mafia-type manifestations of OC were found in 7 press news. Consider for instance the following statement of Europol's Director Rob Wainwright, as reported in the press:

> "Top computer graduates are being lured into Mafia cybercrime booming and with it a whole service industry" (*Independent*, 8 December 2015).

Here, it is particularly evident the use of the rhetoric of (mafia-type) OC to sensationalise the reporting of cybercrime.

Moral panic

If we consider the characteristic of moral panics as identified by Goode and Yeheuda (1994, see above), the representation of cyber-OC in the UK press seems to cover all the required attributes. However, if we focus on the need of a "moral" dimension of the social reaction (see Garland 2008, above), this can be found only in 21 references. Consider, for instance:

> "William Hague, the Foreign Secretary, said […] Britain was under attack over the internet from states and criminals determined to steal secrets and that he wanted to establish new "norms of behaviour in cyberspace"" (*The Telegraph*, 5 September 2011).

> "No longer the stuff of spy thrillers and action movies, cyber attacks are a reality and they are happening now […] Attacks can cause economic damage, erode public trust in online services and by enabling fraud do real harm to individuals, their property and their privacy" (*The Telegraph*, 31 October 2016)

> "Young people are being drawn into increasingly serious cyber crime after beginning with acts of petty theft inside online fantasy games such as World of Warcraft, Britain's most senior cyber detective has said. Key figures within organised gangs involved in large-scale fraud are known to have moved from a culture of "laddish" online behaviour that is not punished into something "extremely corrosive", the director of the National Cyber Crime Unit of the National Crime Agency has told *The Independent*. […] "There are some sorts of criminality that youngsters don't think of as serious. Stealing gold off each other in online games, cheating if you like […] It does start with play: stealing swords and gold in online games. The second conclusion is the lack of awareness of the social cost of something that is criminal," he said" (*The Independent*, 7 February 2015).

The existence of a past, offline "golden age" with fewer and less serious criminal threats is implied – in line with the past golden age where social stability and strong moral discipline acted as a deterrent to delinquency and disorder that we can find in traditional moral panic analyses (McRobbie and Thornton 1995). In this context, the "solutions" proposed by primary definers (*in primis*, new legislation and a different resource allocation) are perceived by the general public as relatively cost-free (Levi 2009).

Further discussion and conclusions

This study, departing from a critique of the juxtaposition of the terms "cyber" and "organised" in the UK press when merely used to emphasise the seriousness of many cybercrimes, has shown how news media – which are fundamental actors in presenting and promoting policy developments – have succumbed to the temptation to use "organised" as an intensifier to describe cybercrimes. This has been done in a way that is not substantiated by research and that leaves unchallenged the framing of a crime control discourse by primary definers with vested interests on the issue. This arbitrary migration of OC into the conceptualisation of cybercrime, however, is not without practical consequences (at least in terms of resource allocation and action prioritisation), especially in a country where the fight against cybercrime has already been subsumed within the more general fight against OC at the national security level (Lavorgna and Sergi 2016). Evoking threat images of OC in order to make the case for effective crime repression is not something new: institutions from different countries have used this mechanism over the years to make the case for effective crime repression (van Duyne and Vander Beken, 2009), often pairing OC with other attributes (such as "transnational", see van Duyne, 2011; van Duyne and Nelemans, 2012) or other security threats (such as "terrorism", see Ruggiero 2017 for a critique). These hybrid notions, often contested in critical academic literature, rarely proved a heuristical or practical value, but rather caused assumptions and confusion in defining, describing, and addressing various and heterogeneous phenomena. In the case of cybercrime, without denying the seriousness of many times of cybercrime*s* and the possibility to have certain OC groups involved, it is important to maintain a critical attitude in assessing emerging narratives as they are still developing.

This study has also shown that moral panic demonstrates its continuing value as a critical tool, and as an organising framework to better understand the development and the expansion of the cyber-OC rhetoric (or its tentative superimposition, see Lavorgna 2016). As summarised by Hier (2016), notwithstanding the diversity of moral panic studies, they all share the aim to show how people in positions of power can construct claims that frame deviance in a distorted manner. In addition, the value of the moral panic approach holds true in presenting the role of media in shaping events and attitudes. The role of news in strategically advancing campaigns towards particular scopes has become so powerful that in recent years it has been claimed that moral panic has become institutionalised, thus becoming an integral part of the infrastructure of contemporary society (Simon and Feeley 2013). However, some differences are evident and do not allow an uncritical and plain reception of the moral panic framework as regards risks and anxieties in cyberspace, or to explain the advancement of the cyber-OC narrative in the UK. First, as explained above, the element of "morality" is generally missing. Second, the concept of moral panics, as already suggested by Ungar (2001), might be too limited to capture the threats and conditions associated with our complex society: while moral panics depend on "a relatively small pool of mostly familiar threats", our society "is constituted by a vast number of relatively unfamiliar threats, with new threats always lurking in the background" (Ungar 2001: 276). Consequently, it would be very useful to integrate the moral panic framework with Beck's risk society perspective: there are in fact important overlaps between the moral panic

and the risk society literatures as they both discuss of the general politics and sociology of risks (Garland 2008). Integrating these approaches can allow us to overcome Ungar's criticism. As suggested by Hier (2003, 2008), the anxieties associated with late modern risks generate a great number of panics, as a convergence is formed between the anxieties endemic to the risk society and those contained at the level of community. In a time of pervasive insecurity, a time in which "governing through crime" has become a quintessential characteristic of a culture of control spreading through most aspects of social life, moral panic approach has not lost its usefulness because of the permanent crisis of inequality and insecurity we live in, and the increasingly complex and contradictory nature of powers in society (Hier 2008; McRobbie and Thornton 1995; Horsley 2017). Moral panics have rather become "part of the manufactured background, a feature […] that never goes away, and that must be constantly guarded against" (Simon and Feeley 2013: 51).

As regards more specifically the scope of this study, integration with a risk society approach can help us to better understand the broader implications of the framing of cybercrime as OC (and, through this juxtaposition, as a national security issue), to explain why securitisation and the politics of fear are used for cybercrimes, and why the public is likely to be receptive to this kind of fear (Hill and Marion 2016; Steinmetz 2016). According to Beck (1992), in fact, advancing technology can generate new threats; people feel insecure because of the increased perception of risk, but cannot see the "invisible" – even if omnipresent – digital threat. As already observed in Hill and Marion (2016), the coupling of national security with general cybercrime issues represents an attempt to define these issues in a way that is helpful to the policy-makers' (and the cyber-security industries') agendas. Anxiety is a powerful social force and, because of the risk involved with cybercrimes, people can become more easily compelled to support these agendas, including solutions that tend to shift the discussion away from basic principles such as privacy and the meaningful exercise of the freedom of expression (Wall 2005/2015; Steinmetz 2016).

It is a known fact that challenging the spread of dominant narratives and myths surrounding crime and justice is difficult, even if a long-standing concern of criminology (Steinmetz 2016). Recognising the tactics and rhetorical constructions of the primary definers, as well as the consequences of using a certain narrative in framing cybercrime news, does not want to deny the seriousness of the cyber-related risk, nor the fact that the existing equilibria in resources allocation and power distribution might have to be re-discussed: after all, cybercrime risks are extremely real and here to stay, they cannot be dismissed as moral panics or as immodest threats. Nonetheless, the fact that the ambiguity of the language entails lowering (even more) the thresholds in the already contested OC definition, and possibly alter the delicate balances in the privacy-security dilemma, requires critical attention and rigour in the terminology employed before crystallising "cyber OC" as a new empty signifier (but with important consequences in terms of resource allocation and action prioritisation). If on the one hand meaningful policies can be pushed in other ways (for instance, understanding better the harms posed by different cybercrimes, or evaluating different types of policing when confronted with new sets of challenges in cyberspace), further research on different criminal networks active online and on diverse types of cybercrimes is needed, at least to test and possibly generalise the scarce empirical findings currently available.

Appendix

Table 1 Coding framework

Codes	Sub-codes	No of references
year	2010	20
	2011	34
	2012	23
	2013	28
	2014	43
	2015	32
	2016	33
primary definers	high policy level	49
	cybersecurity company or consultant	42
	law enforcement	21
	Independent researcher (author, blogger)	11
	private company	5
	Europol, EC3	5
	think-tank	2
	trade association	2
	academic (author)	2
OC juxtaposition	general	134
	via relevant agencies	72
	new powers/resources needed	13
OC understanding	as alien conspiracy	36
	as profit-driven enterprise	19
	as response to opportunities due to economic crisis	2
	mafia parallelism	7
	"British" OC	1
other	"moral" panic	21
	extreme advert	5

References

Antonopoulos GA (2009) Are the others coming? Evidence on alien conspiracy from three illegal markets in Greece. Crime Law Soc Chang 52(5):475–493

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

Beck U (1992) Risk society: towards a new modernity. Sage, London

Becker HS (1963) Outsiders: studies in the sociology of deviance. Free Press, New York

Birk D, Gajek S, Grobert F and Sadeghi AR (2007) Phishing phishers. Observing and tracing organized cybercrime. Second International Conference on Internet Monitoring and Protection (ICIMP)
Broadhurst R, Grabosky P, Alazab M, Chon S (2014) Organization and cybercrime: an analysis of the nature of groups engaged in cybercrime. Int J Cyber Criminol 8(1):1–20
Calderoni F (2010) Organized crime legislation in the European Union: harmonization and approximation of criminal law, national legislations and the EU framework decision on the fight against organized crime. Springer, Heidelberg
Campbell L (2014) Organized crime and national security: a dubious connection? New Crim Law Rev 17(2):220–251
Carrapico H (2014) Analysing the European Union's responses to organized crime through different securitization lenses. Eur Secur 23(4):601–661
Choo KKR, Smith RG (2008) Criminal exploitation of online systems by organised crime groups. Asian J Criminol 3(1):37–59
Cohen S (1972) Folk devils and moral panics: the creation of the mods and the rockers. MacGibbon and Kee, London
Cohen S (1980) *Folk Devils and Moral Panics*, 2nd edn. Oxford: Martin Robertson
Cohen S (2011) Whose side were we on? The undeclared politics of moral panic theory. Crime Media Cult 7(3):237–243
Décary-Hétu D, Dupont B (2012) The social network of hackers. Global Crime 13(3):160–175
Europol (2017) Internet facilitated organized crime (IOCTA). European Police Office, The Hague
Felson MK, Boba R (2010) Crime and everyday life. Sage, Thousand Oaks
Ferrell J, Sanders C (1995) Cultural Criminology. Boston: Northeastern University Press
Finckenauer J (2005) Problems of definition: what is organized crime? Trends Organ Crime 8:63–83
Formby D, Durbha S and Beyah R (2017) Out of control: ransomware for industrial control systems. Available at: http://www.cap.gatech.edu/plcransomware.pdf
Garland D (2008) On the concept of moral panic. Crime Media Cult 4(1):9–30
Goode E, Ben-Yehuda N (1994) Moral panics: the social construction of deviance. Blackwell, Cambridge
Grabosky PN (2007) The internet, technology, and organised crime. Asian J Criminol 2(2):145–161
Hall S, Critcher C, Jefferson T, Clarke J, Roberts B (1978) Policing the crisis: mugging, the state, and law and order. Macmillan, London
Hier S (2003) Risk and panic in late modernity: implications of the converging sites of social anxiety. Br J Sociol 54(1):3–20
Hier S (2008) Thinking beyond moral panic: risk, responsibility, and the politics of moralization. Theor Criminol 12(2):171–188
Hier S (2016) Moral panic, moral regulation, and the civilizing process. Br J Sociol 67(3):414–434
Hill JB and Marion NE (2016) Presidential rhetoric on cybercrime: links to terrorism? Crim Justice Stud 29(2): 163–177
Hobbs D (2013) Lush life: constructing organised crime in the UK. Oxford University Press, Oxford
Holt TJ, Strumsky D, Smirnova O, Kilger M (2012) Examining the social networks of malware writers and hackers. Int J Cyber Criminol 6(1):891–903
Horsley M (2017) Forget "moral panics". J Theor Philos Criminol 9(2):84–98
Hutchings A (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime Law Soc Chang 62(1):1–20
Jewkes Y (2015) Media and crime. Sage, London
Lavorgna A (2015) Organised crime goes online: realities and challenges. J Money Laundering 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, von Lampe K (eds) Narratives on organised crime in Europe. Criminals, corrupters and policy. Wolf legal publishers, Nijmegen, pp 193–221
Lavorgna A, Sergi A (2014) Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis an in the use of internet technologies. Int J Law Crime Justice 42(1):16–32
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
Leukfeldt R, Lavorgna A and Kleemans ER (2016) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of Criminal Policy and Research* (online first, https://doi.org/10.1007/s10610-016-9332-z)
Leukfeldt R, Kleemans ER, Stol WP (2017) A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime Law Soc Chang 67(1):21–37
Levi M (2009) Suite revenge? The shaping of folk devils and moral panics about white –collar crimes. Br J Criminol 49:48–67
Lusthaus J (2013) How organised is organised cybercrime? Global Crime 14(1):52–60

McCarthy DMP (2011) An economic history of organized crime. A national and transnational approach. Routledge, Abingdon
McGuire M (2012) Organised crime in the digital age. John Grieve Centre for Policing and Security and BAE Systems Detica
McRobbie A, Thornton S (1995) Rethinking "moral panic" for multi-mediated social worlds. Br J Sociol 46(4):559–574
Odabaş M, Jolt TH, Breiger RL (2017) Markets as governance environments for organizations at the edge of illegality: insights from social network analysis. Am Behav Sci 61(11):1267–1288
Paoli L (2002) The paradoxes of organized crime. Crime Law Soc Chang 37(1):51–97
Philips D (2003) 'Three "moral entrepreneurs" and the creation of a "criminal class in England, c.1790s-1840s', *Crime, Histoire et Societes* 7:79–107
Ruggiero V (2017) Hybrids: on the crime-terror nexus. Int J Comp Appl Crim Justice. https://doi.org/10.1080/01924036.2017.1411283
Sergi A (2015) Divergent mind-sets, convergent policies. Policing models against organised crime in Italy and in England within international frameworks. Eur J Criminol 12(6):658–680
Sergi A (2016) National security vs criminal law. Perspectives, doubts and concerns on the criminalisation of organised crime in England and Wales. Eur J Crim Policy Res 22(4):713–729
Simon J (2007) Governing through crime. How the war on crime transformed American democracy and created a culture of fear. Oxford University Press, Oxford
Simon J, Feeley M (2013) Folk devils and moral panics: an appreciation from North America. In: Downes D, Rock P, Chinkin C, Gearty C (eds) *Crime, social control and human rights. From moral panics to states of denial, essays in honour of Stanley Cohen*. Willan, London
Smith DC Jr (1975) The mafia mystique. Basic Books and Hutchinson, New York and London
Smith DC Jr (2016) The alien conspiracy theory: aka the elephant in the front parlor. Eur Rev Organ Crime 3(1):50–77
Steinmetz KF (2016) Hacked. A radical approach to hacker culture and crime. New York University Press, New York
Symantec (2008) Report on the underground economy July 07–June 08. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf
Thibodeaux J (2014) Three versions of constructionism and their reliance on social conditions in social problems research. Sociology 48(4):829–837
Thompston B, Williams A (2013) The myth of moral panics: sex, snuff and Satan. Routledge, London
Ungar S (2001) Moral panic versus the risk society: the implications of the changing sites of social anxiety. Br J Sociol 52(2):271–291
van Duyne PC (2011) (transnational) organised crime, laundering and the congregation of the gullible. Tilburg University, 14 March. Available at: http://www.cross-border-crime.net/index.php?page=Free%20Downloads
van Duyne PC, Nelemans MDH (2012) Transnational organized crime: thinking in and out of Plato's cave. In: Felia A, Gilmour S (eds) Routledge handbook of transnational organized crime. Routledge, London
van Duyne PC, Vander Beken T (2009) The incantations of the EU organised crime policy making. Crime Law Soc Chang 51:261–281
von Lampe K (2008) Organized crime in Europe: conceptions and realities. Policing 2(1):7–17
Waddington PAJ (1986) Mugging as a moral panic: a question of proportion. Br J Sociol 37(2):245–259
Wall DS (2005/15) The internet as a conduit for criminals (pp, 77-98). In: Pattavina A (ed) Information technology and the criminal justice system. Sage, Thousand Oaks
Wall DS (2008) Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime. Int Rev Law Comp Technol 22(1–2):45–63
Wall D (2015) Dis-organised crime: towards a distributed model of the organisation of cybercrime. Eur Rev Organ Crime 2(2):71–90
Weaver DA, Bimber B (2008) Finding news stories: a comparison of searches using Lexisnexis and google news. J Mass Comm Q 85(3):515–530
Williams Ph (2001) Organized crime and cybercrime: synergies, trends and responses. Arresting Transnational Crime. An Electronic Journal of the US Department of State 6(2)
Woodiwiss M, Hobbs D (2008) Organized evil and the Atlantic alliance: moral panics and the rhetoric of organized crime policing in America and Britain. Br J Criminol 49(1):106–128
Yip M, Webber C, Shadbolt N (2013) Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Polic Soc 23(4):516–539