Copyright © 2016 International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089
July – December 2016. Vol. 10 (2): 170–187. DOI: 10.5281/zenodo.163400/ IJCC is a Diamond Open Access (Authors / Readers No Pay Journal).

Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom

Anita Lavorgna[1]
University of Southampton, United Kingdom

Anna Sergi[2]
University of Essex, United Kingdom

Abstract

This paper, based on discourse analysis of policy documents, departs from a critique of the juxtaposition of the terms "serious" and "organised" in policies against organised crime in the UK. The conceptualisation of organised crime as national security threat supports our hypothesis that a similar critique can be applied to the emerging narrative of cyber-organised crime in the country. We argue that, whereby organised crime has become essentially "serious" as consequence of its characterisation as a national security threat, cyber crime is becoming "organised" in the policy narrative because of its seriousness. The seriousness and organisation of cyber crime justifies its inclusion within the national security agenda, thus accessing the procedural benefits of criminal intelligence assigned to national security threats. The implications associated to the evolution of such narratives in policy-making need to be assessed while policies are still developing.

Keywords: Organised Crime, Cyber crime, Serious Crime, National Security Threat.

Introduction

In the United Kingdom (UK), at the policy level, the conceptualisation of organised crime[3] has been evolving and refining over the years – as showed by the growing numbers

[1] Lecturer in Criminology, Faculty of Social and Human Sciences, University of Southampton, Murray Building, Highfield Campus, SO17 1BJ, United Kingdom. Email: A.Lavorgna@soton.ac.uk

[2] Deputy Director, Centre for Criminology, Department of Sociology, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, United Kingdom. Email: asergi@essex.ac.uk

[3] A whole range of different crimes and groups are included within the same label of organised crime (Calderoni, 2010; Finckenauer, 2005). From a legal perspective, in the UK the reference frame for a definition of OC is the 2015 Serious Crime Act, section 45(6), according to which *"organised crime group" means "a group that (a) has as its purpose, or as one of its purposes, the carrying on of criminal activities, and (b) consists of three or more persons who act, or agree to act, together to further that purpose"*. The very low standards that have been set for inclusions of different and diverse

of policy documents published since 2000.[4] These documents have been criticised as the result of "policy construction" based on attempts of securitisation – i.e., the social construction of organised crime as a threat (Carrapico, 2014) – rather than on evidence-based observations of the evolution of organised criminality in the country (Hobbs, 2013; Campbell, 2014). As a result of this process, organised crime since 2010 appears in the UK as national security threat and, as such, it is dealt with through an enhanced national strategy centred on criminal intelligence (King & Sharp, 2006; HM Government, 2010; Sergi, 2015a).

As we will see in the following sections, the conceptualisation of organised crime in the UK has pivoted around a broad and undefined notion of *seriousness*.[5] This "paradigm of seriousness" as well as ambiguities around the notion of organised crime have been used in policy-making for producing consensus around increased resources and domestic powers (Edwards & Gill, 2006; Edwards & Levi, 2008). Arguably, defining a group of offenders as "organised" allows the approval of more intrusive and secretive investigative power (van Duyne, 2004; Levi, 2014).

Given the increasing consensus that the cyberspace offers plenty of new possibilities for committing *serious* types of cyber crime[6], and considering the emergence of a non-evidence-based "cyber-organised crime" rhetoric in the international and European public discourse (Lavorgna, 2016), it is worth investigating whether a similar rhetoric has been developing also in the UK. If this is the case, the juxtaposition of "organised", "serious", and "cyber" would entail key implications for regulatory measures and policing in national strategies.

The framework within which we situate our work is social constructivism applied to security threats. Such an approach, borrowed from the field of international relations (Katzenstein, 1996; Huysmans, 2004; McDonald, 2008) has already been used in the field

phenomena as organised crime have already been severely criticised in academia (Campbell, 2013, 2014; Hobbs, 2013; Sergi, 2016). These criticisms are not new: already in the past, "organised crime" has been accused to be used as "a catchphrase to express the growing anxieties" on the expansion of illegal markets and the perceived growing undermining of the legal economy and political institutions (Paoli, 2002, p.51).

[4] See for example, the 2004 Home Office's White Paper *One step ahead: a 21st century strategy to defeat organised crime*, the 2009 Cabinet Office paper *Extending our reach: a comprehensive approach to tackling serious organised crime*, or the 2010 Home Office strategy *Local to Global: reducing the risk from organised crime*.

[5] Some definitions of "serious crime" exist but they are linked to the law and the punishability threshold. Consider for instance the Palermo Convention on Transnational Organised Crime, 2(b), according to which "serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty or the Serious Crime Act 2015, which punishes participation in crimes punishable with seven years imprisonment). In the criminological debate, the conceptualisation of "seriousness" is also linked to what the law classifies as "serious crimes" in terms of their potential harm to the general public and their degree of proximity and sophistication (Edwards and Levi, 2008).

[6] Here broadly defined, in line with the 2001 Budapest Convention on Cybercrime, as offences against the confidentiality, integrity, and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, and misuse of services); computer-related offences (computer-related forgery and computer-related fraud); content-related offences (offences related to child pornography); offences related to infringements of copyright and related rights.

of drugs, asylum, and immigration among others (Huysmans, 2002), and even organised crime (Carrapico, 2014). It allows us to look at the topics at hand through the lenses of the securitisation conceptual framework (Buzan et al., 1998) and to explain the significance of language in national policy-making in enlarging the concept of security to cover also for crime issues (Farrand & Carrapico, 2012).

In our study, based on discourse analysis of policy documents, we argue that the juxtaposition of the term "serious" and the term "organised" in policies on organised crime can be observed also in the emerging narrative of cyber-organised crime in the UK: there is in fact an inverted parallelism between the characterisation of organised crime as serious threat to national security and the developing characterisation of cyber crime as serious crime too, therefore organised "by default". We argue that this juxtaposition of "serious" and "organised" in framing cyber crime is an example of securitisation and more in general can be understood as "shorthand for the construction of security" (McDonald, 2008, p.566). Whereby organised crime has become inherently *serious* as consequence of its own securitisation process (Sergi, 2016), mirrored in its current national security characterisation, cyber crime is becoming *organised* in the policy narrative *because of* its seriousness, which shall justify its inclusion within the national security agenda as well. This inclusion shall mean accessing the procedural benefits of criminal intelligence paired to national security threats. The implications associated to the evolution of such narratives in policy-making need to be assessed while policies are still developing.

This paper will first present the process of securitisation, which has allowed the "seriousness" of organised crime to enter successfully the national security agenda. After explaining our methodology, the paper will present our analysis of the language used for describing cyber crime in policy documents. The findings support our main argument that through the use of the word "serious" also the word "organised" has arbitrarily migrated into the conceptualisation of cyber crime.

Background

The securitisation of organised crime

Organised crime in the UK is mainly described as a threat for the economic sector nationwide rather than as an issue for traditional street policing approaches (NCA, 2014a; Home Office, 2010a). As organised crime is detrimental for the financial health of the country, and any "economic deficit is also a security deficit" (Home Office, 2010b, p.4), organised crime has been conceptualised as a security threat since 2010, with the Home Office (2010b) declaring officially that organised crime – which is *serious*– is a threat to national security, thus explicitly establishing the link between national security and organised crime through its *seriousness* (Sergi, 2016). As highlighted by the Home Office (2013, p.7) in the latest strategy against Serious and Organised Crime, "the strategy uses the framework we have developed for our counter-terrorist work", which confirms the national security dimension. However, this high policing approach has been criticised, as it incurs the risk of losing different local manifestations of organised crime (Hobbs, 2013).

The process whereby a threat is identified as a security issue or "constructed" to create legitimacy and authority for dealing with that issue (Weaver, 1995; Neal, 2009) is the securitisation process. The way "construction" works towards securitisation can differ. It has been argued that by focusing on the "social significance of language" (Huysmans, 2002, p. 44) – i.e., the idea that, by bringing social practices into a communicative

framework, language supports the integration of social relations – we can understand how the speech act can construct a security problem. For instance, in the case of organised crime as policy category in the UK, sentences like "organised crime is a serious threat to our economy" or "any threat to our economy is a security threat" are not neutral statements: security language is made of a body of rules like any other language (Foucault, 1972), and the repetition of specific *organisations* of sentences – one sentence following another, one word following another – makes these enunciations security utterances. As Wæver argued (1995, p. 55), "by uttering 'security', a state representative moves a particular development into a specific area, and thereby claims a special right to use whatever means necessary to block it". This securitisation of the UK public discourse has been observed for instance in the wake of the United States 9/11, London 7/7, and continued Islamist attacks: counterterrorism moved to the top of the policy agenda through the production of a narrative by policy-makers. This resulted in the proliferation of counterterrorism legislation, increased budgets for counterterrorism, and increased state powers (Huysmans & Buonfino, 2008; Bright, 2012; Heath-Kelly 2013).

Since organised crime has been subsumed within the national security agenda in 2010, there is a direct connection between the serious character of organised crime and its national security status. It has been already noticed (Sergi, 2016) that the "serious" character attached of organised crime in policy-making has supported changes in criminal law with the Serious Crime Act 2015, which criminalises organised crime participation. If a threat is serious, then the law needs to intervene also through criminalisation.

The process of securitisation of organised crime is not just a recent trend (Campbell, 2014). Historically, organised crime in the UK has been paired with *serious crime* since the late 1990s, when the National Criminal Intelligence Service included in its annual national threat assessment an evaluation of both serious *and* organised crime (NCIS, 2000). With the use of the word *serious* in the Serious and Organised Crime Policing Act 2005 establishing the Serious Organised Crime Agency (SOCA, replaced in 2013 by the National Crime Agency (NCA)), a "paradigm of seriousness" officially became a quintessential feature of policy on organised crime in the country. The paradigm of seriousness can be defined as a pattern of assertions supporting the underlying idea that most serious crimes *ought to be* organised as well as most organised *crimes* (emphasis on the plural) raise concerns because of their seriousness (Sergi, 2016).

From a policing perspective, the marriage between serious and organised has been strengthened also because of the difficulty in securing convictions against "organised criminals"; the focus on the seriousness of crimes that are also organised has disregarded the proof of the organisational character of criminal groups for the purposes of crime classification (Campbell, 2013; Sergi, 2014, 2015b). This aspect has been reviewed in the latest Serious Crime Act 2015, with the new offence for participation in organised crime groups' activities (Sergi, 2016).[7] In essence, in order to be prosecuted through the support of criminal intelligence agencies (namely the NCA), a crime needs to be *serious enough* (Campbell, 2013).

[7] The new Serious Crime Act 2015, at section 45(4b) describes activities of organised crime groups as offences punishable "with imprisonment for a term of 7 years or more", thus serious offences. The focus, in line with Sergi's "Activity Model" (Sergi, 2014, 2015a), is on the criminal activity, identified as *serious* through its sentencing classification.

The link between the "seriousness" of crimes and their "organised" character has been also established through the ranking of criminal threats in the National Intelligence Model (NIM) as developed since the 1990s by the National Criminal Intelligence Service (NCIS, 2000). There are three levels of policing based on *risk* and *harm* and linked to the criminal capacity of groups: (1) single-jurisdictional for local issues (gang crimes), (2) multi-jurisdictional for cross-border issues, and (3) national and international for "serious and organised" crime (Centrex, 2007, p.12). This is reflected in the National Security Strategy (Home Office, 2010b), which also classifies organised crime both within tier 2 priority risks (as nationally born and bred threat) and within tier 3 priority risks (as threat coming from abroad). In common understanding, therefore, the seriousness of organised crime equates to the *sophistication* of criminal networks.

In a securitisation framework that looks at the language of security constructivism, it is not indifferent that in its 2013 *Serious Organised Crime Strategy* the Home Office approved the label of "serious" *in addition to* "organised" (serious + organised). This choice was clearly linked to the necessity of centring the strategy on the "seriousness" rather than the "organisation" of crimes. As the Home Office (2013, p. 13) declared:

> This strategy for dealing with serious and organised crime is issued to coincide with the creation of the NCA. It reflects significant changes in organised crime and […] also sets out our response to serious crime, which may not always be 'organised' but requires a national response, notably many aspects of fraud and child sexual exploitation.

Hence, not all serious crimes are organised. On the other hand, there might be organised crimes not serious enough to be dealt with at the national level instead (such as organised pick pocketing). Overall, the Home Office suggests a focus on serious crimes, both organised and not organised, but not the opposite: only organised crimes which are serious are part of the strategy and fall within the scope of the NCA. This is essentially justified by the necessity to centralise investigations within criminal intelligence agencies with all the benefits that "reserved matters" of national security entail for law enforcement (Home Office, 2013, p. 13). The focus on criminal intelligence to counter organised criminal networks advocated by the Home Office and the National Security Strategy, indeed, opens a number of doors and resources for law enforcement (van Duyne, 2004; Edwards & Levi, 2008). For example, this includes a national, rather than regional or local approach, with more funding available and also an increased secrecy in terms of freedom of information procedures. This also contributes to an alarm related to financial crimes and economic repercussions of certain large-scale crime that bring large-scale investigations and the possibility to recover proceeds (Sergi, 2016). It would be difficult – without intelligence data and beyond the immediate benefits for policing – to actually understand whether the securitisation process of organised crime happened because of rational reactions from the authority to secret intelligence data or out of other contingencies. However, this process is not unique to the UK: similar securitisation attempts took place for instance at the EU level, which gradually expanded its counter-organised crime efforts through both political and legal instruments (Carrapico, 2014; Lavorgna, 2016). Therefore, literature on this subject can be a good starting point for such an enquiry.

Framing "cyber-organised crime"

There is increasing consensus that the cyberspace offers plenty of new possibilities for committing *serious* types of crime, including crimes traditionally associated with organised crime (Europol, 2015). Research in the US, for instance, showed a growing public concern with the seriousness of certain cyber crimes (e.g., financially motivated crimes such as Internet frauds) and the criminal justice ability to control it (Burns et al., 2004; Rebovich, & Layne, 2010; Bossler & Holt, 2012). In the UK, it has been suggested that, while different cyber crimes are dealt with differently in policing depending on their perceived seriousness by public, political, and expert assessments (Yar, 2013), there is overall a general concern, propagated by the media, that the Internet is dangerous and criminogenic (Wall, 2008). Hence, it is not surprising that cyber crime is receiving increasing attention, also at the policy level. Problematically, the use of a seriousness connotation – that is, cyber crime is a serious type of crime – has led to an assumption of the organisational character of certain manifestations of cyber crime (among others, Rider, 2001; Europol, 2015).

We argue that, in the same way the "serious" character of organised crime has bought the phenomenon a place among national security threat, the juxtaposition of "serious" and "organised" can trigger the securitisation of cyber crime. Even if we agree that cyber crime is serious, is it correct to infer that it is often organised? The answer, we argue, is not. The existing evidence-based criminological literature has not yet sufficiently addressed the nature and the rate of criminal adaptability. There are only a few studies (such as Lusthaus, 2013; Hutchings, 2014; Lavorgna, 2015; Leukfeldt, Lavorgna, & Kleemans, 2016) focusing on the presence of both traditional organised crime and newly formed criminal groups in cyberspace. The scarce research on this topic, even when of great criminological interest, is mostly of speculative or anecdotal nature (see, among others, Brenner, 2002; McCusker, 2006; Choo & Smith, 2007). The issue seems to be linked to the technical specialism required to collect and analyse data from the web, often through the use of computer science. Some recent studies have carried out more systematic analyses (for instance, McGuire, 2012). However, scholars are cautious in their conclusions and tend to stress how more detailed data and analyses are needed: most of the existing studies are in fact mostly based on secondary sources whose accuracy might be questionable. Also, they often adopt very broad working definitions of "organised crime".[8] As known in organised crime studies, extremely low standards for inclusions of different and diverse phenomena as "organised crime" eventually turn the concept into "an empty signifier" (Carrapico, 2014, p. 11).

Inferences from these studies about the presence of organised crime in cyberspace can be misleading: online criminal opportunities might be exploited also by sole offenders, and there is still scarce evidence as to whether new criminal actors created organised groups in cyberspace and/or traditional organised crime groups operate in online marketplaces. Rather, evidence points in the direction of the presence in cyberspace of loose, flat, and fluid networks, generally without a common functional unit (Martin, 2014; Wall, 2014, 2015). Despite the lack of clear evidence on the presence of organised crime groups in cyberspace, however, a cyber-organised crime narrative has been developing over the last decade also in policy documents at the European and international level, where the notion

[8] For a more complete critical review of the literature on cyber organised crime, see also Lavorgna, 2016 and Leukfeldt, Lavorgna, & Kleemans (2016).

of cyber-organised crime has been used to emphasise certain security threats as they "ought to be" organised crime (Lavorgna, 2016). Once again (van Duyne, 2004; van Duyne & Vander Beken, 2009) the vague concept of organised crime seems to be used in order to make the case for strong crime repression.

Methodology

In this study, we carried out a discourse analysis of UK policy-making documents to assess whether and to what extent the cyber-organised crime narrative has been developing in the country. Official outputs from the major relevant agencies and institutions addressing the possible intersections between organised crime and cyber crime at the national level were identified by looking at the documents, press speeches, and press sections of their online databases through a keyword search ((cyber OR internet OR web) AND organis*). We run the searches in the websites of the Home Office and the NCA (and its predecessor SOCA),[9] the Serious Fraud Office (SFO), the Crown Prosecution Service (CPS), the Crown Office and Procurator Fiscal Service (COPFS, the Scotland's Prosecution Service), the Public Prosecution Service for Northern Ireland (PPS), the National Police Chiefs' Council (NPCC, former Association of Chief Police Officers (ACPO)), the Child Exploitation and Online Protection Centre (CEOP), the Metropolitan Police, the City of London Police,[10] Police Scotland, and the Police Service for Northern Ireland. Documents published until 30st April 2016 were taken into consideration, for a total of 1693 results. Once the documents were identified, they were manually sorted out to dismiss those that were not relevant to this study. The final sample size for the analysis comprised 92 documents.[11] The accuracy of the study is limited by the fact that the webpages of the selected agencies might not necessarily constitute archives of the whole relevant content ever published, and we have not considered all possible policy making agents. However, to minimise these limitations, we kept the keyword searches as comprehensive as possible and we covered all major relevant agencies and institutions in the UK.

Detailed coding was carried out throughout the files to capture, classify, and sort the relevant content. This data-dependent process took into consideration a wide variety of diverse themes and information, summarised in Table 1. NVivo, a data analysis software

[9] As regards the SOCA, given that it no longer exists, documents were retrieved via the database that can be found at the following link: https://www.gov.uk/government/organisations/serious-organised-crime-agency.

[10] The Metropolitan Police was chosen as the largest one in England and Wales, and the one with national competence and powers in complex organised crime investigations. The City of London Police was chosen because it is the main police force dealing with financial crimes including those committed online.

[11] Home Office: 311 results, 34 relevant. National Crime Agency (NCA): 125 results, 24 relevant. Serious and Organised Crime Agency (SOCA): 11 results, 4 relevant. Serious Fraud Office (SFO): 7 results, 0 relevant. Crown Prosecution Service (CPS): 463 results, 3 relevant. The Crown Office and Procurator Fiscal Service (COPFS): 4 results, 0 relevant. The Public Prosecution Service for Northern Ireland (PPS): 0 results, 0 relevant. National Police Chiefs' Council (NPCC): 138 results, 4 relevant. Child Exploitation and Online Protection Centre (CEOP): 34 result, 3 relevant. Metropolitan Police: 62 results, 5 relevant. City of London Police: 35 results, 13 relevant. Police Scotland: 18 results, 2 relevant. Police Service for Northern Ireland: 485 results, 0 relevant.

package that allows managing and arranging unstructured information, was used to systematically organise and analyse the data sampled.

Table 1. Coding scheme

CATEGORIES	SUB-CATEGORIES
INSTITUTION	Home Office; NCA; SOCA; CPS; NPCC; MetPolice; City of London Police; Police Scotland
TYPE OF DOCUMENT	News/press release (focus on: specific law enforcement operation, quote, reference to report/official announcement); report/strategy; speech; website; blog; policy paper; minutes
YEAR	From 2010 to 2016
WHAT (criminal activity discussed in the document)	Arms trafficking; counterfeit and pirated goods; drug trafficking; fraud; general cyber crime; hate crime; human trafficking; malware; money laundering; pedopornography
ORGANISED CRIME (what "organised crime" is about, its relationship with the "cyber" component)	Organised crime group; cyber crime as OC activity; cyber crime as OC threat; cyber crime for OC funding

In the analysis, special attention was given to the framing[12] and the evolution of the discourse, in line with our theoretical approach. Indeed, the language used in policy documents to present a crime issue is of key importance to gain a better understanding of its social construction by policy makers towards political decision makers, law enforcement, and the broader public (Druckman, 2001; Stritzel, 2012; Carrapico, 2014). It should be underlined that our study analyses an emerging narrative as it develops, hence it has the intrinsic limitation of information being incomplete and potentially broadening as we proceed. Consequently, the analysis has to be cautious. Nonetheless, as it will be further discussed in the conclusive section of this paper, we believe it is important to analyse, interpret, and in case debunk policy discourse before it crystallises in a certain security language or it further sets policy agendas, with important consequences in terms of resource allocation and action prioritisation.

Results

Institution and type of document

The Home Office (34 documents), the NCA (24 documents) and the City of London Police (13 documents) were by far the agencies that used more the cyber-organised crime narrative, followed by the Metropolitan Police (5 documents), SOCA and the NCPP (4 documents each), the CPS (3 documents), CEOP (3 documents), and Police Scotland (2 documents). No relevant documents were found in the other agencies considered.

[12] Defined as "the process by which a source defines the essential problem underlying a particular social or political issue and outlines a set of considerations purportedly relevant to that issue" (Nelson, Clawson, & Oxley, 1997, p. 222).

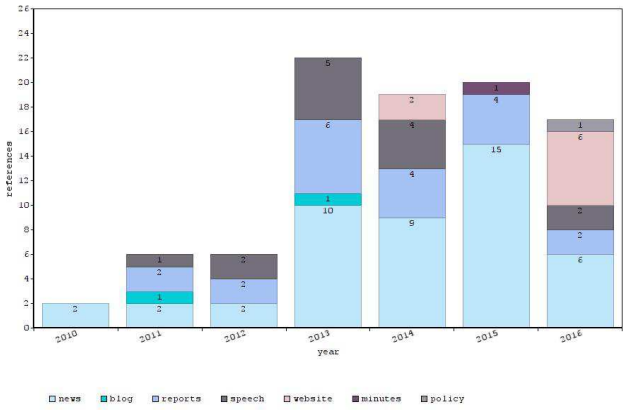
Most of the documents analysed are news or press releases (44 documents), followed by reports or strategy-setting documents (20), speeches (14), website pages (10), blog entries by law enforcement officers and policy makers (2), policy papers (1), and meeting minutes (1). However, if we look more in detail into the "news or press releases" category, we discover that only 19 documents link organised crime and cyber crime in reporting a specific law enforcement operation. Among these, only in 5 cases the cyber-organised crime narrative is not part of a quote by national policy makers or law enforcement officers. The remaining documents (therefore 14 documents) rely on this narrative by making references to official announcements, speeches, or other published reports. Hence, there is a clear prevalence in using the cyber-organised crime narrative in sources presenting an official discourse. This suggests an attempt to expand the counter-cyber crime efforts through the superimposition of the notion of cyber-organised crime (Lavorgna, 2016), similarly to what happened with the organised crime narrative in the past (Paoli, 2002).

Year

No documents using or suggesting a narrative of cyber-organised crime were found before 2010. The number of relevant documents is rather scarce in the time period stretching from 2010 to 2012 (with respectively 2, 6, and 6 documents) even if, for instance, already the former SOCA in its reports warned about "the threat of technology-enabled organised crime" (SOCA, 2011, p.16). From 2013 onwards, the number of relevant documents significantly increased, reaching its highest number in 2013 (22 documents), and counting high numbers also in the following years (19 in 2014, 20 in 2015, and 17 until the end of April 2016, which suggests that a new peak will be reached in 2016). It is worth noting that 2013 was the year when the NCA – the UK's lead national agency against serious and organised crime – was launched, assuming a number of responsibilities of other agencies.

Figure 1 below shows the clear increase in the number of references, and specifies their type. Please note that for the year 2016 only documents released until 30 April were taken into consideration.

Figure 1 – Type and number of references per year



What

Most documents, when linking cyber crime and organised crime, deal with cyber crime in general (49 documents), without making any reference to specific cases but rather treating cyber crime as a hodgepodge of serious criminal activities and assuming the organisational aspect. Consider for instance the following example, where the criminal activities gathered under the cyber crime umbrella are so diverse that potential victims can range from banking systems to abused children:

> Cyber crime is no longer about those who seek to access computer systems for fun or to prove it can be done. The criminals behind such crimes are organised, and seek to take advantage of those using Internet services. Whether this is for •nancial gain, or as threats to children, the effect on the victims can be devastating" (Home Office, 2010c, p.4, forward by the Parliamentary Under Secretary of State for Crime Reduction).

Similarly, in the following example, the Minister of Internet Safety and Security emphasises the criminogenic features that cyberspace offers with particular reference to organised crime groups:

> Advances in technology offer criminals, particularly organised criminals, the scope to commit new types of crimes on an unprecedented scale and across jurisdictions (Shields, 2016).

It is worth noting that these policy documents rarely disclose their methodology and share their primary data, making it practically impossible to check effectively their findings against evidence.

Online frauds (23 documents), pedopornography (10 documents), malware (including ransomware, 6 documents), Internet-facilitated drug trafficking (6 documents), counterfeit and pirated goods (6 documents), Internet-facilitated human trafficking (2 documents), money laundering (1 document), and arms trafficking (1 document) follow in number. There is an apparent contradiction with recent critical research showing how most criminal actors in cyberspace do not gather in well-defined organisational units or enterprises (among others, Lavorgna, 2015; Wall, 2015; Leukfeldt, Lavorgna, & Kleemans, 2016). This can be explained if we notice that most documents use a very general language, mostly without reference to particular cases when linking specific cyber crime activities to organised crime. Consider for instance the following snippet, where a direct relationship between the online sale of counterfeit goods and "other" organised crime is assumed:

> Many fraudsters will use the proceeds from selling counterfeit goods to fund other types of serious organised crime (City of London Police, 2016).

Conversely, the following excerpt suggests the involvement of organised crime groups in a variety of *serious* criminal activities:

> The scale of the threat from serious and organised crime has been demonstrated by high pro•le cases of child sexual exploitation; growing use of cyber techniques by organised criminals to commit fraud and trade illegal drugs and •rearms on the

> internet; and the spread of banking malware responsible for losses of hundreds of millions of pounds" (Home Office, 2015, p. 5, forward by the Home Secretary).

Once again, this reinforces the interpretation that "organised" is used *en passant* as an attribute of crimes being perceived as serious.

Organised Crime

If we consider what it is meant by "organised crime" when paired with a cyber-related attribute, the analysis shows that in most cases it is somehow implied that (traditional, offline) organised crime *groups* operate online (55 references). For instance, in the words of Home Secretary Theresa May (Home Office, 2014), "someone who is scammed on the internet, or finds their computer infected by malware that harvests their personal and financial data to be sold into criminal markets, or finds they have spent their savings on fake shares – all these activities can be traced back to organised crime".

However, apart from rare cases (5 documents) when reference to organised crime was made to mention a specific law enforcement operation (see subsection *Institution and type of document* above), the documents never refer to a specific organised crime group. A total of 22 references consider cyber crime as a specific type of organised crime *activity*, and 5 references imply that cyber crimes activities are somehow a *funding source* for traditional organised crime groups. This is in line with the "Activity" focus of the organised crime strategy in the UK that has already been critiqued as it leads to logical fallacies (Sergi, 2015a; 2016). Finally, 17 references define explicitly cyber-organised crime as a specific type of *threat*. Hence, similarly to what has been observed in policy making at the European and international level, the cyber-organised narrative seems to foster definitional ambiguities (Lavorgna, 2016). In addition, it completely ignores the conceptualisation of organised crime as *power*, seeking a social function through the control over the production and distribution of a certain commodities in the underworld, protection services, or an alliance with political and economic elites (von Lampe, 2008).

Discussion

We argue that in the documents analysed the adjective "organised" is often used as synonym of "serious", in line with a successful *paradigm of seriousness,* tool of a securitisation process of cyber crime. Seriousness is intended as sophistication, as described above. This narrative seeks no longer to qualitatively assess the distinct features of organised crime in the case of cyber crime. Rather, the "organised" feature is linked to the seriousness of certain online criminal activities. For instance, the NCA Deputy Director McComb commented the arrest of some suspected of setting up Silk Road 2.0 (a criminal marketplace in the so-called deep web, the part of the web that is not indexed by standard search engines and therefore is hidden from the wider public) as follows:

> Criminals like to think that the dark web provides a safe, anonymous haven but in reality this is just like any other organised crime network. It may take time and effort to investigate and build a criminal case, but we are determined to identify and prosecute people caught dealing drugs and committing serious crime using the dark web (NCA, 2014b).

The underlying logic is that cyber crime is highly harmful and entails several risks: it is therefore serious and as such falls in the above-mentioned level 3 of the NIM, where it meets and overlaps with organised crime. It is understandable to give (certain) cyber crimes national security relevance. However, by using "organised" as an intensifier, criminal policy presumes a character of cyber crime that is not substantiated by research. The same *is-ought fallacy*[13] identified by Sergi (2015a) in institutional language and with reference to the seriousness paradigm for organised crime can therefore be recognised also in this case, where the notion of cyber-organised crime is used to establish a new security threat and therefore to justify the inclusion of cyber crime under the national security umbrella. In the same way organised crime *ought to be* a threat to national security because *it is* serious, cyber crime *ought to be* a threat to national security threat as well because *it is* (described as) "organised" without much empirical evidence supporting the overlapping of the two crime categories. In other words, cyber crime fits the seriousness paradigm: it can become a national security threat because of its seriousness; its seriousness however is inferred also by an unsubstantiated "organised" character. Hence, the label "organised crime" is once again assigned to certain criminal activities associated to a particular risk and/or harm as they were a unique threat ("the ought to be") in order to make them a matter of national security. In so doing, we lose sight of the fact that organised crime (from an historical, criminological, and "law in action" perspective) should refer to certain types of unlawful associations ("what is"), and ignores the conceptualisation of organised crime as *power* (von Lampe, 2008).

As a consequence, within law enforcement agencies and especially the NCA, the fight against cyber crime has been subsumed within the more general fight against organised crime. This is clearly symbolised by the creation of the National Cyber Crime Unit as a specialised team within the NCA, using NCA officers and resources. The cyber-organised crime narrative, because of the seriousness attached to the risks and harms of cyber crime, has *de facto* turned cyber crimes of whichever nature into national security threats. Within the same security constructivism approach that we have observed for organised crime, cyber crime has been constructed first as "serious" and then as "organised" to build its security profile. This has been achieved throughout a reiteration of the security utterances in relation to cyber crime in policy documents citing each other and referring to each other in circles. Another good example can be found in the linguistic shift used to justify the fact that the Child Exploitation and Online Protection Centre (CEOP) became an integral part of the NCA. While the CEOP itself (2012, p.5) stressed its "understanding of the similarities between organised crime and a large amount of child sexual exploitation and abuse" in justifying its becoming part of the NCA, it then made clear that "[…] often where true group offending does occur, this shares few of the characteristics traditionally associated with organised crime. Child sexual exploitation and abuse offending is, however, often extremely serious and complex in both execution and impact" (CEOP, 2013, p.6). Therefore, the seriousness of the criminal activity was the ground to use the organised crime connotation, and the organised crime narrative was used to give reason for merging within a national intelligence agency.

[13] 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.

Eventually, the common denominator between serious, organised, and cyber *crimes* (emphasis on the plural) – the national security connotation – also comes with yet another bonus, which is the peculiar attachment to disruption and prevention as key policing strategies of the National Crime Agency and its units. As it happened for organised crime – where the organisational characteristics of group criminal activities were assumed but eventually difficult to prosecute (Campbell, 2013; Sergi, 2016) – cyber crime too poses challenges from a juridical point of view: prosecution and investigation of cyber crimes is neither simple, nor straightforward (Brown, 2015; Dragan, 2015). Not only the amount of work required to follow crimes online explodes the limits of common police workload, but also it is not bound by traditional jurisdiction borders. In other words, disrupting and preventing cyber crime – by focusing on reducing the harm within the jurisdictional boundaries – is a much easier choice to distribute police work and success. In order to secure a focus on disruption, criminal intelligence agencies must be involved and in order to do so a national security connotation is needed too. The argument is again circular: cyber crime is "serious" because it poses complex issues to common policing. Moreover, it needs to be "organised" to fall within the remit of criminal intelligence agencies. The need to fall within the remit of criminal intelligence agencies is justified to secure the national security connotation and therefore the possibility to employ disruption techniques. As it has been observed, "disruption is a way of overcoming some of the problems encountered by police organizations in coping with heavy workloads" (Innes & Sheptycki, 2004, p.13). This seems to be the case for both organised crime and cyber crime and the challenges they pose to investigators and prosecutors.

Conclusion

One could argue that a commonality of understanding is more important than definitory precision, but in the case of cyber-organised crime this does not seem to be the case. In this new binary relationship cyber/organised, the threshold to consider something as "organised crime" is lowered, if possible, even more than it was for other serious and organised criminal activities in the country. As already remarked by Lusthaus (2013), there is the need to apply scholarly rigour to the question of whether criminals operating in cyberspace can fit formal definitions of organised crime. Without denying the possibility of organised crime groups increasingly operating online and of the creation of new organised crime groups in cyberspace, limited reliable data available do not allow to draw an exact comparison between the existing offline criminological categorisations and the new online phenomena (Lavorgna, 2015). The risk is that the cyber-OC narrative crystallises not because of new compelling evidence but because of a vicious circle, a mechanism of cross-fertilisation of sources and references. Overall, it seems the case that official sources of information are succumbing to the temptation to deploy the vague concept of *organised* in order to make the case for effective crime repression (in line with Lavorgna, 2016). The problem with the crystallisation of this security language is in setting and confirming a security agenda, which carries important consequences in terms of resource distribution and action prioritisation. From a policing perspective, the categorisation of cyber crime as "organised" crime, as said, carries a number of consequences. If cyber crime is *by default* organised crime, law enforcement will be called to act within the preferred tools of disruption and prevention rather than common policing strategies, which might be at times more appropriate (in cases for example of

support to victims). The high policing approach that is typical of national security threats carries an enhanced focus on the perpetrators of crimes and on the crime types. This means that issues like victimisation, radicalisation, social networks' relations and social harm at the local level struggle to come to the surface and require ad hoc plans and partnerships to function (Home Office, 2013).

However, the risk is not solely one of confusing terminology or definitions. Indeed, the law tends to follow up on evolving and established policy narrative. The Serious Crime Act 2015 is the perfect example of the crystallisation of a security paradigm and the seriousness connotation for organised crime in criminal law (Sergi, 2016). The new Serious Crime Act 2015, at section 45 (participation in activities of organised crime groups, see footnotes 1 and 5), represents the counterpart in criminal law of the narrative that has been employing terminology of serious and organised crime to construct a national security threat. On one side, organised crime (because of the seriousness paradigm) has been affirmed as a national security threat in criminal policy; on the other side, this affirmation is now the basis of new criminal law provisions. The new offence, in fact, almost entirely borrowing from the international legal framework (especially the UN Palermo Convention of 2000), lowers the threshold for organised crime at the point of being over inclusive of virtually every type of (serious) gang-style crime. Therefore, ambiguities of the language and the presumption of seriousness have made organised crime an over-inflated concept. Considering the emerging discourses on cyber crime, there is a risk that a similar crystallisation of cyber crime as a too general and empty signifier might also occur. Cyber crime is an umbrella term that covers for a broad range of criminal activities, carried out by different actors and characterised by different levels of "seriousness"; a presumption of seriousness or organisation could lower the threshold for virtually all crimes with a cyber component to be considered as a national security threat.

All the actors involved in the framing of an emerging security issue, including those at the policy level, should be careful and rigorous in the terminology employed. This is not a judgement on the operational capability of law enforcement, but rather a critical statement of their outputs in policy documents. The risk, otherwise, is that evolutions in criminal panorama will just shift attention and resources from the current fight against organised crime without a serious reflection on how to adapt the traditional criminological paradigms to better meet new security challenges in an effective and efficient way. The current use of the cyber-organised crime narrative should be at least problematised. As it is used now it does not allow for a sufficient level of understanding in public and scientific debates, while the juxtaposition of organised crime and cyber crime – united only by their seriousness characterisation – risks missing out the real picture of both phenomena.

References

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management*, *35*(1), 165-181.

Brenner, S. W. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law and Technology,* 4(1), 1-50.

Bright, J. (2012). Securitisation, terror, and control: towards a theory of the breaking point. *Review of International Studies*, *38*(4), 861-879.

Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55-73.

Burns, R. G., Withworth, K. H., & Thompson, C.Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, 32(5), 477-493.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Cabinet Office (2009). *Extending our reach: a comprehensive approach to tackling serious organised crime*. London: Home Office.

Campbell, L. (2013). *Organised crime and the law: a comparative analysis*. Bloomsbury Publishing.

Campbell, L. (2014). Organized Crime and National Security: A Dubious Connection? *New Criminal Law Review, 17*(2).

Carrapico, H. (2014). Analysing the European Union's responses to organized crime through different securitization lenses, *European Security, 23*(4), 601-661.

CENTREX (2007). *Practice Advice: Introduction to Intelligence-Led Policing, on behalf of Association of Chief Police Officers*. Wyboston, England: National Centre for Policing Excellence.

CEOP (2012). Threat Assessment of child Sexual Exploitation and Abuse. London: Child Exploitation and Online Protection Centre.

CEOP (2013). Threat Assessment of child Sexual Exploitation and Abuse. London: Child Exploitation and Online Protection Centre.

Choo, K. K. R., & Smith, R. G. (2007). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3*(1), 37–59.

City of London Police (2016). Counterfeit Goods. Retrieved from: https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/counterfeit-goods.aspx.

Dragan, A. T. (2015). Procedural Aspects of Cybercrime Investigation. *Journal of Legal Studies, 16*(30), 55-66.

Druckman, J. N. (2001). The Implications of Framing Effects for Citizen Competence. *Political Behavior, 23*(3), 225-256.

Edwards, A., & Gill, P. (2006). After Transnational Organised Crime? The Politics of Public Safety. In: A. Edwards & P. Gill (Eds.), *Transnational Organised Crime: Perspectives on Global Security* (pp. 264-282). London: Routledge.

Edwards, A., & Levi, M. (2008). Researching the organization of serious crimes. *Criminology and Criminal Justice, 8*(4), 363-388.

Europol (2015). *Internet facilitated organized crime (IOCTA)*. The Hague: European Police Office.

Farrand, B., & Carrapico, H. (2012). Copyright law as a matter of (inter)national security? The attempt to securitise commercial infringement and its spill over onto individual liability. *Crime Law Soc Change, 57*(4), 373–401.

Foucault, M. (1972). *The Archaeology of Knowledge and the Discourse on Language*. New York: Pantheons Books.

Heath-Kelly, C. (2013). Counter-Terrorism and the Counterfactual: Producing the "Radicalisation" Discourse and the UK PREVENT Strategy. *The British Journal of Politics and International Relations*, *15*(3), 394-415.

HM Government (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationery Office.

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

Home Office (2004). *One step ahead: a 21st century strategy to defeat organised crime*. London: Home Office.

Home Office (2010a). *Local to Global: reducing the risk from organised crime*. London: Home Office.

Home Office (2010b). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The stationery office.

Home Office (2010c). *Cyber Crime Strategy*. London: The stationery office.

Home Office (2013). *Serious organised crime strategy*. London: The Stationery Office.

Home Office (2014). Home Secretary's speech "Understanding and Confronting Organised Crime", delivered at the Royal United Services Institute on Wednesday 11 June. Retrieved from https://www.gov.uk/government/speeches/home-secretarys-speech-on-organised-crime-at-rusi.

Home Office (2015). *The serious and organised crime strategy: annual report for 2014*. London: The Stationery Office.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*(1), 1–20.

Huysmans, J. (2002). Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security. *Alternatives: Global, Local, Political, 27*(1), 41-62.

Huysmans, J. (2004). Minding Exceptions: Politics of Insecurity and Liberal Democracy. *Contemporary Political Theory, 3*(3), 321–41.

Huysmans, J., & Buonfino, A. (2008). Politics of Exception and Unease: Immigration, Asylum and Terrorism in Parliamentary Debates in the UK. *Political Studies*, *56*(4), 766-788.

Innes, M., & Sheptycki, J. W. E. (2004). From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the United Kingdom. *International Criminal Justice Review, 14*, 1-18.

Katzenstein, P. (1996). *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.

King, M., & Sharp, D. (2006). Global security and policing change: the impact of "securitisation" on policing in England and Wales. *Police Practice and Research,* 7(5), 379-390.

Lavorgna, A. (2015). Organised crime goes online: Realities and challenges. *Journal of Money Laundering Control,* 18(2).

Lavorgna, A. (2016). Exploring the cyber-organised crime narrative: The hunt for a new bogeyman? In P.C. van Duyne et al. (Eds.), *Organising fears, Crime & Law Enforcement New horizons and trends in Europe & beyond*. Oisterveijk: Wolf Legal Publishers.

Leukfeldt E. R., Lavorgna A., & Kleemans E. R. (2016). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime (under review)

Levi, M. (2014). Thinking about Organised Crime. Structure and Threat. *The RUSI Journal, 159*(1), 6-14.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52-60.

Martin, J. (2014). Lost on the Silk Road: online drug distribution and the "cryptomarket". *Criminology and Criminal Justice, 14*, 351–367.

McCusker, R. (2006). Transnational organized cyber crime: distinguishing threat from reality. *Crime, Law and Social Change, 46*(4), 257-273.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations,* 14(4), 563–587.

McGuire M. (2007). *Hypercrime. The new geometry of harm*. Oxon (UK) & New York: Routledge.

NCA (2014a). *National Strategic Assessment of Serious and Organised Crime 2014*, London: The Stationery Office.

NCA (2014b). International law enforcement deals major blow to dark web markets. *News*. Retrieved from http://www.nationalcrimeagency.gov.uk/news/483-international-law-enforcement-deals-major-blow-to-dark-web-markets.

NCIS (2000). *The National Intelligence Model*, London: National Criminal Intelligence Service.

Neal, A. W. (2009). Securitization and risk at the EU border: the origins of FRONTEX. *Journal of Common Market Studies, 47*(2), 333-356.

Nelson, T. E., Clawson, R. A., & Oxley, Z. M. (1997). Media framing of a civil liberties conflict and its effect on tolerance. *American Political Science Review*, *91*, 567–583.

Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law and Social Change,* 37(1), 51–97.

Rebovich, D. J., & Layne, J. (with Jiandani, J. & Hage, S.) (2010). *The National Public Survey on White Collar Crime*, Morgantown, WV: National White Collar Crime Center.

Rider B. A. K. (2001). Cyber-organised crime. The impact of information technology on organised crime. *Journal of Financial Crime, 8*(4), 332-346.

Sergi, A. (2014). Structure versus Activity. Policing Organized Crime in Italy and in the UK, Distance and Convergence. *Policing, 8*(1), 69-78.

Sergi, A. (2015a). Divergent Mind-sets, Convergent Policies. Policing Models against Organised Crime in Italy and in England within International Frameworks. *European Journal of Criminology, 12*(6), 568-680.

Sergi, A. (2015b). Organised crime in English criminal law: lessons from the United States on conspiracy and criminal enterprise. *Journal of Money Laundering Control, 18*(2), 182-201.

Sergi, A. (2016). National security vs criminal law. Perspectives, doubts and concerns on the criminalisation of organised crime in England and Wales. *European Journal on Criminal Policy and Research* (online first), 1007/s10610-016-9304-3.

Shields, J. (2016). Baroness Shields on preventing crime in the digital age. *Speech*. Retrieved from https://www.gov.uk/government/speeches/baroness-shields-on-preventing-crime-in-the-digital-age.

SOCA (2011). *Annual Report 2010-11*. London: The Stationery Office.

Stritzel, H. (2012). Securitization, power, intertextuality: discourse theory and the translations of organized crime. *Security Dialogue, 43*(6), 549-567.

van Duyne, P.C. (2004). Fears, naming and knowing: an introduction. In: P.C. van Duyne, M. Jager, K. von Lampe, & J. L. Newell (Eds.), *Threats and phantoms of organised crime, corruption and terrorism*. Nijmegen: Wolf Legal Publishers, pp.1-21.

van Duyne, P.C., & Vander Beken, T. (2009). The incantations of the EU organised crime policy making. *Crime Law and Social Change, 51*, 261-281.

von Lampe, K. (2008). Organized Crime in Europe: Conceptions and Realities. *Policing, 2*(1), 7-17.

Wæver, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On Security* (pp. 46-86) New York: Columbia University Press.

Wall, D. (2015). Dis-organised crime: Towards a distributed model of the organisation of cybercrime. *The European Review of Organised Crime, 2*(2), 71-90.

Wall, D.S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers, & Technology*, *22*(1-2), 45-63.

Wall, D. S. (2014). Internet Mafias? The Dis-Organisation of Crime on the Internet. In S. Caneppele & F. Calderoni (Eds.), *Organised Crime, Corruption and Crime Prevention* (pp. 227-239). London, Springer,

Yar, M. (2013). The policing of Internet sex offences: pluralised governance versus hierarchies of standing. *Policing and Society*, *23*(4), 482-497.