The Challenges of Cybercrime Governance in the European Union

George Christou
**Politics and International Studies, University of Warwick, Coventry, UK*

Abstract
Information and Communications Technologies, in particular the Internet, have been an increasingly important aspect of global social, political and economic life for two decades, and are the backbone of the global information society today. Their evolution and development has brought many benefits but also the threat and practice of serious cyber attacks, cyber espionage and cybercrime within the virtual, networked ecosystem that we live in. In this context, the European Union over the past ten years has been developing its policies towards cyber threats. Drastically reducing cybercrime featured as a key priority objective in the Cybersecurity Strategy of the European Union (2013) delineating several lines of action, including enhanced operational capability to combat cybercrime. Focusing on the operational aspects and in particular the European Cybercrime Centre's Joint Cybercrime Action Taskforce, this article demonstrates how this represents novel, collaborative and flexible (informal) governance bounded by a broader formal milieu, reflecting the complexity of cybercrime investigations. It is also shown that, despite the relative success of J-CAT, challenges still remain.

Key words: European Union, cybersecurity, cybercrime, governance, Information and Communications Technologies

Introduction

Whilst the reporting of the impact of cybercrime no doubt varies widely – with estimates between half a million to one million people a day being affected (ENISA, Threat Landscape Report, 2016), there is no doubt given rapid technological developments and the growing importance of the Internet of Things (IoT), that it is an issue that has social, economic and political costs for citizens, governments and businesses. For the European Union (EU) cybercrime, if not addressed through the appropriate mechanisms, tools and processes can severely hinder the EU's plans for economic growth embodied in the Europe 2020 strategy (European Commission 2010a), the Digital Agenda for Europe (European Commission 2010b), and the Digital Single Market Strategy (European Commission 2015a). It will also impact adversely on the EU's ability to achieve the priorities outlined in the European Agenda on Security (European Commission 2015b) and the EU's Global Strategy (Council of the EU 2016). The Cybersecurity Strategy of the European Union (CSSEU) (European Commission and High Representative 2013) outlined as one of its strategic priorities the drastic reduction of cybercrime. Such a priority sat alongside achieving cyber resilience, developing cyber defence, developing the industrial and technical resources for cybersecurity and establishing an international EU cyberspace policy. In this context, whilst the focus in this article is on cybercrime, it is important to recognise that it does not sit in isolation from these other priorities. Achieving cyber resilience and reacting to and recovering from cyber attacks, for example, are very much related to addressing cybercriminal activity. In turn, cybercrime is not limited by borders - the Internet is global in nature and thus any strategy to reduce cybercrime must incorporate effective collaboration, coordination and cooperation not just within Europe, but also relevant agencies, international organisations, networks and actors in other countries and regions. Initiatives to tackle cybercrime, of course, did not simply begin with the CSSEU. The issue of computer crime dates back and was recognised by the European Community (EC) in the 1970s with Internet security subsequently incorporated into the EU's information society strategies and a series of framework decisions, directives, communications and strategies that sought to create legal clarity and improve network and information security resilience (Christou 2016).

Despite these efforts to construct a comprehensive approach, however, there was a recognition that obstacles continued to exist for dealing with cybercrime effectively within the EU. These included issues relating to jurisdictional boundaries, legal clarity, technical aspects related to tracing cybercriminals, asymmetric forensic and investigative capacities across Member States, insufficiently trained staff, limited capability with regard to information sharing, and inconsistent cooperation between actors involved in cybersecurity (European Commission 2012, p.3). Furthermore, law enforcement officials dealing with cybercrime bemoan the move to more sophisticated encryption by large Information and Communications Technology (ICT) companies and the problems of anonymity, in particular in relation to the use of the dark web by cybercriminals to conduct their activities effectively (European Parliament 2015, p.13).

The aim of this article is to focus on operational capability with a particular emphasis on the role of the Joint Cybercrime Action Taskforce (J-CAT) located with the EU's European Cybercrime Centre (EC3), which was established within Europol in January 2013. Moreover, its central contribution is to provide a more substantive understanding and characterisation of the emerging modes of governance around the operational aspects of cybercrime and the implications that this has for the evolving EU cybercrime ecosystem. This has become an important and challenging issue for the EU and Europol in relation to the legal framework that underpins cybercrime, in particular relating to efficient data collection, building trust in order to allow effective and timely information-sharing, and effective prosecution of cybercriminals in the operational sphere.

Whilst much work on EU agencies and in particular Europol has focused on its emergence, legitimacy and accountability, as well as its impact on EU-policy making (see Carrapiço and Trauner 2013; Busuioc et al 2011, 2012; Busuioc 2010, 2013), there has been very little academic attention paid to the implications of emerging cooperative governance arrangements within the EC3 and its operational dimension. Such operational governance has political and legal elements that impact debates on the effectiveness of such mechanisms for addressing the issue of cybercrime. This article seeks to situate itself and contribute to our knowledge on an evolving and novel governance mechanism within Europol and more specifically the EC3's J-CAT, through engaging with the literature on informal and formal governance (Christiansen and Neuhold 2013) and network organisations (Mueller 2010) within the emerging operational cybercrime ecosystem. The central argument developed in the article is that whilst novel governance arrangements such as J-CAT have arisen precisely because of the frustration with formal governance, challenges remain in the effective investigation and prosecution of cybercriminals transnationally. Furthermore, the suggestion in this article is that informal and formal governance are not mutually exclusive, but rather, complement each other even though certain tensions remain between the two that represent challenges to addressing the cybercrime challenge more effectively. The questions being asked then, relate to the emerging form of operational governance in relation to J-CAT, the degree to which it can be characterised on the formal-informal governance spectrum, and the implications of J-CAT governance relating to the challenges of cybercrime.

The article unfolds in four parts in order to address the above issues and questions. The first section provides an overview of the relevant conceptual and theoretical literature relating to formal and informal governance and networks. Section 2 offers a brief context in relation to the EU's broader cybercrime milieu. Section 3 provides an overview of the emergence and central functions, remit and features of EC3, and analyses J-CAT operational governance. It focuses on its key characteristics and novel innovations, and attempts to locate it on the formal-informal spectrum. It also discusses core challenges, issues and problems relating to J-CAT in the context of the broader formal governance environment within which it is located. The final section offers reflection on the role of J-CAT going forward and the implications for the EU's approach to the governance of cybercrime more broadly.

Formal and Informal Governance

Much of the literature on governance has focused on the formal elements of EU policymaking, from agenda setting to implementation, at multiple levels, among different public and private actors in the areas of low and more recently, high politics (for example, Eising and Kohler-Koch 1999; Jachtenfuchs 2001; Bache and Flinders 2005; Peters and Pierre 2009). Others have provided analyses of multiple types of governance – incorporating both formal and informal aspects – across different levels and dimensions (Bevir 2012; David Levi-Faur 2012). Alongside this, there has also been a growth in the literature that focuses specifically on informal politics and governance in the EU that seeks to dig beneath the formal institutional process to reveal the informal practices and governance arrangements across a host of policy domains. In doing so, it highlights the benefits and the implications of such governance arrangements for accountability, legitimacy and effectiveness (Justaert and Keukeleire 2011, p.15; Christiansen and Piattoni 2003; Christiansen and Neuhold 2012; Christiansen and Neuhold 2013). Issues of accountability and legitimacy are also raised in the literature on EU agencification – that is, the delegation of powers to agencies to deal with a plethora of perceived challenges and threats that cannot simply be dealt with through the 'normal' EU policy process (Busuioc 2013). In the area of Justice and Home Affairs in particular, much literature has focused on the degree to which agencies set up for the purposes of addressing specific challenges, have gained autonomy, and the implications this has for legitimacy, governance and EU policymaking (for example, Kaunert et al 2013. See also Occhipinti 2003; Mounier 2009; Kaunert 2010; Busuioc et al 2011; Carrapiço and Trauner 2013).

Such literature, it can be argued, is germane to the study of cybercrime in the EU context in the operational domain. Indeed, there is some overlap in such literature in so far as, first, informal governance and governance of agencies raise questions of efficacy, legitimacy and accountability. Second, both involve formal and informal dimensions, which is important in cybercrime given that there is a legal (substantive and procedural law) and institutional framework that underpins policy in this and related areas such as Network and Information

Security (NIS). In this sense, the relationship between the formal and informal has been conceptualised in a useful way by Helmke and Levitsky (2004, p729), in that they propose a typology of informal arrangements – complementary, accommodating, competing and substitutive – and how these relate to formal institutions and outcomes (Table 1).

Table 1 – Informal and formal governance

Performance of formal institutions		Effective	Ineffective
Outcomes of informal governance	Convergent	Result: Complementary informal institutions	Result: Substitutive informal institutions
	Divergent	Result: Accommodating informal institutions	Result: Competing informal institutions

Source: Helmke and Levitsky (2004, p729)

It is the purpose of this article and its main contribution, to explore formal and informal operational governance in cybercrime. In particular, it is to assess how operational aspects coexist with formal arrangements. In this context, it is widely acknowledged that governance encompasses formal and informal relationships and interactions (Christiansen and Neuhold 2013, p1197; Eberlein 2003, p.150). Thus for the purposes of this article, informal governance is being understood and defined as 'the operation of networks of individual and collective, public and private actors pursuing common goals – which lead to cooperation, patterned relations and public decisions – through regular though non-codified and not publicly sanctioned exchanges' (Christiansen, Follesdal and Piattoni 2003, p.7). To elaborate further, informal governance has a variety of characteristics and can operate under various modes, as well as taking on different functions. For example, in relation to modes, the informal governance literature refers to policy networks of different types: advocacy coalitions, expert-based epistemic communities or variable interest and resource based constellations (see Justaert and Keukeleire 2011, p-5-6). Useful as a starting point in relation to cybercrime is the definition of policy networks as 'semi-stable informal clusters of interdependent actors, who have or take a specific interest or stake in solving a certain policy problem and who dispose of resources required for shaping and implementing the policy, and who are willing to mobilize and pool these resources' (Ibid, p.5). Importantly, such policy networks are characterised by their flexibility, speed and expertise with regard to improving the capacity to resolve problems or tackle threats. This is most pertinent in cybercrime, as the discourse on effectiveness from a law enforcement perspective often evolves around being able to act in real time through flexible procedures and processes (EC3 First Year Report, 2014).

A further distinction is also helpful and indeed required that differentiates an associate cluster from a network organisation in the context of the informal-formal spectrum in cybercrime. To this end it is important to acknowledge that in relation to J-CAT, we are referring to consciously arranged groupings and not *de facto*, clustering patterns. That is, we must understand a network organisation 'as bounded and consciously arranged' and that 'the actors that participate in them *design* the relationships among a bounded set of individuals or organisations to pursue a common objective' (Mueller 2010, p.42). Also salient is that such networks retain (even if minimal) organisational characteristics – hierarchy, shared infrastructure, budgets, employees etc. to support network operations. Finally, the 'network form of organisation is a design choice, a method of association that actors can use or refrain from using based on a conscious assessment of their objectives and constraints' (Ibid.). When assessing the emergence of J-CAT and its informal governance characteristics then, we should be mindful that it was designed to avoid the constraints of traditional or formal governance procedures, but that it is still supported, and bound by the rules and procedures of EC3 and Europol, as well as being guided by the broader, relevant EU legal frameworks (Reitano et al 2015, p.143-144).

In relation to function, informal governance is a broad enough concept that allows the capture of complexity, characterised by a variety of levels, actors, logics and processes, which operate beyond formal policy as well as interacting with it. The fight against cybercrime involves multiple actors, is cross-jurisdictional and international in nature given the borderless nature of the internet, and involves public and private institutions, agencies and bodies coming together to identify, investigate and prosecute cybercriminals. It is also argued that informal governance, through bringing together relevant actors to address a specific issue, can lead to better output legitimacy through greater effectiveness on the ground. In turn, interactions within policy network organisations can lead to an environment conducive to trust-building and (thick) learning through (successful) doing. Conceptually then, informal governance can often provide an alternative – an escape route - where formal policy-making is constrained because an issue is particularly complex and an environment uncertain (Eberlein 2003, p.150).

However, whilst there are no doubt benefits to utilising informal governance, there are also normative concerns regarding the extent to which such arrangements provide for effective and legitimate governance. Some scholars point to questions arising from the potential impact on democratic legitimacy across three domains: authority, participation and assurance (Christiansen et al 2003, p.13). The first relates to the bypassing of legitimate – formal procedures – and the impact this has on policy-making; the second relates to who decides and what determines participation; and the third on how well informal arrangements actually address the policy problem.

Christiansen and Neuhold allude to the fact that the literature on informal governance demonstrates a mixed picture, across different contexts. Importantly, they argue that 'the real issue…concerns the identification of conditions under which informal governance is helpful or…essential to the achievement of better outcomes…while remaining sensitive to the point at which the lack of formality and transparency induce inefficiencies…and turns informal governance from a solution into a problem' (2013, p.1202). In relation to cybercrime, important questions relate to whether: a) the governance emergent in EC3 and specifically the modes visible in J-CAT with regard to operational governance, have aided in addressing the challenge of cybercrime more effectively; b) Such modes are underpinned by the necessary safeguards for the protection of the fundamental (privacy and data protection) rights of individuals; c) Procedures, functions and working practices are transparent, adequate and subject to robust oversight mechanisms to ensure accountability.

Finally, we need to conceptually open up the possibility that informal cooperative governance arrangements are fluid, and can often terminate once a threat has been dealt with, or morph, if successful, transferable and scalable, into more formal, institutionalised, arrangements around particular issues. So, what does this movement from networked organisation to more formal institutional arrangement imply conceptually? Mueller (2010, p46), argues that it implies regular interaction of the actors involved in any networked arrangement, and those actors accepting and understanding rules, norms and conventions for their interaction, and how they can be enforced. Moreover, such mutual agreement on action also brings collective benefits and effective outcomes, with further negotiation on such benefits often moving networked arrangements to more formal, binding forms of institutionalisation. To elaborate further, once the collective benefits of a networked organisational form become more obvious, it can lead to further deliberation and contestation within the network on issues relating to binding rules, procedures, or issues such as how to (re) define its boundaries (who should be included/excluded), future resource and control and, regulation of the network organisation.

To this end, it is important to note that the creation of a network organisation and the movement to institutionalisation can be driven by a variety of factors and indeed actors internal to but also external to the issue area at hand. In the case of J-CAT, the aim here is to chart an understanding of its evolving features through the conceptual literature on informal and formal governance. This is not to argue that J-CAT is informal *per se* – indeed it was an initiative driven by transgovernmental actors within the cybercrime network - but that many of the features and day-to-day practices and interactions within J-CAT are reflective of informal modes and functions, with a recognition that it is located within a broader formalised environment. J-CAT, therefore, is being considered as a novel network organisation that complements a pre-existing institutional environment (EC3/Europol, EU). Having demonstrated operational benefits since its formation, J-CAT, it can be argued, has become permanently embedded in the pre-existing environment, and faces issues of how to evolve and define its boundaries going forward. The next section provides an overview of the broader formal EU cybercrime environment to provide a context for understanding the emergence of J-CAT within the EC3.

The European Union's Formal Cybercrime Policy Milieu

The EU approach towards cybercrime has developed in parallel to its information society strategies such as, for instance, the White Paper on Growth, Competitiveness and Employment (1993) which referenced the completion of the e-common market and the *e*Europe initiative (1999) for enhancing the use and enjoying the benefits of digital technologies in a socially inclusive way. As the EU's aspirations to become an information society have progressed, so too have its efforts to protect those emerging benefits from criminal activity. The EU's approach has also been driven by EU internal security documents and Justice and Home Affairs programmes (e.g. Internal Security Strategy, 2010 and Stockholm programme, 2010-14), as well as the European Agenda on Security (European Commission 2015b) and the Joint Framework on Countering Hybrid Threats (European Commission and EEAS 2016) which have provided strategic guidance on cybersecurity and *cybercrime*. The EAS defines the latter as a priority area - and cybersecurity is an essential component of the European Commission Communication on achieving an effective and genuine Security Union (see European Commission, 2016c).

Externally the European Convention on Cybercrime (Council of Europe 2001) has been a central reference point for the development of EU policy[1] and a catalyst for the construction of the EU Council Framework decision on attacks against information systems (Council of the EU 2005); the latter was updated and replaced by the Directive of the same name in 2013 (EU Parliament and Council 2013; for details see Christou 2016). However, it was not until 2007, and the European Commission's Communication (2007) 'Towards a general policy on the fight against cybercrime' that a dedicated policy began to emerge. Prior to this the fight against cybercrime featured in various Communications on Information Security and computer-related crime (European Commission 2001a, 2001b), as well as Directives and Framework decisions, for example, on attacks against information systems (European Commission 2005) but also child sexual exploitation (European Parliament and Council 2004) and Combating the Sexual Abuse and Sexual Exploitation of Children (European Parliament and Council 2011).

The EU also developed its 'Strategy for a Secure Information Society' which aimed to 'develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment' (European Commission 2006, p.3). Furthermore, there was significant overlap between the EU's policy towards protecting critical infrastructure and initiatives and measures to deal with cybercrime. Indeed, the EU's Directive on Network and Information Security (European Parliament and Council 2016a), agreed in December 2015, which accompanied the CSSEU, proved controversial through mandating an obligation to report data breaches (cybercrime and significant security incidents) across *all* infrastructure sectors and operators of essential services, including digital service providers (see European Commission 2015). Finally, the EU's policy frameworks related to issues such as terrorism, organised crime and virtual currencies also have significant governance implications for cybercrime, in particular given that many non-legislative measures are developed in informal, often secretive fora such as, for instance, the EU Internal Referral Unit (EU IRU) or the Standing Committee on Operational Cooperation (COSI) (European Parliament 2015, p.35-37).

The 2007 Communication sought to improve cooperation and coordination at an operational and strategic level among law enforcement agencies, and at a political level among Member

States of the EU. In addition, it promoted cooperation with third countries, and put a specific emphasis on continuous learning - through articulation of training needs in relation to cybercrime issues for law enforcement and judicial authorities, and increased linkage and commonality between the training programmes of the authorities involved in order to achieve better coordination. Furthermore, and given the important role of the private sector in any effective cybercrime solutions, the improvement of the public-private aspect of the Commission's cybercrime policy through enhanced mechanisms of dialogue was emphasised. Various partnerships and non-legislative measures were subsequently developed, such as, for example, the collaboration between law enforcement agencies and credit card companies that allowed the effective tracking of persons purchasing child pornography online, as well as the development of a common EU blacklist of child sexual exploitation material (European Parliament 2015, p.28). Despite this, however, the challenge was to improve operational cooperation in Europe given the lack of legal obligation for private companies to share information on cybercrime with public authorities.

Integral to improving cross-sectoral exchange of information was also the EU's rules on data privacy, retention and protection of personal data. Indeed, the EU's legal instruments – the E-Privacy Directive (European Parliament and Council 2002, amended 2009; see also European Commission proposal 2017) and the Data Retention Directive (European Parliament and Council 2006) - have proved controversial – sitting at the centre of the tension between data protection and privacy more broadly and the operational requirement for access to data to combat cybercrime. Within the latter Directive, which was annulled by the European Court of Justice in 2014, there was a requirement for all Member States to put legislation in place that ensured Internet Service Providers (ISPs) and telecommunications companies maintained records on user traffic (connections not content) for between 6 months and two years. Thus, although this was established practice for companies in the electronic communications sector, it was not the case for ISPs. From a law enforcement perspective, such a Directive would aid access to critical data for operational purposes. From a digital rights perspective, the Directive increased the prospect of data misuse, was not transparent in its use of data, fostered a surveillance society mentality, and undermined fundamental rights. Indeed, the European Data Protection Supervisor (EDPS) argued in its evaluation of the

Directive that it would be illegal under the EU Charter of Fundamental Rights constituted by the Lisbon Treaty (Rodriguez, 2011).

Fears among the European public over privacy and data protection (Special Eurobarometer 2011; Data Protection Eurobarometer 2015) and the Snowden revelations (2013) prompted a comprehensive review and reform of the data protection legal framework in the EU, underpinned since 1995 by the Data Protection Directive (European Parliament and Council Directive 1995[2]). This took the form of a Regulation (General EU Framework for Data Protection) and Directive (on protection of personal data related to criminal and judicial matters), proposed in 2012. This new legal framework – adopted in April 2016 and to take effect May 2018 (European Parliament and Council 2016b) - seeks to resolve the tension between privacy/rights and security through injecting further legal clarity, in particular in relation to the processing of personal data in criminal investigations, including cybercrime. Indeed, this and the E-Privacy Directive also sought to ensure the confidentiality of communications and to prevent the unauthorised access to customer data. However, even though the Data Retention Directive was declared invalid by the European Court of Justice (ECJ) in April 2014 on the grounds that it represented an infringement on the individual's right to privacy and protection of data, it is effectively embedded and still enforced in many EU Member States (e.g. the UK Investigatory Powers Act; see also De Zan and Autolitano 2016). The effect, together with other EU procedural law, is to 'impose additional obligations on private actors who restrict the right to privacy of their customers on law enforcement grounds' (European Parliament 2015, p.26; European Parliament and Council 2014).

The EU's formal cybercrime policy is underpinned by a comprehensive but not altogether, coherent body of substantial and procedural law. Europol and the EC3 located within it – the latter in particular established to be able to respond more effectively to the challenges of cybercrime (European Commission 2012) - operate under a separate legal framework for data protection related specifically to police and judicial cooperation in criminal matters (Drewer and Ellermann 2012[3]), as well as the principles of Council of Europe Convention 108[4] and Recommendation No R (87) 15[5][6]. Moreover, agencies such as Europol – as will be alluded to below – have internal review mechanisms in place that ensure operational practices in EC3/J-CAT adhere to and comply with the Europol mandate and the EU legal framework. For some though, such governance practices raise questions of legitimacy and accountability (and call for a greater role for the EP in this), as well as of how existing laws, such as those on law enforcement access and use of data are regulated by effective oversight mechanisms (European Parliament 2015, p.26).

Agencies and the Fight Against Cybercrime in the EU: Europol and the emergence of EC3 and J-CAT

Further to the above formal legal milieu, institutionally, Europol had been involved in cybercrime matters since 2000, and had established a high-tech crime centre in 2007, renaming it the Europol European Cybercrime Centre in 2012. The formal establishment of EC3 in January 2013, a key priority in the EU's Internal Security Strategy (Council of the European Union 2010a), meant that Europol took a dedicated role through an additional resource to fight cybercrime. Its main role was to help protect European business, governments and citizens through enhancing law enforcement capability in cybercrime. Its function was to facilitate existing activities related to cybercrime, but importantly, given the asymmetry in skills and capabilities within European countries, to extend operational and analytical support to Member States. Beyond this, EC3 was also expected to provide such support for investigations and cooperation with international partners given that much cybercrime within Europe is instigated from outside its borders. New functions were also established for EC3 which focused on three broad areas: Cybercrimes committed by organised crime groups, particularly those generating large criminal profits, such as online fraud; cybercrimes which cause serious harm to their victims, such as online child sexual exploitation; finally, cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union (European Cybercrime Centre, 2014 p.2)

To this end, EC3 was conceived as the European focal point for the fight against cybercrime. Consisting of three divisions – Operations, Strategy and Forensics (see European Cybercrime Centre, 2014a) – it was a central node within the EU that would facilitate the effective coordination of member state investigations in cybercrime. In addition, EC3 was tasked with ensuring that operational activities align with relevant EU policy, and with coordinating and collaborating with other relevant EU agencies such as Eurojust, the European Network and Information Security Agency (ENISA) and the European Union Agency for Law Enforcement Training (CEPOL) in order to ensure that the priority areas identified under the formally agreed 2013-2017 EU policy cycle (specifically the EMPACT priorities, which are part of this) - training, capacity-building, outreach, strategic analysis and technical support - are addressed effectively (European Cybercrime Centre, 2014a). The EMPACT priorities were created by the Council of the EU in 2010 to 'tackle the most important criminal threats in a coherent and methodological manner through optimum cooperation between the relevant services of the Member States, EU Institutions and EU Agencies, as well as relevant third countries and organisations' (Table on the Implementation of the CSSEU 2014, p.9). Such threats are identified by the Europol Serious and Organised Crime Assessment (SOCTA 2017; see also iOCTA 2016). In its 2017 report (SOCTA 2017), for example, malware and ID theft, cryptoware, network attacks, payment order and card fraud, and online child sexual exploitation, were identified as primary threats. Strategic goals are agreed on the basis of the identified threats by Member States and other relevant stakeholders and form the basis of the EC3's priorities and actions (Ibid, 10).

Examples abound in the European Cybercrime Centre First Year Report (2014; see also Joint Cybercrime Task Force 2017) on how cooperative arrangements have brought operational success. For example, the EC3 operation to takedown the ZeroAccess botnet, it is argued, demonstrated how cooperation can work in a cross-jurisdictional operation that incorporates public and private sector actors. Important in this, it is asserted, is being able to move as swiftly as the cybercriminal but also engaging in partnership with the relevant stakeholders to disrupt a cybercriminal network; the partnership between EC3 and Microsoft identified as particularly important in this case (Ibid, p.13). Another example is that of taking action to combat the Shylock Trojan, where the UK National Crime Agency (NCA) brought together partners which included the FBI, Europol, BAE Systems Applied Intelligence, GCHQ, Dell Secure Networks, Kaspersky Lab and the German Federal police. The investigation was conducted from the operational centre at EC3 and, it was reported, allowed effective cooperation between cyber investigators, coordinated by the NCA and supported by the necessary organisational country partners involved. Conceptually, we could see such EC3 operational networks of experts – public and private – being brought together by the UK NCA – to collaborate on a specific cybercrime case in real-time – and indeed, this provided the foundation for J-CAT's unique model for operational governance that is analysed below.

The Joint Cybercrime Action Taskforce

Given the above formal environment, a key question in this article is how far operational governance mechanisms such as J-CAT can be characterised in relation to the EU's legal and institutional cybercrime milieu. Why was J-CAT needed and how can it be understood conceptually in terms of the relationship between formal and informal and the form of networked governance that has emerged? The borderless nature of cybercrime brought forth challenges in relation to traditional, territorially fixed, legal frameworks that were constructed for physical crime, where typically criminals can only commit one offence at a time. After the first year of EC3 operations three key issues were evident that suggested new and more flexible governance arrangements would be needed to allow law enforcement to more effectively address the challenges of cybercrime – that is, and as alluded to by one former senior EC3 official, to provide tools appropriate for fighting crime in the 21st Century (Interview, anonymous, EC3 September 2014).

The establishment of J-CAT in September 2014, initially as a six-month pilot initiative, emanated from the emergence of such issues and frustration 'after a decade of ad-hoc bilateral cooperation within the framework of regional and international police operation structures' (Reitano et al 2015, p.143). The first issue was the cross-border nature of the cases being handled – that is, there would be at least three or four countries involved, not all of which had direct operational cooperation agreements with Europol; so it became obvious that an international approach would be required to be able to have a global cooperation and implementation reach. Second, whilst individual countries already had established cybercrime units, as one J-CAT member noted 'we were finding that most of the cybercrime investigations we were dealing with had cross-border or cross-country angles…that some of the legal processes were laborious…and that there were multiple investigations in different countries looking at the same individuals or groups…so each country was putting in their own resource for looking at the same groups of people' (Interviews, anonymous, J-CAT 2016). The implication here was that pooling resource would be much more effective and efficient. The third issue was the increased global connectivity between different cases that were previously, seemingly unconnected – across, for example, infrastructure, finance, and money laundering cases – making it necessary to develop mechanisms for global synergy and joint action, capability and execution. The final issue was related to electronic evidence – trans-border access, the connectivity of the evidence, the speed at which evidence was collected and used, and the need to exchange information not only on an intelligence basis but also evidential basis so that it could be subsequently used for court proceedings (Interviews, anonymous, J-CAT 2016).

It is argued here that the way in which J-CAT was established imbues it with modes of informality – and emergent features of a network organisation, even though still complementary to and embedded in EU formal agencies and policies. One of the reasons for its establishment as a Taskforce rather than as a Europol Target Group or Analysis Project was to provide law enforcement with the necessary flexibility to react quickly in the dynamic cybercrime environment – and to circumvent the impediments created by formal legislative and bureaucratic procedures (Reitano et al 2015, p.145; Interviews, anonymous, J-CAT 2016).

To this end, it brought together public actors in the form of cyber liaison officers from (resource able) committed EU Member States (UK, France, Germany, Spain, Italy, the Netherlands, and Austria), non-EU state partners (Australia, Canada, and Columbia)[7], US law enforcement agencies (FBI ad Secret Service) and the EC3[8]. It also cooperates and consults with a plethora of other public and private actors and networks that can support and provide intelligence in relation to combating cyber criminality – and such actors and networks can also initiate J-CAT investigations (Interviews, anonymous, J-CAT 2016). Indeed, it is the latter that differentiates it from a simple transgovernmental network, as it brings together in one single physical, co-located space, 'a variety of experts … to better fight cybercrime and to improve the network of existing partnerships' (Meywirth 2016). It is thus a network form of organisation consciously designed in a specific mode in order to meet the objectives of combating cybercrime effectively.

Beyond this, it is important to understand how those within the J-CAT are able to act as agents of informal governance. What are the mechanisms and conditions through which this happens? How can we further explain the difference between how J-CAT is operationally different to Europol/EC3 in order to better comprehend the informal aspects that allows it to act with more speed and flexibility.

The first feature is the single, co-located space within which agents work – thus, cyber liaison officers, instead of being in separate national units – are able to communicate, interact, and discuss different aspects of cases informally, on a daily basis. This has several benefits in terms of socialisation and building trust between J-CAT partners; trust, in turn, is crucial condition and ingredient for members' inclination to share intelligence and the ability of law enforcement officials to undertake effective investigations (Reitano et al 2015, p150). On a practical level, the very fact that cyber liaison officers sit together in a single space, allows real-time communication, information and intelligence sharing – the latter through a coded system organised around the sensitivity of data (Ibid, p151) - when a problem arises. This, rather than having to move through the traditional system where national law enforcement agencies had to make formal requests for information, wait for responses to decide whether there were matching leads, and where ultimately, it took upwards of six to seven weeks for any action to be taken. From a law enforcement perspective, given the dynamic nature of cybercrime (e.g. servers being investigated could be taken down in a day), this process was too slow and laborious (Interviews, anonymous, J-CAT 2016).

This does not imply that Mutual Legal Assistance Treaties (MLAT's) – even though problematic from a law enforcement perspective (for arguments to the contrary see Carrera et al 2014, pp65-72), could be bypassed when it came to sharing and using evidence, but rather that, 'law enforcement authorities and providers have struck agreements or informal arrangements…to exchange e-evidence' (De Zan and Autolitano 2016, p11). In the words of one official, 'evidentially…we cannot get away from MLATs and international Letters of Request (LoR). However, what we can do is speed those processes up by already having the contacts in those countries and knowing where to send it…whereas previously, it would go through central authorities it would sit on peoples' desks for weeks on end not knowing where to send it' (Interviews, anonymous, J-CAT 2016).

Second, although J-CAT is a network organisation that operates within established institutional bounds – it also has its own *ad hoc* procedures in place that allow it to act quickly, should cases arise outside of formally established meetings between relevant actors within J-CAT, EC3 and Europol. For example, there are formal meetings between the Heads of all EU Member State Cybercrime Units (EUCTF) bi-annually to discuss trends, threats, J-CAT, as well as strategic direction and other relevant developments. Operationally, however, if there are urgent cases that need J-CAT attention, they do not need to wait for such formal meeting points. Indeed, national cybercrime units can contact cyber liaison officers directly for them to assess and potentially investigate cases. Thus, another informal feature of J-CAT is the flexibility to consider, assess and act upon, if agreed by its members and the J-CAT Board[9], urgent cases – that can be brought to them by public or private actors and networks at any given point in time. Moreover, cyber liaison officers have the autonomy to take a decision to investigate a case, without waiting for formal approval from the Board. This, again, is due to the trust placed in cyber liaison officers as experts that are able to exercise their judgement and make the right decisions – an important code of practice that ensures they are able to be proactive rather than reactive in any operational investigation (Interviews, anonymous, J-CAT 2016).

Third, the J-CAT governance framework enabled it, as a taskforce, to work more effectively with non-Member States. Because of the borderless and international nature of cybercrime, quite often criminals are located in countries outside the EU. Countries with whom J-CAT would need to cooperate to secure information and ensure prosecutions – did not have operational cooperation agreements with Europol because of, typically, human rights or data protection concerns at the EU level. This limited joint operational collaboration and action. Thus, prior to the European Union Agency for Law Enforcement Cooperation Regulation (European Parliament and Council 2016c)[10], Europol was not able to exchange operational data with such non-members, instead facing a myriad of legal obstacles in cooperating to pursue cybercrime investigations. However, 'because J-CAT is an independent Member States' initiative, it is able to work with…other non-Member States through ad-hoc proxy agreements' (Reitano et al 2015, p.145). That is, whenever pursuing cases with non-members, a Member State could be designated by J-CAT to act as proxy and liaise with Russian law enforcement in order to investigate and prosecute cybercriminals (Ibid).

This is important for our understanding of the evolution of J-CAT and the relationship between the informal and formal aspects. Indeed, this provides a good example of how such informal practice can lead to complementary legal institutionalisation to improve the efficacy of operational process. The European Union Agency for Law Enforcement Cooperation Regulation (European Parliament and Council 2016c) opened up 'a lot how we can cooperate with external parties with whom we could not sign an operational cooperation agreement…' (Interviews, anonymous, J-CAT 2016). Whilst it did not allow Europol to sign an operational agreement with external parties, it would allow them – and thus J-CAT - to exchange operational data on a bilateral basis without such an agreement – with this being regulated directly by the European Commission in line with EU requirements related to data access, protection, security, use and exchange. This, in the opinion of one J-CAT official 'would simplify the work…and the whole lengthy procedure of bureaucracy which would allow us to work and establish partnerships with those countries, faster' (Interviews, anonymous, J-CAT 2016).

In line with the conceptual aspects of a networked organisation J-CAT, whilst having a great deal of operational flexibility and its own procedural system of governance and working norms, also retains organisational features through its embeddedness within EC3 in relation to budget (resource), support and outreach. Its status has a permanent taskforce has also been endorsed by the Europol Management Board. Furthermore, the collective benefits of J-CAT through its operational success (Reitano 2015, p.146-8) as a networked organisational form, has led to an extension of its initial mandate (Europol, 2015a, 2015b, 2015c). J-CAT has received praise for pro-actively leading intelligence-led coordinated actions against key cybercrime threats and top targets thus providing a mode of governance that should be emulated and resourced. This has further led to deliberation on evolving informal norms, binding rules and procedures and importantly, on (re) defining its boundaries and the broader formal regulatory environment within which it operates (e.g. European Council and Council of the EU 2016, European Parliament and Council 2016c). Conceptually then, J-CAT is a fluid network organisation, 'an evolving platform' in the words of one official (Interviews, anonymous, J-CAT 2016), with discussions ongoing on how far such a model can and should be scaled up. To this end, membership eligibility criteria have already been defined for any new members that wish to join the J-CAT network – with the J-CAT Board able to define further specific criteria for participation if necessary (Ibid). One key issue in expanding membership is maintaining its novel features but also ensuring that any new additions to the J-CAT team bring added operational value. A second issue is of ensuring that trust and therefore members' willingness to share information is not lost through scaling up in relation to members[11].

Finally, if we refer back to Christiansen et al's (2003) dimensions when considering informal governance arrangements, several issues arise relating to the politics of operational governance found within the J-CAT model. The first is the issue of the effectiveness of informal governance arrangements. It is clear in the case of cybercrime governance that the informal modes within J-CAT have facilitated the move to more efficient and effective mechanisms and conditions for addressing the challenges of cybercrime – that is, the policy problem related to crime in cyberspace which formal modes, on their own, have not been able to do. Thus, such informal modes have provided more innovative and alternative ways of identifying and executing cybercrime investigations that have overcome some of the problems with working through older, traditional, nationally based bilateral methods and bureaucratic procedures. The J-CAT has clearly been convergent and complementary to existing formal legislation and has sort to work within existing, evolving formal legislation to provide alternatives modes of doing cybercrime investigation.

The second relates to the degree of political accountability relating to the everyday activities of fora such as J-CAT and the *ad hoc* networks brought together to take down botnets, for example. Moreover, whilst there is some accountability related to the EP's right to call a representative of Europol to respond to questions, it is utilised infrequently and is not extended to members of J-CAT. The European Parliament can invite members of J-CAT (e.g. national cyber liaison officers) but it would not be mandatory for them to attend. Indeed, it would be the decision of the relevant national government on whether its own representatives should attend even if requested. In addition, although J-CAT members are nationally seconded, scrutiny is undertaken by Europol and the EC3[12]. Whilst this ensures J-CAT adherence to their legal frameworks and mandate, it has, nevertheless, led some commentators to argue that, 'further information should be requested on the operational aspects of J-CAT, such as detailed mapping of the liaison officers, their affiliations and respective roles, as well as the forms of coordination and cooperation they carry out' (European Parliament 2015, p55). This, they argue, would further improve transparency.

A third and final issue relates to legal accountability and the extent to which informal operational governance modes facilitate access to relevant evidential data within the established EU legal frameworks (European Parliament and Council 2016c) and indeed established bilateral legal agreements such as MLATs. Concerns have been raised more broadly, for instance, regarding third country access to data outside MLAT agreements, and the extent to which fundamental rights to data protection are circumvented in such actions within the operational environment through more informal arrangements (De Zan and Autolitano 2016, p12). According to the 2016 Europol Regulation, 'Any information which has clearly been obtained in obvious violation of human rights should not be processed'

(European Parliament and Council 2016c, p.6), and whilst there are no doubt innovative informal modes are utilised within J-CAT, these do not circumvent the MLAT or Letters of Request procedures, but rather involve, given the informal working features of J-CAT, more effective day-to-day processes of identification and familiarity with differing national legal systems and what is possible within and between them in terms of sharing and using evidence in cybercrime prosecutions (Interviews, anonymous, J-CAT 2016; see also, European Parliament 2015, p.50).

Although the entry into force of the European Investigative Order Directive (EIO) in May 2017 (European Parliament and Council 2014) will simplify matters (but not eliminate all problems) in relation to evidence sharing within EU countries whilst also providing clear limits in relation to cooperation on human rights and proportionality grounds (similarly the EU-US Umbrella Agreement will ensure EU citizens rights in law enforcement cooperation[13]), issues of uncertainty, legitimacy and effectiveness will still remain because of the lack of a single, common international convention governing e-evidence sharing and use in relation to cybercrime (see De Zan and Autolitano 2016, p78-90). That is, the problem of international asymmetry will still remain. Furthermore, there are issues related to the fragmentation of the EU data retention regime following decision by the ECJ to invalidate the Data Retention Directive (2006) in terms of the potential negative effects of this on cross-border police and judicial cooperation. A balance here must be found between allowing retention for criminal investigation purposes and ensuring the rights of EU citizens.

Conclusion

This article has sought to characterise J-CAT as an emergent and evolving operational form of governance to address the challenges of cybercrime. To this end, it has shown that J-CAT modes and functions are reflective of *informal practice* within the bounds of the EC3/Europol governance framework, as well as the broader EU legal framework on cybercrime. It has been shown that the way in which it was established reflected a *conscious move* to avoid the obstacles present in traditional – often slow and bureaucratic - governance arrangements for cybercrime. That is, the J-CAT network organisation was deliberately constructed to allow for greater flexibility through establishing conditions – for example, the single co-habited space, day-to-day flexibility to assess cases outside formal meeting points, restricted membership to create the trust necessary for information sharing – that would lead to more novel and effective investigation of cybercrime.

Conceptually, J-CAT can be seen as convergent and complementary – in that the practices within J-CAT have been reinforced by, rather than developed in opposition to formal EU legal frameworks for combating cybercrime. Moreover, the success of J-CAT in its network organisational form, has raise questions of how J-CAT should evolve and indeed expand further whilst still ensuring the conditions that have led to its effectiveness are maintained. To this end, J-CAT Terms of Reference have been written and clear eligibility criteria have been constructed based on ensuring that any additional members will be able to contribute in terms of resource and expertise. Important, also, is that they will be able to operate within the ethos of J-CAT (Interviews, anonymous, J-CAT 2016). As J-CAT has evolved as an organisational network, so too have understandings of rules, norms and conventions for actor behaviour, process and interaction, and how they can be implemented.

Questions have also been raised in relation to the transparency and accountability of J-CAT, which whilst present can further be improved through, for example, making more public, information on J-CAT membership and function, as well as also making mandatory the attendance of J-CAT members to respond to questions if called upon by the EP. In terms of the protection of data protection and privacy rights in J-CAT operations, whilst novel modes have been employed to speed up evidence sharing processes, such modes have been employed within the international and EU legal frameworks that exist. Indeed, they have been reinforced by the latter through, for example, the EIO Directive and the European Union Agency for Law Enforcement Cooperation Regulation, as well as specific bilateral agreements such as the Umbrella Agreement between the EU and US which ensures more effective (right-based) legal protection in relation to the governance of information and evidence exchange in cybercrime cooperation.

Finally, whilst J-CAT as a model for operational cybercrime has resulted in better outcomes, broader issues do remain for the more effective combating of cybercrime going forward – in particular stemming from asymmetry in legal frameworks at the intra-EU and international levels. For example, since the Data Retention Directive was annulled by the ECJ, there is no longer EU-wide legislation on data retention and obtaining evidence from private parties. This situation is further exacerbated by the fact that certain Member States have, despite the ECJ judgement, retained legislation in this area, whilst others have not, causing uncertainty on the rules for obtaining data from private parties in cybercrime investigations. Related to this, is the asymmetry between states – within and outside the EU - in the transposition of existing international legislative instruments. This causes problems, in particular in relation to the expedited sharing of evidence in cybercrime, as no common legal framework exists (in contrast to the preservation of evidence, where it does).

Furthermore, and related to international cooperation is the issue of collecting and sharing international evidence in a time-sensitive way – there is a need to reform the MLAT system, in this sense, whilst ensuring that all relevant legal frameworks of requesting countries are adhered to. Finally, there are also issues relating to tensions between legal frameworks and effective trust-based cooperation – and indeed specifically, the lack of consensus on how far formal, legal frameworks can facilitate effective collaboration with the private sector (Europol and Eurojust 2016). Any long term (formal) solutions to such challenges - for which J-CAT has provided some novel practices – will need to ensure the right balance between security, speed and efficiency and civil liberties in terms of the right to privacy, data protection and free speech. Moreover, such challenges will pose problems for the evolving relationship between the formal environment and the informal practices that have thus far emerged to provide responses to these challenges. J-CAT, in this sense, is networked organisation that sits at the centre of wider international web of networks, institutions and legal frameworks; the issue going forward is how such forms of more flexible governance can evolve and continue to secure better outcomes in cybercrime whilst ensuring that the conditions that allow it to be more effective are sustained and further developed in European and international spaces.

Notes

[1] Previous to this the Council of Europe Conference on Criminological aspects of Economic Crime (1976) was also very important in defining computer crime and its various forms.

[2] Complemented by specific rules concerning police and judicial cooperation through instruments such as the 2008 Framework decision (Directive 2008/977/JHA)

[3] See also https://www.europol.europa.eu/st/DPO/#/the_legal_framework

[4] Convention on the Protection of Individuals with regards to automatic processing of personal data

[5] Of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted in 17 September 1987.

[6] Whilst these have been in part, superseded by EU substantive law relating to cybercrime that provide for more effective protection of data, criticism still exists of Council of Europe efforts to extend and strengthen rules on law enforcement access to data stored extraterritorially. The implications if this are twofold: a) that it could undermine EU law on privacy and data protection b) that the Convention could facilitate a global framework for surveillance through the backdoor (see European Parliament 2015, p28).

[7] With which Europol has an operational cooperation agreement.

[8] EC3 provides J-CAT permanent secretariat services as well as operational and technical support on daily basis. It is also responsible for daily operational coordination.

[9] The EUCTF consists of the Heads of the EU Member State Cybercrime Units, while the J-CAT Board is represented by the Heads of the Cyber Units of the J-CAT member countries only. The former meets twice per year. The latter, from 2-4 times depending on need.

[10] Under this Regulation, which entered into force in May 2017, there will no longer exist cooperation agreements but adequacy decisions and there will be no restrictive list of countries that Europol can cooperate with, so theoretically it is possible to sign one in the future with any country as long as they cover the EU criteria.

[11] INTERPOL's Digital Crime Centre, for example, whilst having similar features to J-CAT, has a much broader membership open to all 190 INTERPOL member states. This has made it more difficult to find a framework through which members can directly share information (Reitano 2015, p152).

[12] See, for example: https://www.europol.europa.eu/about-europol/accountability and https://www.europol.europa.eu/about-europol/transparency

[13] The EU and US signed the 'Umbrella agreement' in June 2016 which put in place a comprehensive high-level data protection framework for criminal law enforcement cooperation. The agreement improves the rights of EU citizens by providing equal treatment with US citizens when it comes to judicial redress rights before US courts (European Council and Council of the European Union 2016)

References

Bache, I., and Flinders, M. (eds) (2005) Multi-level Governance, (Oxford: Oxford University Press)

Busuioc, M. (2013) European Agencies: Law and Practices of Accountability, (Oxford: Oxford University Press)

Busuioc, M., Curtin, D. and Groenleer, M. (2011), 'Agency growth between autonomy and accountability: The European Police Office as a 'living institution', Journal of European Public Policy, 18(6): p.842-867

Bevir, M. (2012) Governance: A Very Short Introduction, (Oxford: Oxford University Press)

Carrapiço, H. and Trauner, F. (2013), 'Europol and its influence on EU policy-making on Organized Crime: Analyzing Governance Dynamics and Opportunities', *Perspectives on European Politics and Society*, Special Issue, 14 (3), p.357-371.

Carrera, S., González Fuster, G., Guild, E., and Mitsilega, V. (2015), 'Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights', (Brussels: Centre for European Studies)

Christiansen, T. and Neuhold, C. (2013), 'Informal Politics in the EU', *Journal of Common Market Studies*, 51 (6), pp.1196-1206

Christiansen, T. and Neuhold, C. (eds) (2012), International Handbook on Informal Governance, (Cheltenham, UK: Edward Elgar)

Christiansen, T. and Piattoni, S. (2003), Informal Governance in the European Union, (Cheltenham, UK: Edward Elgar)

Christiansen, T., Follesdal, and Piattoni, S. (2003) 'Informal Governance in the European Union: an Introduction', in Christiansen, T. and Piattoni, S. (2003), *Informal Governance in the European Union*, (Cheltenham, UK: Edward Elgar)

Christou, G. (2016), *Cybersecurity in the Europe Union: Resilience and Adaptability in Governance Policy*, New Security Challenges Series, (Basingstoke: Palgrave Macmillan)

Council of Europe (2001), Convention on Cybercrime, CETS No.185: Budapest, 23 November 2001

Council of the European Union (2016). Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the EU's Foreign and Security Policy. Brussels. Available at: http://europa.eu/globalstrategy/en (accessed 23 March 2017).

Council of the European Union (2010a) Internal Security Strategy for the European Union: Towards a European security model, March 2010. Available at: https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf (accessed 23 March 2017).

Council of the European Union (2010b) The Stockholm Programme – An open and secure Europe serving and protecting citizens [Official Journal C 115 of 4.5.2010]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:jl0034 (accessed 23 March 2017).

Council of the European Union (2005) Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Council of the European Union (2004) Council Framework Decision 2004/68/ JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography

Council of the European Union (2003) Secure Europe in a Better World: European Security Strategy, Brussels, 12 December 2003

Council of the European Union (1997) 'Action Plan to Combat Organised Crime'. Official Journal of the European Communities. 15 August 1997. No C 251/1.

Data Protection Eurobarometer (2015), 24 June 2015. Available at: http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm (accessed October 2016)

De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Istituto Afaari Internazionali, Document 16/17, November 2016.

Drewer, D. and Ellermann, J. (2012) 'Europol's data protection framework as an asset in the fight against cybercrime', Europol, 19 November 2012. Available at: https://www.europol.europa.eu/content/publication/europols-data-protection-framework-asset-fight-against-cybercrime-1838 (accessed November 2016)

Eberlein. B. (2003), 'Formal and Informal Governance in the Single Market Regulation', in Christiansen, T. and Piattoni, S. (2003), Informal Governance in the European Union, (Cheltenham, UK: Edward Elgar)

Eising, R, Kohler-Koch, B. (eds) (1999), The Transformation of Governance in the European Union, Routledge: London

ENISA Threat Landscape Report (2016). Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (accessed June 2017)

European Commission (2017), Proposal for a Regulation of the European Parliament and of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017, COM (2017) 10 final

European Commission (2015a). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

European Commission (2015b) Communication from the Commission to the Council and the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, The Agenda on European Security, Strasbourg, 28.4.2015, COM(2015) 185 final

European Commission (2015c) 'Commission welcomes agreement to make EU online environment more secure', Press Release, Brussels, 8 December 2015. Available at: http://europa.eu/rapid/press-release_IP-15-6270_en.htm (accessed May 2017)

European Commission (2013a), Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union, Brussels 7.2.13, COM(2013) 48 final.

European Commission (2013b), Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, Brussels, 27.3.13, COM (2013) 173 final, 2013/0091 (COD)

European Commission (2012), Communication from the Commission to the Council and the European Parliament, 'Tackling Cybercrime in our Digital Age: Establishing a European Cybercrime Centre', COM (2012) 140 final, Brussels, 28 March 2012

European Commission (2010a), 'Europe 2020: A strategy for smart, sustainable and inclusive growth', European Commission, COM (2010) 2020, 3 March 2010

European Commission, (2010b), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A Digital Agenda for Europe', COM (2010) 245 final/2 26 August 2010

European Commission Communication (2007), 'Towards a general policy on the fight against cyber crime', Press Release, MEMO/07/199, Brussels, 22 May 2007. Available at: file:///C:/Users/George/Downloads/MEMO-07-199_EN.pdf (accessed June 2017)

European Commission (2001a) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Network and Information Security: Proposal for A European Policy Approach, COM(2001)298 final, Brussels, 6.6.2001.

European Commission (2001b) 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-related Crime', COM (2000) 890, 26 January 2001.

European Council and Council of the European Union (2016), 'Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign "Umbrella agreement"'. Available at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/02-umbrella-agreement/ (accessed July 2016)

European Commission and European External Action Service (EEAS) (2016). Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: A European Union response. 6 April, JOIN(2016) 18 final.

European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013, JOIN(2013) 1 final

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy / Vice-President of the Commission (2013). Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace, Brussels, 7 February, JOIN (2013) 1 FINAL.

European Court of Justice (2014), Judgement of the Court (Grand Chamber), Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, 8 April 2014. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322)

European Cybercrime Centre (2014), First Year Report, Europol, 2014, http://www.europol.org (accessed April 2017)

European Cybercrime Centre (2014a), Combating Crime in a Digital Age, Europol https://www.europol.europa.eu/ec3 (accessed June 2017)

European Parliament and Council (2016a), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

European Parliament and Council (2016b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016/L 119/1.

European Parliament and Council (2016c), Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions

2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479897160399&uri=CELEX%3A32016R0794 (accessed April 2017)

European Parliament and Council (2014), Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Official Journal of the European Union, L130/1, 1.5.14.

European Parliament and Council (2013), Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

European Parliament and Council (2011) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework Decision 2004/68/JHA.

European Parliament and Council (2009) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

European Parliament and Council (2008) Directive 2008/114/EC of 8 December 2008 of the European Parliament and of the Council on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection

European Parliament and Council (2006) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (annulled by ECJ in Case number C-293/12, 8 April 2014)

European Parliament and Council (2004) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

European Parliament and Council (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002.

European Parliament and Council (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Parliament and Council (2011), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework Decision 2004/68/JHA.

European Parliament and Council (2014), Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

European Parliament (2015) *The Law Enforcement Challenges of Cybercrime: Are we Really Playing Catch-up?* Technical Report, Directorate-General for Internal Policies, Policy Department C: Citizens’ Rights and Constitutional Affairs, Study for the LIBE Committee, October 2015.

Europol (2015a), ‘Botnet Taken Down through Internal Law Enforcement Cooperation’, press release, 25 February 2015.

Europol (2015b), ‘International Operation Dismantles Criminal Group of Cyber-Fraudsters’, press release, 10 June 2015.

Europol (2015c), ‘Mandate of Joint Cybercrime Action Taskforce Extended after Successful First Six months’, press release, 24 June 2015.

Europol and Eurojust (2016), Common challenges in combating cybercrime 1. As identified by Eurojust (EJ) and Europol (EP) Version 1.0, The Hague, 03/02/2016, EDOC# 802918. Available at: http://docplayer.net/28113031-Common-challenges-in-combating-cybercrime-1-as-identified-by-eurojust-ej-and-europol-ep-version-1-0.html (accessed July 2017)

Helmke G. and Levitsky, S. (2004), ‘Informal Institutions and Comparative Politics: A Research Agenda’, *Perspectives on Politics*, 2 (4), p725-40.

iOCTA (2016) The Internet Organised Crime Threat Assessment Report, Europol, The Hague, Netherlands

Jachtenfuchs, M. (2001), ‘The Governance Approach to European Integration’, Journal of Common Market Studies, 39 (2), p245-64

Joint Cybercrime Task Force (2017). Available at: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (accessed July 2017)

Justaert, A., and Keukeleire, S. (2011), ‘Informal Governance and Networks in EU Foreign Policy’, Available at: https://soc.kuleuven.be/web/files/11/72/W04-99.pdf (accessed November 2016)

Kaunert, C., Leonard, S., and Occhipinti, D.J. (2013) ‘Agency Governance in the European Union’s Area of Freedom, Security and Justice’, Perspectives on European Politics and Society, Special Issue, 14 (3), 2013.

Kaunert, C. (2010), 'The External Dimension of EU Counterterrorism Relations: Competences, Interests and Institutions', Studies in Conflict and Terrorism, 27 (1), p.41-61

Levi-Faur, D. (2012), The Oxford Handbook of Governance, (Oxford: Oxford University Press)

Meywirth, C. (2016), 'The 'orchestra approach' as a successful way forward', Europol, The Hague

Mounier, G. (2009), Europol: A new player in the EU External policy field? Perspectives in European Politics and Society, 10(4), p.582-602.

Mueller, M. (2010) Networks and States: The Global Politics of Internet Governance, (Cambridge, Massachusetts and London, England: MIT Press)

Occhipinti, D.J. (2003), The Politics of EU Police Cooperation: Towards a European FBI? (Boulder, CO: Lynne Reinner)

Peters, B.G. and Pierre, J. (2009), 'Governance Approaches' in Antje Weiner and Thomas Diez (eds), European Integration Theory (2nd edition), (Oxford: Oxford University Press)

Rodriguez, K. (2011), 'Dangerous Cybercrime Treaty Pushes Surveillance and Security Worldwide', European Frontiers Foundation, 25 August 2011.

Special Eurobarometer 359 (2011), Attitudes on Data Protection and Electronic Identity in the European Union, June 2011. Available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed October 2016)

SOCTA (2017), EU Serious and Organised Crime Threat Assessment Report, Europol, The Hague, Netherlands. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 (accessed July 2017)

Table on the Implementation of the 'Cybersecurity Strategy of the European Union: A Open, Safe and Secure Cyberspace', (JOIN(2014)1), Working Document, 28 Feb 2014. Available at:

http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference-0 (accessed March 2017)