Centre for European Integration Research

Working Paper Series

Institutionalising EU Cyber Law:

Can the EU institutionalise its many subjects and objects?

Elaine Fahey

Working Paper No. 01/2020

Centre for European Integration Research
Department of Political Science
University of Vienna

Apostelgasse 23
1030 Vienna/Austria

Telefon: +43-1-4277-49456
Fax: +43-1-4277-49497

Email: eif@univie.ac.at
Web: eif.univie.ac.at

Table of Contents

Introduction

Cyber-law-making is one of the most challenging fields of global governance because there State-centric regulatory and governance structures of public international law clash with the reality of private actors as war generators, civil society collides with international organisations and State and transnational regulators catch up with technical realities. Cybersecurity at global level is deadlocked between China, Russia and the EU, US and other parts of the developed world and a Global Pact remains elusive. For the EU as an emerging actor, the challenges in this field are magnified because they relate to its incomplete and uneven competences, and a patchwork-quilt of emerging actors, practices and rules. Efforts to develop 'global' standards, for example, the Budapest Convention, are depicted to constitute more esoteric instruments, rather than holistic standard-setting (Council of Europe, 2001). The EU has undertaken considerable efforts at cyber law-making over the course of two decades (Fahey, 2014). However, the EU has approached cyber regulation with a particularly unwieldly mix of powers, sanctions and agencification.

One of the most significant features of widespread scholarship on the EU as a cyber-actor has been its overwhelming direction towards focus on the EU as a unified, coherent and effective actor (e.g. Carrapiço and Barrinha, 2018). Cyber law-making arguably exposes the EU self-evidently as a weak global governance actor, conflicted, beholder to private actors and vexed by its competences- but also highly innovative and transparent. EU cyber action is significant in understanding EU integration practices because it exposes a partially institutionalised field, with incomplete and awkwardly non-intersecting competences, straddling incomplete Security and Digital Single Market policies, evolving sanctions and new agencies.

Cyber laws and policies fall as a law-making exercise only partly within EU security. In the context of the EU, the awkward and contestable imbalance between the 'F' 'S' and 'J' of the Area of Freedom, Security and Justice remains a complex endeavour. Scholarship is divided between the operationalised formula of Justice and Home Affairs and the political and legal reality of AFSJ. The rapid growth of EU security institutions, norms and

capacities has been shown not to lead to the convergence of national systems and a corresponding rapid growth of the use of these resources. EU security institutionalisation has been shown to not necessarily correlate to the building of efficient supranational systems (Ekengren and Hollis, 2019; Buono, 2012). However, the incompleteness of the EU in this field may easily be overstated. Major efforts have taken place recently to develop new autonomous AFSJ systems, actors and practices, from evolutions of existing AFSJ agencies to new systems in databases e.g. as Europol (Regulation 2016/794), Eurojust (Regulation 2018/1727) or a European Border and Coast Guard (Regulation (EU) 2016/162), eu-LISA (Regulation (EU) 2018/1726), ETIAS-TCN (Regulation (EU) 2019/816) etc is significant in crisis-related times. Certain 'new entities' e.g. European Border and Coast Guard as independent EU agencies represent a continuing trend of agencification of the AFSJ and its gradual institutionalisation. Cyber law-making awkwardly traverses the AFSJ incompletely and demonstrates its challenges in this regard (Christou, 2019).

The EU is globally unique in its commitment to internal and external institutionalisation practices (Fahey, 2018). Institutionalisation forms a spectrum for analysis which is 'process-based' and possibly incomplete or is dynamic and under development (Fahey, 2018, 1-8). Institutionalisation incorporates a sliding scale of minimalist enforcement, bottom-up processes of development, accountability processes, stabilisation and actorness all merging together as part of a 'process' narrative. A legal view of institutionalisation is necessarily 'bottom up', piecing together a range of instruments, regimes, practices, norms and enforcement issues. It may involve a consideration of rights and effectiveness of good governance and how existing institutions shape norms. It is a valuable metric of the evolution of EU policies.

The EU's capacity to generate new configurations of institutions, for its own actors to evolve as agencies or quasi-agencies into autonomous agencies and to generate new international institutions is a core feature of EU law-making in the global legal order. Externally, the EU has a recent history of promoting and nudging institutional multilateral innovations, from the International Criminal Court, a UN Ombudsman to a Multilateral

Investment Court (Fahey, 2018). It is proposing large-scale reform of the WTO on the verge of institutional collapse. Internally, the EU struggles with partial institutionalisation as a solution to many complex policy fields e.g. migration and Eurozone (Caparaso, 2018). For example, in the most crisis-ridden domains of the EU, partial-institutionalisation and incomplete architectural design (legal, political, structural) is often at root of major challenges. Yet institutionalisation has broadly positive goals when pursued by the EU.

The EU as a cyber-actor appears to institutionalise cyber-matters increasingly yet is also subject to an increasingly wide variety of subjects and objects that it cannot institutionalise. This will inevitably affect the 'unitary' ideal of EU action in this field. Major developments in EU cyber action internally and externally increasingly focus upon both institutionalisation and also the co-opting of private actors into governance which are argued here not to be consistent. Until recently, there had long been a lack of a unitary or central figure in EU cyber law-making with overarching responsibility for policy development. Significant legal competences have been accorded in criminal law and AFSJ and CFSP law-making over successive treaty changes but this is not reflected in cyber law-making. Indeed, the AFSJ has developed a significant portfolio of directives and regulations predicated upon maximum harmonisation and operationalisation in the post-Lisbon era of the regularisation of the AFSJ (Fahey, 2014). Certain recent EU cyber law-making developments do not necessarily reflect these developments, appearing to evolve in many different competence directions.

This paper shows that the EU as a cyber-actor constitutes a significant example of EU institutionalisation taking place in practice, caught between complex global challenges and contested taxonomies. The EU harbours multiple conflicting definitions of cybercrime between actors and entities and multiple working definitions of cybersecurity. Some key terms also lack common definition in the EU context e.g. cyber defence, albeit as a key competence of the EU Member States, where it fails to draw from commonalities sufficiently. The EU lacks sufficiently robust institutions, agencies or actors and risks conflicts and impingement upon many fundamental rights through its partial

institutionalisation of a field. It also appears afflicted by paradoxically both over-legalisation and under-legalisation of cyber law-making (Drewer and Ellermann, 2012). As a result, the EU as a Global cyber actor risks becoming an inadequate international partner through its own weak institutionalisation.

The paper examines I) cyber law-making and its subjects and objects, II) the two key planks of internal cyber-law-making firstly cybercrime then III), cyber security, followed by a look at the cyber actors in IV, and, finally, by external considerations in V).

I. INTERNAL EU CYBER LAW-MAKING

The EU's Security Union law-making: the thickening institutionalisation?

a. EU Cyber law-making: on subjects and objects

Although not unique to law-making beyond the State, arguably one of the most complex elements of cyber law-making is its mainly composite and multi-level structure (Fahey, 2018). Cyber law-making, from cybercrime to cybersecurity, governance and regulation appears increasingly defined by private actors standards, regimes and roles who assume by both stealth and also by design significant roles in regimes (Carrapiço and Farrand, 2018). The freedom from regulation and governance has 'iconically' defined cyber regimes from the outset (e.g. the internet), giving private actors the ultimate say (Barlow, 1996) — leaving others to catch up.

The problematisation of cybercrime as a regulatory subject is long disputed which has rendered its progress thorny. There has long been much confusion about the risks posed by cybercrime and the consensus that it exists (Wall, 2007; 2008: 861, 862). Few national level prosecutions, fueled by reports of a high rate of cybercrime activity, render it problematic. Added to this is the role of external malware unconnected to the internet, for example, Stuxnet via a USB key, yet also commonly problematized as a form of cyber risk warranting regulation (Fahey, 2014; Bendiek and Porter, 2013). The Commission published its new Eurobarometer report on Internet security and cybercrime in early 2019 showing that Europeans were increasingly concerned about cybercrime, with 79% of them believing that the risk of becoming a victim of cybercrime is greater than in the

past (Europeans' Attitudes Towards Internet Security, 2019). Such statistics were published on the same day in the advent of the EP elections with data to the effect that the EU had passed 15 out of 22 legislative proposals on the EU Security Union by early 2019 (European Commission, A Europe that Protects, 2019).

This politicisation of EU cyber law-making is thus of much significance but it is also embedded in longer-term uncertainty as to subjects and objects. It is uncertainty which is borne out in the weak institutionalisation taking effect.

Prior to this, however, the paper examines the nature of cyber law-making.

II. Institutionalisating EU Cybercrime: (Third Generation) EU Criminal Law

a. Overview

EU Cybercrime law has evolved piecemeal and is scattered amongst legal instruments, which continues to bear upon its longer term evolution. EU Cybercrime policy is a relatively recent legislative phenomenon, ostensibly beginning with the Framework Decision on attacks against information systems in 2005 (Council Framework Decision 2005/22/JHA, 2005). The Framework Decision provided for the criminalisation of online and offline conduct, provided for serious penalties and jurisdictional rules. However, the Commission Communication "*Towards a general policy on fight against cybercrime*" (2007) sought a broader policy framework and outlined key elements of desired EU Cybercrime policy to include increased law enforcement cooperation, public-private partnerships and international cooperation. The title of this communication underscores the *evolving* idea of EU cybercrime law and policy. The Commission Communication in 2009 on Critical Information infrastructure Protection entitled "*Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*" focused upon the threat posed by cyber-attacks and the need to secure information systems. This Communication was followed by proposed directives, which would repeal and update the provisions of the Framework Decision on attacks against information systems (Proposal for a Directive of the European Parliament and Council on attacks

against information systems and repealing Council Framework Decision 2005/222/JHA, 2010).

While some argue that soft law has been gradually replaced by hard law or actual legislation in the form of a Directive on cybercrime, a rising number of instances are also evident where private actors set standards, enforce them as judge and jury of conduct (Farrand & Carrapico, 2018). It is a trend increasingly evident not just in cybercrime but broadly in the external JHA as to cyber matters, a trend which also represents a worrisome state of EU governance and accountability standards (Christou, 2018). This role for the private sector has generated a complex balance of power as to the bottom up development of cybercrime.

b. The legal basis for EU Cybercrime action: top-down 'strength'?

Internal EU cybercrime policy has historically been situated in an *internal market* rationale but perhaps mainly theoretically rather than practically (Fahey, 2014). Internal EU cybercrime and security policies additionally have a relevance to the operation of the internal market, to the safety of consumers and the functioning of business. However, cybersecurity most recently takes its legal origins as CFSP measures. This bifurcated understanding of regulatory structures stands as an important reminder of the highly confused, incomplete traversing of ideas, institutions and actors afflicting cyber matters.

Post-Lisbon, there are ostensibly several legal bases in the treaties *outside* of the internal market rationale to legislate in order to regulate cybercrime and security. For example, there are grounds in the treaties to legislate for procedural EU Criminal law in Article 82 TFEU, allowing for the Parliament and Council to establish minimum rules to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension. In Article 83 TFEU, there is competence for the EU to enact substantive criminal law. More specifically, Article 83(1) TFEU provides that the Parliament and Council may establish minimum rules concerning the definition of criminal law offences and sanctions in the area of particularly serious crime with a cross border dimension resulting from the

impact of such offences or need to combat such offences jointly. This provision includes thereafter a list of crimes in which the EU has legislative competence which specifically includes terrorism. Article 83(2) TFEU also provides for harmonisation in the event to ensure the effective implementation of EU policy already subject to harmonisation measures. Post-Lisbon, a legal basis for cybercrime and cybersecurity seems easily grounded on these legal bases in respect of serious crime across borders. Put differently, terrorism does not appear as the only rationale of EU cyber policies and the emphasis on the impact of non-regulation of cybercrime on the internal market is notable. The gap in the type of legal instruments emerging appears thus as significant.

c. Directive

A Directive adopted in late 2013 (hereafter the Cybercrime Directive) places emphasis in particular upon a Strategy to fight *new* methods of creating cybercrime, for example, large scale 'botnets' i.e. networks of computers with a cross-border dimension (see Directive 2013/40/EU, 2013). It purports to criminalise access to systems, system interferences and data interference, with penalties from two to five years. It provides for an ostensibly unwieldy procedure in Article 12, whereby a Member State must inform the Commission where it wishes to take jurisdiction over offences *outside* its territory. An earlier version of the Cybercrime Directive has been criticised for its vague legal obligations and its over-criminalisation, especially of 'small-scale' hackers. The Commission has invoked Eurobarometer surveys on cybercrime referencing the legal uncertainty surrounding protections for consumers making online payments to warrant the use of so-called 'Third Generation' EU Criminal law (European Commission Press Release IP/12/751, 2012; Fichera, 2013). However, in this regard, in contrast to the Framework Decision, it is not necessarily a superior regulatory instrument. As a Directive, disparities inherent in its implementation practices may cause its provisions to be unevenly interpreted across the Member States, which seems undesirable from the perspective of regulating holistically. It is worth noting that a 'comprehensive' vision of EU cybercrime law was mooted at the launch of the Directive by the Commission to include provisions for financial cybercrime, illegal Internet content, the collection, storage and transfer of electronic evidence, as well as more detailed jurisdiction rules, in the form of 'comprehensive' legislation operating in

parallel with the Convention, with non-legislative measures. It is a formulation of cybercrime law which has yet to materialise.

Cybercrime is conventionally said to be differentiated from cybersecurity through *temporal constructs* one relating to the past, the other to the future (Bernik, 2014: 143). As will be argued here this temporal division is problematic from a broader EU law perspective because in many respects the division is highly constructivist and unduly separatist. Arguably, it precludes more logical and reflective thinking on the capacity of law to engage with systems which are innate complex to regulate. It also has no link to how the EU operationalised crime and security in cyber issues — both are partially institutionalised but unlinked to 'time'.

It might be said that the internal market basis for cybercrime gives it the 'fire power' to generate strong actors and agencies, but whether this is the case remains to be seen. Thus far, this has not yet taken effect. It represents the most definitive locus for a strong institutionalisation and further agencification.

It nonetheless has a specific link to cybersecurity, discussed next.

III. Institutionalisating EU cybersecurity: A concept in search of a definition?

a. Overview

The historical absence of a common EU framework on cyber security has been the subject of much critique, from inside and outside the EU institutions, such as the European Parliament and ENISA, as is the absence of cyber-security strategies at national level. The EU's law-making in cybercrime and cybersecurity begins in policy terms most concretely from its Cybersecurity Strategy in 2013 which defines cybersecurity extremely broadly. Cybersecurity is referred to as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information

infrastructure" (EU Cybersecurity Strategy, 2013: 3). What is significant about the Strategy is the dominance of security therein and the lack of specificity about the definition of cybercrime to be deployed. Others point to the narrower definition of cybersecurity used by the EU Agency for Network and Information Security (ENISA), distinguishing cybercrime, cyber espionage and cyber warfare (see Odermatt, 2018). Despite being explicitly a cybersecurity strategy the EU's Strategy has a complex engagement with cybercrime therein relegated to "[…] a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (EU Cybersecurity Strategy, 2013: 3).

An overwhelming number of legal and policy documents relating to cybersecurity often begin with a conceptual discussion about what exactly cybersecurity means (Odermatt, 2018). It is a term which is often ambiguous and ill-defined partly because of the evolving nature of the treats. It is not mentioned as a policy field in the EU treaties and there is no explicit basis for it in EU law largely because the EU has traditionally related to the economic effects of cyber-attacks in order to legislate in cybercrime (Odermatt, 2018). The EU's Strategy for cyber security was finally published in early 2013 and it follows many less than successful or complete policy initiatives in this area. These include a proposal for an Networks and Information Policy in 2001, soft law strategies and various programmes, instruments and policies on so-called Critical Infrastructure, policies that did not establish binding legal obligations upon the operators of critical infrastructures (for example, European Commission Communication 298, 2001; European Commission Communication 251, 2006; European Commission Communication 14, 2009; Council Directive 2016/1148, 2016). This reliance upon soft law to regulate cyber risk has been overtaken. Cyber security is depicted in the EU's Strategy as referring to 'the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure' (EUCSS, 2013: 3). This generates three definitional questions concerning cyber risk. Firstly, the relationship of Cyber Security and confidentiality of information with data protection matters is ostensibly of much significance from the type of harm formulation but is not reflected in the Strategy or its

legal tools, discussed next. Secondly, its definition presupposes the relevance of militarisation to it conceptually. The militarisation of cyber offences is perceived to be a distinctive feature of cyber security particularly in the US and accordingly, there is much debate concerning the application of international law relating to war on cyber-attacks (for example, Schmitt, 2013). While the text of the Council of Europe Convention itself does not mention terrorism, a listed activity on the website of the Council of Europe is cyber-terrorism. However, the Strategy does not appear to be substantively motivated by or governed by such concerns as to risk overall. Thirdly, the Strategy describes *cybercrime* to include a range of different criminal activities, not precisely as in the Convention, only approximately so (EUCSS, 2013; 3). Its definition of cybercrime has generated infelicities in its taxonomy, infelicities that have generated much critique and which impact upon its over-arching framework for institutionalisation, seemingly improbably in the current state of affairs (the European Data Protection Supervisor, 2013).

This leads to the key Act developed in 2019.

b. Cybersecurity 'Act', 2019: the beginnings of 'strong' institutionalisation?

Some key EU Criminal law Directives deploy maximum harmonization on the bases of Article 82(2) and 83(1) TFEU in order to regulate the sexual exploitation of children online and child pornography as measures for judicial cooperation in criminal matters of the EU (e.g. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography). On the one hand, examples such as this show the extraordinarily broad parameters of cyber matters. However, on the other hand there are even more striking developments. For example, on 13 September 2017 the Commission adopted a cybersecurity package predicated upon a Regulation formulated as a so-called 'Cybersecurity Act' on the basis of Article 114 TFEU as an act in the context of the Digital Single Market Strategy (Regulation 2019/881/EU, 2019). As part of a so-called 'package' the Act has the intention to set up a high level of cybersecurity, cyber resilience and trust within the Union with a view to ensuring the proper functioning of the internal market. The changes this new EU Regulation sought to bring about relate to both: a

comprehensive reform of ENISA and the creation of a certification framework. In reality, the Act is about a trend towards permanent agencification and governance of the private sector through their coopting in complex ways. It brings into sharp focus earlier efforts at development of EC3 as a desk in Europol, discussed below. The Agency established will thus 'succeed' ENISA as established by Regulation No. 526/2013 as a significant step in the agencification of cyber policies traversing a variety of domains — and its consequent deeper institutionalisation. The Act thus represents a definitive step towards agencificiation through internal market competences. Yet other criminal law competences are not deployed and the nature of the use of the internal market may be said here to be 'light'. The weak definition of cybersecurity appears at root a core issue and a contributor to weak institutionalisation.

However, as to cybersecurity, new CFSP cyber sanctions are also a core plank thereof and are discussed next.

c. EU Cyber sanctions: 'top-down' Executive-led horizontalisation of the CFSP?

The EU has adopted sanctions against 35 countries and four thematic sanctions regimes regarding chemical weapons and terrorism and most recently cyber sanctions and human rights (Portela 2019; EU Sanctions: A Key Foreign and Security Policy Instrument, 2018; Eckes, 2019; EU Sanctions Map, 2019). The EU is the world's second-most active user of restrictive measures after the United States (US). On 18 October 2018, the European Council adopted conclusions calling for work on the capacity to respond to and deter cyber-attacks through EU restrictive measures to be taken forward. As a follow up, on 17 May 2019, the Council adopted the necessary legal acts establishing a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. These acts also allow for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations, pursuant to Article 21 TEU. On 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks

against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP) (Council Decision 7299/19, Council Conclusions 13/18, 2018). It is a striking executive-led legal formula to deploy. Yet it occurs in a field where the CJEU has become gradually more pervasive and extended its own powers of review in the area of the CFSP and so this tempers to some degree its executive-led nature (cf Eckes, 2019).

It is also widely recognised that the United Kingdom (UK) is one of the driving forces behind the EU's active sanctions policy, as are the Netherlands, both key targets of Russian foreign policy activities in recent times. How non-EU States will view this state of affairs remains to be seen e.g. who will align with EU CFSP cybersanctions and who will litigate them going forward constitute issues of note. To similar effect, how the post-Brexit constellation of States advocating innovative sanctions in foreign policy as a tool thereof remains to be seen or how executive-led cybersanctions policy will become. Sanctions constitute an ad hoc response of sorts and do not appear to represent a deeper institutionalisation, more so just mere widening.

This leads to a broader discussion of actors and cyber law-making.

IV. EU Cyber Actors: On Compartmentalisation

a. Overview

A variety of entities were initially involved in embryonic cyber policies, with both and internal and external mandate and all these entities contribute to the web of actors evolving here. The necessity of the number of entities has been explained as part of the knowledge-building or discovery process for the EU to build a cyber-regulatory structure. Responsibility for EU Cybercrime and cyber security was historically divided in the first post-Lisbon Commission between the Vice-President of the Commission, Nelie Kroes (Cyber security/Digital Agenda) and the then Commissioner for Home Affairs, Cecilia Malmstrom (Cybercrime). The original joint involvement of three Commission DG's:

Home Affairs, Justice and Information Society, as well as numerous agencies in the development of an EU cyber strategy is indicative of the challenges of internal security which has a considerable external or global dimension and the development of an EU cyber strategy is touted also as a major success as regards inter-institutional cooperation. In the new Commission of 2019 cybercrime and security traverse DG Internal Market; DG Connect (CNECT) (DG CNECT: Communications Networks, Content & Technology). In charge of all directorates - Deputy Director-Khalil Rouhana; Directorate H Digital Society, Trust & Cybersecurity K. Rouhana (acting) H1 Cybersecurity Technology & Capacity Building - M. González-Sancho; H2 Cybersecurity & Digital Privacy Policy - J. Boratynski; Digital Single Market – Directorate F: Digital Single Market – Gerard de Graaf (as per 01/12/2019) and DG HOME: General Migration and Home Affairs. Directorate D4 – Cybercrime – Cathrin Bauer-Bulst). It is a very broad, institutionalised and balanced composition of teams on one level, but also seeks to separate content in ways which are not necessarily aligned with actual law-making.

Considerable differences between the two fields of digital single market and internal market exist from a legal perspective — as an incomplete sub-field thereof despite the use of broader internal market legal policies here. Security and internal market matters have a complex intersection in cyber matters and it remains to be seen how much the legal and infrastructure support structures will be adequately aligned. For now, the compartmentalization of teams in no way relates to the putative or attempted institutionalisation of EU cyber law-making taking place.

b. ENISA: Top-down and bottom-up institutionalisation?

ENISA constitutes one of the earliest EU efforts at the institutionalisation of cyber law-making. Originally, ENISA had a restricted mandate and liaised predominantly with largely national law enforcement bodies on the security aspects of cybercrime. ENISA was involved in establishing the European cybersecurity certification framework by preparing certification and helping EU Member States who would request it to handle cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross borders cyber-attacks and crises. This task built on ENISA's role as secretariat of the

National Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive). ENISA was concerned with improving the EU's resilience against cyber-attacks, notably by capacity-building but also by exchanging information and providing analyses. Furthermore, at the request of one or more Member States, ENISA assisted Member States in the assessment of incidents having a substantial impact by providing expertise and facilitating the technical handling of such incidents. It also provided support to ex-post technical inquiries and provided the secretariat for the CSIRTs network.

As discussed above, in 2017, a new Act providing for a Cybersecurity Agency was adopted which would give ENISA more tasks and resources to assist Member States, e.g. through a stronger mandate, a permanent status and more resources. In particular, a core plank of its work would relate to an EU framework for cybersecurity certification as an EU-wide framework, thereby embedding its institutionalisation into systems.

Whether ENISA can evolve into a major actor remains to be seen in its latest iteration. Its international activities are of note with key partners e.g. capacity building with Japan in 2020. However, its reliance on a vast multitude of (sub-)national and technical actors remains it core challenge — 'bottom up' and 'top down' — a group which continues to evolve. It challenges its capacity to generate strong and autonomous institutions.

c. EU Cybercrime Centre 'EC3': the weakest institutional link?

Another actor of note is the EU Cybercrime Centre, with the acronym "EC3", which was established in early 2012, operational by 2013 as a 'desk' within Europol. The placement of the Cybercrime Centre 'within' Europol was explicitly part of the Action Plan to implement the Stockholm Programme (Action Plan Implementing the Stockholm Programme, 2010: 38). Also, the Cybercrime Centre was asserted to complement Directives on attacks against Information Systems and the Directive adopted in 2011 on combating the sexual exploitation of children online and child pornography (European Parliament and Council Proposal 517, 2010; Directive 2011/92/EU, 2011). Its purpose was thus institutional and strategic and has been established within an evolving EU

agency, the European Police Office, Europol, thereby forming an EU focal point in fighting cybercrime, fusing information and informing Member States of threats. While one could quibble with the necessity for such an entity and the extent to which it overlaps with other agencies such as Europol in particular, but also Interpol, the G8 and Eurojust, Europol was asserted at the launch of the Cybercrime Centre to lack resources to gather information from a broad range of sources and to lack the specific capacity to deal with requests from law enforcements agencies, the judiciary and the private sector (European Commission, 2012). The novelty of the Centre was that it purported to adopt a "cross-community approach", to exchange information beyond the law enforcement community, develop a common standard for cybercrime reporting and assume the collective voice of cybercrime investigation. The Cybercrime Centre was to post liaison officers to the European Commission and the European External Action Service as well as to EU agencies (Nielsen, 2012).

Curiously, the Centre had no express link or nomenclature associated with Cyber security. Moreover, its express function is to disrupt organized crime networks and monitor illegal activities which begs the question as to what precisely was illegal under EU law, given the broad parameters of the existing Framework Decisions and the discretion accorded to Member States therein. The establishment of an EU agency to engage in cybercrime monitoring *prior* to the development of a coherent cybercrime and cyber security strategy thus lacking overarching legal infrastructure indicates the piecemeal and evolving nature of the EU internal policies. If we can say this constitutes an example of extremely weak institutionalisation — and thus a low-water mark of EU action, this is also an important observation of the nature of EU institutionalisation taking place, initially antipathetic to institutions and lacking clear policies.

d. EU as an International Cyber Actor: Centralised EU Action through the prism of International Law

Beyond individual entities, the EU itself is an increasingly studied actor from an international law perspective. Cyberspace is increasingly argued by public international law specialists not to constitute a new legal domain (e.g. Buchan, 2018). However,

although cyberspace has had a difficult relationship with international law and the Nation State, the EU has a 'healthy' presence in a variety of international fora (e.g. Odermatt, 2018). The EUCSS outlines the goal of establishing a coherent international cyberspace policy in order to be able to promote EU values (EUCSS, 2013: 3). Thus, significant cooperation is also ongoing between the EU and Council of Europe in the area of developing best practice in international governance, discussed below. The EU has also been involved in bilateral actions with many partners as to cyber activities e.g. EU-US, Korea. The EU is also active in many forums where cyber matters are being developed e.g. Organisation for Economic Co-operation and Development (OECD), United Nations General Assembly (UNGA), Organisation for Security and Co-operation in Europe (OSCE), International Telecommunication Union (ITU), World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). Cyber defence policy also requires cooperation with key partners such as NATO, given that cyber defence is a core task of NATO. CERT-EU has a technical agreement relating to information sharing with the NATO Computer incidence response capability. One of the key challenges of EU international action is the presentation of coherent positions where within its own organisational policies, rules and practices, a multiplicity of positions exist.

The Conclusions on Cyber Diplomacy adopted by the Council on 11 February 2015 gave a mandate to the EU and its Member States to uphold freedom, security and prosperity in the cyberspace: this includes inter alia, promotion and protection of human rights, application of international law and norms of responsible state behaviour, internet governance, fight against cybercrime, protection of networks and systems of government and critical infrastructure, international cooperation, capacity building, competitiveness in the digital market, strategic engagement with key partners. This mandate has been labelled as 'ambitious' in 2019 by the European Parliament (Council, 2015). In late November 2017, the Council underlined the need to address cybersecurity with a coherent approach at national, EU *and global level* (Council doc. 14435/17, 2017). This newer diplomatic push was of significance given the timings of many key law-making efforts. For example, the EU developed key cyber sanctions in the field of malicious attacks in the domain of the CFSP immediately prior to the EP elections in 2019 (e.g. Tsagourias,

2019). Cyber-attacks often have an external dimension and in this respect the Council refers to its Conclusions of 19 June 2017 on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('cyber diplomacy toolbox'). The cyber diplomacy toolbox sets out measures, including restrictive measures, which can be used to prevent and respond to malicious cyber activities.

Then on 28 June 2018, the European Council, in its Conclusions, called on institutions and Member States to implement the measures referred to in the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, including the work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox.

On 18 October 2018, the European Council adopted conclusions calling for work on the capacity to respond to and deter cyber-attacks through EU restrictive measures to be taken forward. As a follow up, on 17 May 2019, the Council adopted the necessary legal acts establishing a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. As noted above, these acts also allow for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations, pursuant to Article 21 TEU and significantly enhance the unitary nature of the EU's response — de facto and de jure institutionalising to a degree, subject to the issues raised above.

V. EXTERNAL EU CYBER LAW-MAKING

a. Incomplete International cyber law-making: A lack of institutionalisation

Significant non-state governance in the cyber domain have transformed the meaning of national territory and sovereignty (Fahey, 2018). Digital space is a major new theatre for capital accumulation and global capital. Alternatively, cyberspace can be said to constitute a new domain — but not an unprecedented one per se, whereby the challenges that it

poses for states are similar to those that the international community has faced in the past as to other domains, such as the international law governing the high seas, outer space and Antarctica (Eichensher, 2015:321). One may argue that there are more actors, spaces, communities and users of cyberspace such that it lacks a comparator. Much theorisation on the notion of cyberspace was derived from the 1980s and science fiction. Cyberspace, however, is increasingly argued by public international law specialists not to constitute a new legal domain (Buchan, 2018). Cyberspace has had a difficult relationship with international law and the Nation State because there is still no cyber multilateral or uniform cyber law as an instrument of international law which is all encompassing. Cyber law-making is a predominantly global affair and yet its de-centralisation through according powers to powerful global private entities continues to be paradoxical (Carrapiço and Farrand, 2018). The role of such private entities in cyber law-making appears as the antithesis of global law-making. However, at a global level, there is no global cyber pact and Russia, the US and China remain key stumbling blocks to global reform, discussed next. The paper examines UN and Council of Europe reforms and the EU's role in the latter.

UN level

There has been a series of resolutions and five UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The latest UN Group, in June 2017, witnessed the refusal of China, Russia and Cuba to adopt a paragraph on the applicability of self-defense, countermeasures and the law of armed conflicts in cyberspace. More recently, the international community has moved one step closer to the risk of fragmentation during the last session of the General Assembly of the United Nations in 2018. The General Assembly of the United Nations adopted two resolutions following on the failure of the 2016-2017 UN GGE, both resolutions calling for the creation of a process to follow up on the past UN GGE processes. Having two parallel processes discussing the application of international law to cyberspace, initiated by two different groups of States with divergent approaches on the application of some norms of international law, contribute to the risk

of geographical fragmentation (Delarue, 2019). It is thus a more fragile context broadly overall.

Council of Europe level: fostering stronger institutionalised ties?

The Council of Europe Cybercrime Convention ('Budapest Convention') forms the basis for all EU, EU-US and to some extent US law as a form of 'transnational gold standard'. The Budapest Convention on Cybercrime was opened for signature in 2001. Membership in this treaty increases continuously and any country able to implement its provisions may seek accession. By September 2019, 64 States had become Parties and a further 8 had signed it or been invited to accede. In addition to these 72 States a further 28 are believed to have legislation largely in line with this treaty and a further 52 to have drawn on it at least partially (see also Fahey, 2014). The Budapest Convention is supplemented by an additional Protocol on Xenophobia and Racism committed via computer systems. Much EU Criminal law has its origins in Council of Europe Conventions because of their tendency to set best international practice and to organise regimes of considerable merit (Mitseligas, 2009; Korff, 2013). The Cybercrime Convention is now seen as major transnational venue for internet reform but this has not always been the case. The Cybercrime Convention has been criticised by civil society as too heavily reflecting law enforcement standards and its relationship with the broader regulatory framework of the Council of Europe and large-scale standards on data protection remains less than persuasive (Brown, 2014: 3.3). In particular, the Convention is perceived by privacy advocates as a broad but not the broadest international forum, whereby the UN forms the apex thereof (Brown, 2014). The US is not a member of the Council of Europe but took a significant part in the drafting of the Council of Europe Cybercrime Convention and has signed and ratified it domestically, as have approximately half the Member States of the EU (Ratification Table, 2019; Fahey, 2014: 368). In the wake of the NSA affair, the Cybercrime Convention has been touted by the US in EU-US negotiations on its aftermath recently as setting particularly high international standards in privacy and data protection and as evidence of the willingness of the US to lead and set such standards (Council doc.16987/13, 2013; European Commission Communication 846, 2013).

The Council of Europe Cybercrime Convention adopts a broad perspective on cybercrime. In fact, it is much criticised for its overbroad content, its lack of provision for cross-border enforcement and its obligations imposed upon Internet Service Providers (Goldsmith, 2001; Porcedda, 2011) and also that it does not purport to regulate cyber security. The Convention distinguishes between four types of offences which as a typology may be argued not to be wholly consistent in that three of the types of offences focus upon legal protection whereas the fourth does not and leads as a result to overlap between the categories. In addition, criminal acts such as cyber terrorism or phishing cover acts may fall within several categories (Gercke, 2012). The Convention does not contain as many definitional conceptions of cybercrime as other regional legislative models do, which may appear surprising given its tendency towards harmonisation rather than closing gaps in regulation. Nonetheless, it is the most far-reaching multilateral agreement on cybercrime in existence, purporting to harmonise national legislation procedurally. Substantively, its suitability as a 'gold-standard' source of regulation — pan-European and beyond — may be open to question.

There is a particular emphasis in contemporary Council of Europe Cybercrime policy as to its reform upon the dichotomy of hard and soft law and the relevance of jurisdiction, conceptual focusses that appear surprising (Council of Europe, 2010). For example, the Council of Europe Commissioner for Human Rights has encouraged states not to use data obtained from servers in another country under informal arrangements but instead to use mutual assistance arrangements (Korff, 2014). Moreover, from the perspective of the Council of Europe, placing limits on the extra-territorial exercise of jurisdiction in relation to transnational cybercrimes has also been argued to be essential. This position has much resonance in contemporary US law where the extra-territorial use of law is widely advocated (Hathaway *et al*, 2012). Yet what should the Convention be aiming for? Is its focus in reality conventional rather than progressive? Such a focus appears troubling from the 'transnational gold-standard', as one centered exclusively around enforcement as opposed to rights-based rule-making. Its unequivocal stance as the leading cyber law instrument draws attention to its less than holistic integration of other regimes even within the Council of Europe, its rights-based conceptions of rule-making in this field and

its incompleteness as an instrument. The lack of any meaningful engagement between the Convention and the reform of related UN measures also raises the question as to regime interaction or lack thereof and the ideal of 'holistic' rule.

The Parties to the Budapest Convention have been searching for solutions for some time, that is, from 2012 to 2014 through a working group on transborder access to data and from 2015 to 2017 through the Cloud Evidence Group. In June 2017, the Cybercrime Convention Committee (T-CY) agreed on the Terms of Reference for the preparation of the Protocol and negotiations commenced in September 2017 on: Provisions on more efficient mutual legal assistance; Provisions on direct cooperation with providers in other jurisdictions; Framework and safeguards for existing practices of extending searches transborder; Rule of law and data protection safeguards. The Parties to the Convention have been looking to reform access to electronic evidence by judicial and police authorities through a Second Additional Protocol which would address those challenges by ensuring greater international cooperation. The negotiations on the Protocol started in June 2017 and are due to be concluded at the time of writing. They mostly have not sought institutionalised outcomes.

b. Can the EU institutionalise at regional level?

The EU has had to consider the protection of privacy and personal data (as specified in the General Data Protection Regulation, the e-Privacy Directive and the Data Protection Directive for Police and Criminal Justice Authorities) and the development of EU rules on electronic evidence relative to third countries. In its negotiation directives, the EU has raised the issue as to consistency with respect to e-evidence regimes and third countries, in particular the US. Two recommendations to participate in the Second Additional protocol and to open negotiations with the US were being adopted by the Commission at the same time. The Commission and other EU institutions are observers in the Protocol Drafting Plenary (European Commission Recommendations 70; 71, 2019). An EU specific 'disconnection' clause appeared to raised challenges for a guarantee that only EU law, whether existing or future, will be applied as between EU Member States. However, where the Budapest Convention already contains a provision which should meet the concerns of

the European Union not to compromise its normative acquis or the autonomy of its legislative process (Legal Opinion on Budapest Cybercrime Convention, 2019).

These issues as to the autonomy of EU law should not be discounted since they demonstrate an increasing challenge for the sui generis nature of EU law when engaging with international law-making. The autonomy of EU law has emerged as a complex statement of EU distinctiveness. It appears to increasingly inhibit institutionalisation beyond the State (e.g. CJEU Opinion 2/13 ECHR accession) (Eckes, 2013). Amendments to the Budapest Convention demonstrate the challenges of the EU seeking to act as a global actor and a very important limitation of the 'global' in a forum where the EU can, in theory, influence the global. EU's own internal taxonomies hinder it in institutionalising further and evolving international organisations' positions. This, however, is also a broader phenomenon of EU International relations law where the autonomy of EU law operates as a barrier to deeper institutionalisation.

VI. Concluding reflections

The EU's cyber law-making appears long dominated by weak efforts at institutionalisation and few actors. This could radically change given the unfolding internal market directions of cyber law-making. The reality of cyber law is, however, dominated by a need to use CFSP and criminal law powers and sanctions and the overall matrix of law-making appears increasingly skewed in different directions, destined towards partial institutionalisation and weaker actors.

This paper has outlined how EU law appears divided between cybercrime and cyber security in a manner which is not always logical or effective. The divisions feed into other challenges — e.g. how it relates to privacy or human rights, fair procedures, administrative justice, defence of the state, private companies and individuals etc. A more holistic and unified approach would enable the EU to engage more meaningfully at International level. Cybercrime and security constitute one of the most useful examples of transnational law making and global governance. EU cybercrime and security law-making are thus taking

place in a vacuum against a backdrop of complex international law-making regimes only under development. Its own complexity as an international organisation increasingly is also apparent as the Budapest Convention developments amply demonstrate.

The EU as a cyber-actor appears to institutionalise cyber-matters increasingly yet is also subject to an increasingly wide variety of subjects and objects that it cannot institutionalise. Major developments in EU cyber action internally and externally increasingly focus upon both institutionalisation and also the co-opting of private actors into governance which are not consistent. Significant legal competences have been accorded in criminal law and AFSJ and CFSP law-making over successive treaty changes but this is not optimally reflected yet in cyber law-making.

The paper has argued that cyber law-making must become a holistic and joined-up study as a matter of law and needs to traverse the internal and external of EU law more explicitly and transparently. While many of the challenges affecting EU law-making in the cyber domain are equally evident at international level, EU divergences inhibit further institutionalisation.

BIBLIOGRAPHY:

BOOKS:

Bernik, Igor (2014) *Cybercrime and Cyber Warfare* (London and Hoboken: John Wiley and Sons).

Buchan, Russell (2018) *Cyber-Espionage and International Law* (Oxford and London: Hart Publishing).

Delarue, François (2020) *Cyber Operations and International Law* (Cambridge: Cambridge University Press).

Fahey, Elaine (2018) *Introduction to Law & Global Governance* (Cheltenham and Northampton: Edward Elgar Publishing).

Fahey, Elaine (2018) (ed) *Institutionalisation beyond the Nation State* (Heidelberg: Springer Publishing)

Schmitt, N Michael (ed) (2013) *Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence: Talinn Manual on the International Law applicable to Cyber-Warfare* (Cambridge: Cambridge University Press).

Wall, David (2007) *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge and Malden: Polity Press).

BOOK CHAPTERS:

Carrapiço, Helena and Farrand, Ben (2018) 'Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism' in Bures, Oldrich and Carrapiço, Helena (eds) *Security*

Privatization : How Non-Security-Related Businesses Shape Security Governance, (Cham : Springer International Publishing AG) 197-218.

Eckes, Christina (2019) 'The Law and Practice of EU Sanctions' in Blockmans, Steven and Koutrakos, Panos (eds) *Research Handbook on EU Common Foreign and Security Policy,* (Cheltenham and Northampton: Edward Elgar) 206-229.

Odermatt, Jed (2018) 'The European Union as a Cybersecurity Actor' in Blockmans, Steven and Koutrakos, Panos (eds) *Research Handbook on EU Common Foreign and Security Policy* (Cheltenham andNorthhampton: Edward Elgar Publishing) 354-373.

Porcedda, Maria Grazie (2011) 'Transatlantic Approaches to cyber-security and cybercrime' in Pawlak, Patryk (ed.), '*The EU-US Security and Justice Agenda in Action'* (30 December 2011) EU Institute for Security Studies Chaillot Paper, No 127, (Paris: EU Institute for Security Studies) 41-53.

JOURNAL ARTICLES:

Andiek, Annegret, Porter, Andrew (2013) 'European Cyber Security Policy within a Global Multistakeholder Structure', *European Foreign Affairs Review,* Volume 18 Issue 2, 155-180.

Brown, Ian (2014) 'The feasibility of transatlantic privacy protective standards for surveillance', *International Journal of Law and Information Technology*, Volume 23 Issue 1, 23-40.

Buono, Laviero (2012) 'Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3)', *New Journal of European Criminal Law*, Volume 3 Issues 3-4, 332-343.

Caparaso, James (2018) 'Europe's Triple Crisis and the Uneven Role of Institutions: the Euro, Refugees and Brexit', *Journal of Common Market Studies*, Volume 56 Issue 6, 1345-1361.

Carrapico, H., and Barrinha, A. (2017) The EU as a Coherent (Cyber)Security Actor?. JCMS: Journal of Common Market Studies, 55: 1254– 1272. doi: 10.1111/jcms.12575.

Christou, George (2018) 'The Challenges of Cybercrime Governance in the European Union', *European Politics and Society*, Volume 19, Issue 3, 355-375.

George Christou (2019) The collective securitisation of cyberspace in the European Union, *West European Politics*, Volume 42, Issue 2, 278-301

Eichensher, Kristen (2015) 'The Cyber Law of Nations', *Georgetown Law Journal*, Vol.103, 317-380.

Eckes, Christina (2013) 'EU Accession to the ECHR: between Autonomy and Adaptation', *Modern Law Review*, Volume 76, 254-285

Ekengren, Marcus and Simon Hollis, (2019) 'Explaining the European Union's Security Role in Practice', Journal of Common Market Studies, pp.1-19.

Fahey, Elaine (2014) 'On the Use of Law in Transatlantic Relations: Legal Dialogues Between the EU and US', *European Law Journal,* Volume 20 Issue 3, 368-384.

Fahey, Elaine (2014) 'The EU's Cybercrime and Cybersecurity Rule-Making: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, Volume 5 Issue 1, 46-60.

Fishera, Massimo (2013) 'Criminal Law beyond the State: The European Model', *European Law Journal,* Volume 19, Issue 2, 174-200.

Goldsmith, Jack (2001) 'The Internet and the Legitimacy of Remote Cross-Border Searches', *University of Chicago Legal Forum,* Volume 2001 Issue 1, 103-118.

Hathaway, Oona, Rebecca Crotoff, Philip Levitz, Haley Nix, Aileen Nowlan,, William Perdue and Julia Spiegel (2012) 'The Law of Cyber-Attack', *California Law Review,* Volume 100 (no issue) 817-886.

Sassen, Saskia (2017) 'Embedded Borderings: Making New Geographies of Centrality', *Territory, Politics, Governance*, Volume 6 Issue 1, 5-15.

Trauner, Florian and Rippoll-Servant, Ariadna (2016) The Communitarization of the Area of Freedom, Security and Justice: Why Institutional Change Does not Translate into Policy Change, *Journal of Common Market Studies*, Volume 54 Issue 6, 1417-1432.

Wall, David (2008) 'Cybercrime and the Culture of Fear: Social Science fiction(s) and the production of knowledge about cybercrime', *Information, Communications and Society*, Volume11 Issue 6, 861-884.

DOCUMENTS:

Council of Europe (2001) 'Convention on Cybercrime', European Treaty Series, No.185 (Budapest), 23.11.2001, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, accessed 08.03.2020.

Council of the European Union (2014) 'EU Cyber Defence Policy Framework', - 15585/14 (Brussels), 18.11.2014. 14 pages,

https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf, accessed 08.03.2020.

European Commission (2011) 'Communication from the Commission to the European Parliament and Council - First Annual Report on the implementation of the EU Internal Security Strategy', COM 790 (Brussels), 19 pages.

European Commission (2010) 'Communication from the Commission to the European Parliament and Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', COM 673 (Brussels), 24 pages.

Council of the European Union (2011) 'Draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record Data to the United States Department of Homeland Security', 20.05.2011, Council doc. 10453/11.

Council of the European Union (2010) 'Agreement between the European Union and the United States of America on the processing and Transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program', Official Journal L195/5, 27.07.2010, 2010/420/EU.

European Commission (2012) 'Press Release - EU Cybercrime Centre to Fight Online Criminals and Protect E-consumers', (Brussels), 28.03.2012, IP/12/317.

European Commission (2013) 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' JOIN 1 Final (Brussels), 20 pages.

European Commission (2013) 'Commission Staff Working Document - 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' SWD 32 Final (Strasbourg), 160 pages.

European Commission (2019) 'Press Release - A Europe that Protects: 15 out of 22 Security Union Legislative Initiatives Agreed So Far', (Brussels), 20.03.2019, IP/19/1713.

The Council of the European Union (2005) 'Council Framework Decision 2005/22/JHA of 24 February 2005 on Attacks Against Information Systems', Official Journal L 69, 16.03.2005, 69/67.

Commission of the European Communities (2007) 'Communication From The Commission To The European Parliament, The Council And The Committee Of The Regions - Towards a General Policy on the Fight Against Cyber Crime', COM 267 Final (Brussels), 10 pages.

European Commission (2010) 'Proposal for a Directive of the European Parliament and Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA', COM 517 Final, (Brussels), 18 pages.

European Commission (2012) 'Press Release - Cybercrime: EU citizens concerned by security of personal information and online payments', (Brussels), 9.07.2012, IP/12/751.
The European Parliament and the Council (2013) 'Directive 2013/40/EU On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA', Official Journal L 218/8, 14.08.2013

Commission of the European Communities (2001) 'Communication From The Commission To The Council, The European Parliament, The European Economic And

Social Committee And The Committee Of The Regions - Network and Information Security: Proposal for a European Policy Approach', COM 298, (Brussels), 27 pages.

Commission of the European Communities (2006) 'Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions - Strategy for a Secure Information Society: "Dialogue, Partnership and Empowerment', COM 251, (Brussels), 10 pages.

Commission of the European Communities (2009) 'Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - on Critical Information Infrastructure Protection: Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM 14, (Brussels), 11 pages.

European Parliament and the Council (2019) 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and On Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal L 151/15, 07.06.2019.

Council of the European Union (2019) 'Legislative Acts and other Instruments - Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States', 7299/19 (Brussels), 14.05.2019, 19 pages.

European Council (2018) 'From General Secretariat of the Council to Delegations - Conclusions 18 October 2018', EUCO 13/18, (Brussels), 5 pages.

European Commission (2010) 'Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The

Committee Of The Regions - Action Plan Implementing the Stockholm programme', COM171 (Brussels), 68 pages.

European Commission (2010) 'Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA', COM 517 Final (Brussels), 18 pages.

European Parliament and the Council (2011) 'Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of children and Child Pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal L 335/1, 17.12.2011.

European Commission (2012) 'Press Release - Frequently Asked Questions: the new European Cybercrime Centre', MEMO/12/221, 28.03.2012, 4 pages.

Council of the European Union (2017) 'Outcome of Proceedings - General Secretariat of the Council to Delegations', 14435/17, (Brussels), 20.11.17, 17 pages.

Council of the European Union (2013) 'Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection', Council doc. 16987/13, (Brussels), 2 pages.

European Commission (2013) 'Communication From The Commission To The European Parliament And The Council - Rebuilding Trust in EU-US Data Flows', COM 846 final 9, (Brussels), 9 pages.

Council of Europe (2010) 'Recommendation and Explanatory Memorandum - The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling', CM/Rec 13, Council of Europe Publishing (Strasbourg), 58 pages.

European Commission (2019) 'Recommendation for a Council Decision Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters', COM 70 final, (Brussels) 5.2.2019, 13 pages.

European Commission (2019) 'Recommendation for a Council Decision Authorising the Participation in Negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM 71, (Brussels), 5.2.2019, 11 pages.

Strasbourg (2013) Impact Assessment - Cybersecurity Incidents are Increasing at an Alarming Pace' SWD 32 final, 7.02.2013.

The European Council and the Parliament (2016) 'Directive - On the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime', Official Journal L119/132, 27.04.2016.

European Commission (2013) 'Joint Communication to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace', JOIN 1 Final (Brussels) 07.02.2013, 20 pages.

The European Parliament and the Council (2016) 'Directive 2016/1148 - Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union' Official Journal L194/1, 06.07.2016.

Expert Group on Liability and New Technologies – New Technologies Formation (2019). Liability for Artificial Intelligence and Other Emerging Digital Technologies (European Commission), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608, accessed 08.03.2020.

ONLINE SOURCES:

Barlow, John (1996) 'Declaration of Independence of Cyberspace', Electronic Frontier Foundation, https://www.eff.org/cyberspace-independence, 08.02.1996, accessed 08.03.2020.

Drewer, Daniel and Ellermann, Jan (2012) 'Europol's data protection framework as an asset in the fight against cybercrime', Europol https://www.europol.europa.eu/publications-documents/europols-data-protection-framework-asset-in-fight-against-cybercrime, 19.11.2012, accessed 08.03.2020.

Survey requested by the European Commission, Directorate-General for Migration and Home Affairs and co-ordinated by the Directorate-General for Communication, Europeans' Attitudes Towards Internet Security, Eurobarometer (2019) https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2207 March 2019, accessed 08.03.2020.

Martin Russell (2018)'EU Sanctions: A Key Foreign and Security Policy Instrument',European Parliamentary Research Service, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282018%29621870, May 2018, accessed 08.03.2020.

EU Sanctions Map (2019) https://www.sanctionsmap.eu, 05.12.2019, accessed on 08.03.2020.

Portela, Clara (2019) 'The Spread of Horizontal Sanctions' https://www.ceps.eu/the-spread-of-horizontal-sanctions/ 07.03.2019 accessed 08.03.2020.

Tsagourias, Nicholas (2019) 'Electoral Cyber Interference Self Determination and the Principle of Non-Intervention in Cyberspace' Blog of the European Journal of International Law, https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/ 26.08.2019

accessed: 08.03.2020.

Korff, Douwe (2013) 'Note on European and International law on transnational surveillance prepared for the Civil Liberties Committee of the European Parliament' http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf 23 August 2013, accessed 08.03.2020.

Electronic Privacy Information Center (2005) 'Statement on Council of Europe Cybercrime Convention Treaty' https://www.epic.org/privacy/intl/ccc.html 16.12.2005, accessed: 08.03.2020.

Council of Europe (2019), 'Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime', https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. 10.12.2019, accessed 08.03.2020.

Gercke, Marco (2012) 'International Telecommunication Union: Understanding Cybercrime: Phenomena, Challenges and Legal Reponses', http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, September 2012, accessed: 08.03.2020.

The European Data Protection Supervisor (2013) 'Opinion of the European Data Protection Supervisor on the Cyber Security Strategy and Directive' https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC, 14.06.2013, accessed 08.03.2020.

Korff, Douwe (2014) 'Council of Europe - *The Rule of Law on the Internet and in the Wider Digital World Issue Paper*' https://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf 23.12.2014, accessed 08.03.2020.

Legal Opinion (2019) 'Legal Opinion on Budapest Cybercrime Convention: use of disconnection clause in Second Additional Protocol to the Council of Europe Convention

on Cybercrime' https://www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercri-1 29.04.2019, accessed 08.03.2020

Nielsen, Nikolaj (2012) 'EU cybercrime chief fears massive proliferation' https://euobserver.com/justice/117569 18.09.2012, accessed 08.03.2020.

WORKING PAPERS:

Fahey, Elaine, Odermatt, Jed and O'Loughlin, Elisabeth (2019) 'Whose Global law?: Comparative, Regional and Cyber Approaches to Law-Making', City Law School (CLS) Research Paper: No. 2019/02, http://openaccess.city.ac.uk/id/eprint/22706/1/Whose%20Global%20Law%20CLS%20WPS%202019%202.pdf,August 2019, accessed 08.03.2020.

LEGISLATION:

The Treaty of the European Union

Article 21

The Treaty on the Functioning of the European Union

Article 83

Article 82

Article 114