University of Amsterdam

The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security

Elaine Fahey

Amsterdam Law School Legal Studies Research Paper No. 2014-05

Amsterdam Centre for European Law and Governance Research Paper No. 2014-02

Postnational Rulemaking Working Paper No. 2014-01

THE EU'S CYBERCRIME AND CYBER-SECURITY RULE-MAKING: MAPPING THE INTERNAL AND EXTERNAL DIMENSIONS OF EU SECURITY

Forthcoming European Journal of Risk Regulation, vol 1, 2014

Dr. Elaine Fahey

Amsterdam Centre for European Law & Governance (ACELG), University of Amsterdam, Netherlands

INTRODUCTION

The traditional character of EU risk regulation has been to carve up discrete manageable segments, where risk is narrowly construed in single instruments.[1] While scholarship on risk regulation has sought to look beyond sectoral lines at EU policy, large-scale risk regulation remains distinctive.[2] EU Security as such a category impacts significantly upon individuals and generates many questions of the rule of law, legal certainty and fundamental rights. These are not always central concerns for EU risk regulation, especially given that EU risk regulation has sought to draw close correlations between EU risk and market regulation. Nonetheless, to the extent that risk regulation is 'Janus-headed', it necessitates both inwards and outwards-facing analysis of its subjects and objects. It often requires taking into account external and internal limitations of institutional environments and its actors. The relationship between internal and external security policies of the EU is both a descriptive and normative challenge, as much as it is for the regulation of risk.[3] For example, the EU's Internal Security Strategy aims to target the most urgent security threats facing Europe, such as organised crime, terrorism, cybercrime, the management of EU external borders and civil disasters-seemingly 'outwards-in',[4] while the 'European Security Model' outlines an interdependence between internal and external security in establishing a 'global security' approach with third countries.[5] There is thus a descriptive challenge of deciphering what is external versus internal as much as a normative challenge concerning their inter-relationship. This phenomenon is evident in EU rule-making in the area of cyber policies, as a contemporary casestudy of the process of rule-making in both internal and external security as well as providing an insight into their specific relationship in its formulation and regulation of risk. Cyber regulation inherently necessitates multi-level risk regulation, employing international

[1] Veerle Heyvaert, "Governing Climate Change. Towards a New Paradigm for Risk Regulation," 74(6) *The Modern Law Review* (2011), pp. 817-844, at p. 823.

[2] See, most famously, Francois Ewald, "Two Infinities of Risk" in Brian Massumo (ed.), *The Politics of Everyday Fear* (Minneapolis MN: University of Minneapolis Press, 1993) pp. 221-228; Massimo Fichera and Jens Kremer, (eds.) *Law and Security in Europe: Reconsidering the Security Constitution* (Cambridge: Intersentia, 2013), especially Ch. 7. Cf. As a result, see its 'absence' from 'highly effective' risk-regulation, e.g., Julia Black and Robert Baldwin, "Really responsive risk-based regulation," 32 (2) *Law & Policy* (2010), 181-213.

[3] See Florian Trauner "The internal-external security nexus: more coherence under Lisbon?" (EUISS Occasional Paper No 89, March 2011), available at <http://www.iss.europa.eu/uploads/media/op89_The_internal-external_security_nexus.pdf> (last accessed on 25 November 2013); Florian Trauner and Helena Carrapio, "The external dimension of EU justice and home affairs after the Lisbon Treaty: analysing the dynamics of expansion and diversification", 17 *European Foreign Affairs Review* (2012), 5.

[4] "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe," COM(2010)673 final.

[5] "Towards a European Security Model," Council doc 5842/2/10, 2.

and supranational components and local enforcement. It is thus readily portrayed as fragmentary, multi-sourced and ostensibly unfocussed not least because of its external and internal components but also because it involves new and emerging technologies and *restrictive* regulation.[6] The pre-emption of security risk based upon inadequate assessments of internal and external risk continue to represent a major challenge for the regulation of EU security.[7]

At the end of the life-cycle of the Stockholm Programme, the governing policy document of the EU's Area of Freedom, Security and Justice (AFSJ),[8] a Cyber Security Strategy for the EU has been unveiled, along with a supporting Directive and also a Cybercrime Directive.[9] It purports to launch an EU rule-making process, trailing cooperation by the EU with the US in cybercrime and cyber-security in existence for over two years.[10] And even though modernisation of an EU cybercrime law or any form of over-arching cybercrime policy has only recently materialised, a new 'quasi-institution' had already been created in advance.[11] The absence of and consequent publicised delay in creating an EU cyber framework was the subject of much critique, inside and outside the EU institutions, despite an asserted 'rising incidence' of cyber-attacks and espionage.[12] The link between the EU's external and internal rule-making in cybercrime and cyber security is explicit in the rule-making process itself. For example, the implementation of the EU Internal Security Strategy explicitly references the success and effectiveness of the EU-US cybercrime and Cyber Security Working Group (WGCC) as a reason to pursue EU internal cybercrime rule-making.[13] The EU's Cyber Security Strategy similarly places emphasis upon the US as the EU's lead partner.[14]

There is a specific relationship between the taxonomy of cybercrime and cyber security and the regulation of cyber risk. Questions of its taxonomy presuppose particular commitments to the rule of law and fundamental rights, as well as the character of the regulatory processes and the existence of particular risks. The taxonomy or definitional separation of cybercrime from cyber-security in rule-making is widely criticised and apparent in many legal orders and

[6] Julia Black "Decentring regulation: understanding the role of regulation and self regulation in a "post-regulatory" world," 54 (1) *Current Legal* Problems (2001), pp. 103-146.
[7] Marieke de Goede, "The politics of preemption and the War on Terror in Europe" (2008) 14(1) *European Journal of International Relations,* pp. 161-18, e.g. if institutionalised through listing, alerts or networks.
[8] The Stockholm programme — an open and secure Europe serving and Protecting citizens, OJ 2010 C 115/01.
[9] *Cyber-security Strategy of the European Union: An Open, Safe and Secure Cyberspace* JOIN(2013)1final, Brussels, 7 February 2013. It was met with calls for its urgent implementation by defence officials: see Council doc 7847/13. The Directives are analysed in more detail in S. 1.
[10] EU-US Summit, Joint Statement, Council doc 16726/10, p. 3; Presidency Conclusions of the cybercrime Conference Budapest Conclusions Budapest, 13 April 2011.
[11] The EU Cybercrime Centre, based within an existing agency, Europol ("EC3"): "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre," COM(2012) 140.
[12] For e.g., "Parliament demands single EU voice on cyber-security" *EUObserver.com*, 13 June 2012. Contrariwise, attacks against the Commission and the EEAS in 2011 resulted in cyber-security reportedly being considered as a priority by the then Polish, Danish and Cypriot Trio of Presidencies of the Council.
[13] "First Annual Report on the implementation of the EU Internal Security Strategy," COM(2011)790; "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe," COM(2010) 673 final.
[14] Cyber Security Strategy, *supra* note 9, 15.

systems.[15] But it is usually of more concern to legal rather than other scholarship on rule of law and fundamental rights grounds. The Council of the EU has decided that cybercrime is the more pertinent of the two concepts in order to focus the regulatory process.[16] A comprehensive legal definition of 'cybercrime' for EU law is not yet found in secondary law. Instead, the content of the Council of Europe Convention on cybercrime, i.e. understood here as external norms, is proposed to form the basis for EU rule-making in cyber policies, internally *and* externally. [17] Conceptually, cybercrime may be defined both narrowly, to include offences against computer data and systems but also more broadly, to include offences committed with the help of computer data and systems.[18] By contrast, cyber-security usually relates to four major societal threats- crime, cyberwar, cyber terrorism and espionage.[19] The Council of Europe Convention adopts a broad perspective on cybercrime but is much criticised for its overbroad content,[20] its lack of provision for cross-border enforcement and its obligations imposed upon Internet Service Providers[21] and it does not purport to regulate cyber security. Nonetheless, it is the most far-reaching multilateral agreement on cybercrime in existence, purporting to harmonise national legislation procedurally and substantively, its suitability as a pan-Europe source of regulation may be questioned. Its relative 'age' raises the question as to whether its view of risk regulation, its empirical basis and the exponential rise in use of the internet since its enactment has rendered outdated. As a result, the failure of many EU Member States to ratify it in tandem with a massive change of EU competences in the field since its enactment makes its centrality to the rule-making process somewhat unconvincing.[22] The reduction of *cybercrime* has been prioritised as a regulatory goal for the EU in its rule-making on cybercrime and cyber security.[23] This ostensibly entails the adoption of a 'law and order' approach, one which

[15] E.g. David Thaw, "The Efficacy of Cybersecurity Regulation", 30 *Ga. St. U. L. Rev*. (forthcoming), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298205. See Susan Brenner and Bert-Jaan Koops (eds.), *Cybercrime and Jurisdiction: A Global Survey* (The Hague: Asser Press, 2006).

[16] Informal Justice and Home Affairs Ministers" Meeting, Cyber Security issues, Discussion paper, (18-19 July 2013, Vilnius.

[17] European Treaty Series (ETS), No. 185, Budapest, 23 September 2001.

[18] See Jonathan Clough *Principles of Cybercrime* (Cambridge: Cambridge University Press, 2010).

[19] Joseph Nye, "Cyber Power", Belfer Center for Science and International Affairs Working Paper, May 2010, at p. 16, available on the internet at <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf> (last accessed on 25 November 2013).

[20] It categorises cybercrime in four sets of categories in Articles 2-13 thereof: Offences against the confidentiality, integrity and availability of computer data, computer related offences, content-related offences and offences related to intellectual property rights. It is applicable to any crimes for which it is necessary it collect evidence in electronic form, i.e. not just to cybercrimes: Art. 14(2)(c).

[21] Although, on its enforcement provisions, it is argued that the Convention can be read to permit direct interaction between law enforcement and ISPs. This was the subject of review by the Council of Europe in 2013; see also Jack Goldsmith "the Internet and the Legitimacy of Remote Cross-Border Searches" *University of Chicago Law School Public Law and Legal Theory Working Paper* No. 16; 1 *Chicago Legal Forum* (2001), 103; Maria Grazie Porcedda, "Transatlantic Approaches to cyber-security and cybercrime," in *The EU-US Security and Justice Agenda in Action*, Patryk Pawlak (ed), (EUISS Chaillot Paper, No. 127, 30 December 2011), <http://www.iss.europa.eu/uploads/media/cp127_EU-US_security_justice_agenda.pdf> (last accessed on 25 November 2013).

[22] Opinion of the European Data Protection Supervisor of 14 June 2013 on the Cyber Security Strategy and Directive, at <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC> (last accessed 25 November 2013).

[23] Informal Justice and Home Affairs Ministers" Meeting, *supra* note 16.

heightens the need for a holistic, systematic and transparent framework for the regulation of cyber policies.

There are major regulatory advantages in developing in particular the *external* component of cyber regulation. Rule-making between the EU and US legal orders in security has a broad range of regulatory sub-components, including to enable EU-US trade, spurring global rule-making for the internet and combatting cyber-related criminal activities. In turn, it has clear implications for data protection and privacy which featured initially only *tangentially* in the EU's cyber rule-making with the US. The outbreak of the NSA surveillance saga in the midst of the rule-making processes has operated to place EU citizens fundamental rights and data protection centrally in *all* rule-making of the EU with the US. It also operated to cause the European Parliament to vociferously call into question a range of existing EU-US security agreements, i.e. external EU security.[24] However, the NSA surveillance has also operated paradoxically re-ignite EU-US negotiations on a data protection framework and alter the regulatory components and trade-offs of this external rule-making.[25]

It is argued here that it is noteworthy that although the EU gives primacy to external norms, i.e. the Council of Europe Convention, in both its contemporary internal and external rule-making in security, it produces very different regulatory results despite the commonality of the norms used. Nor has it produced particularly comprehensive, systematic or conceptually transparent processes in either forum. Differences between external and internal rule-making processes may be explicable because of the on-going 'regularisation' of the AFSJ into ordinary EU law. On the other hand, the evolution of EU Criminal law suggests that such a framework should be more holistic, sophisticated and rights dependant. However, the character of EU internal regulation in particular necessitates a schema to formulate and regulate risk holistically, which does not yet exist.

Accordingly, this account examines how the distinction between external and internal security in contemporary EU law manifests itself in large-scale risk regulation and in particular, how the EU relies upon external norms to regulate risk. The account also maps the evolution of the rule-making processes themselves. Section I examines the evolution of the instruments of the EU's internal regulation of Cyber Security and Cybercrime in the EU Cyber Strategy, its supporting Directive along with the development of a Cybercrime Directive. Section II examines the form of risk involved in the development of EU internal rule-making, while Section III assesses rule-making between the EU and US in cybercrime and cyber security and its relationship to internal EU rule-making, as well its regulatory impact. Finally, the overall character of EU internal cyber regulation is considered Section IV, focussing upon its comparative structures and content as a regulatory enterprise, followed by Conclusions.

[24] European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)).
[25] See Joint Press Statement following EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, Council 16418/13, 18 November, 2013.

I. MAPPING EU INTERNAL RULE-MAKING

The account begins by mapping the *definitional* nature of risk in the regulatory components and legal tools of EU internal rule-making in both cybercrime and cyber security, prior to conducting an analysis of the *substantive formulation of risk* within the regulatory structure. The account thus examines, firstly, the nature of EU cyber security, as the 'first in time' legislative component of EU cyber regulation.

I.1. *The EU Cyber Security Strategy*

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.[26] 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.'[27] 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.[28] 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.[29] 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.[30] Its definition of cybercrime has generated

[26] E.g. Commission Communication "Network and Information Security; proposal for a European Policy Approach," COM(2001)298; "Strategy for a Secure Information Society," COM(2006) 251; Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience COM(2009) 14; Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L 345/75.
[27] Cyber Security Strategy *supra* note 9, at 3.
[28] E.g. *Talinn Manual on the International Law applicable to Cyber-warfare* (Cambridge: Cambridge University Press, 2013).
[29] The EU Counterterrorism Coordinator is a participant in the EU-US cooperation.
[30] p. 3, i.e. where computers and information systems are involved either as a primary tool or primary target, comprising traditional offences, content-related offences and offences unique to computers and information systems.

infelicities in its taxonomy, infelicities that have generated much critique and which impact upon its overall formulation of an over-arching framework for risk.[31]

The Strategy purports to pursue five strategic priority areas which include firstly, 'achieving cyber resilience' is to be pursued by legislation, in particular by means of a Directive on Networks and Information Security (NIS), discussed in detail next. An NIS would require Member States to designate at national level competent authorities for NIS, who would in turn cooperate with each other at EU level and private actors would also report to NIS competent authorities. Soft law measures including awareness-raising exercises, key elements of transatlantic cooperation, form part of this specific first strategic target, similar to the EU-US WGCC, discussed above in S.III.[32] In respect of the second priority, that of 'drastically reducing cybercrime,' it is this priority which has become the focus of EU rule-making both internally and externally. The Strategy urges Member States who had not yet ratified the Council of Europe Cybercrime Convention to do so, also similar to the EU-US WGCC. In respect of the third priority, that of 'developing cyber defence policy and capabilities under the Common Security and Defence Policy,' it provides that the High Representative would invite the Member States and the European Defence Agency to develop an EU cyber defence policy, seeking to complement the work of North Atlantic Treaty Organisation (NATO). As regards the fourth priority, the development of the industrial and technological resources for cyber-security, it sought to promote a single market for cyber-security products, including voluntary EU certification and public-private platforms involving NIS solutions would be evolved.[33] As regards the fifth priority, the development of a 'coherent international' cyberspace policy for the EU, the EU would work more closely with International organisations such as the Council of Europe, the OECD, NATO, ASEAN,[34] in addition to its cooperation with the US, described as 'particularly important' therein. Nevertheless, the Strategy states that while the EU would launch international initiatives to promote global cooperation, *it would not call for the creation of new international legal instruments*.[35] Instead, the Convention would remain the model for drafting *national* cybercrime legislation and would also be a model for international cooperation. As regards 'roles and responsibilities', the Strategy explicitly states that EU 'supervision' is not the answer because cyber incidents do not stop at the borders of the digital economy and society.[36] Institutionally, the Strategy envisions overall a division of labour between the areas of (1) Network and Information Systems (NIS), (2) law enforcement and (3) defence,[37] involving a vast range of actors but notably excluding national data protection authorities.

[31] See Opinion of the European Data Protection Supervisor, *supra* note 22.
[32] At p. 7.
[33] At p. 13.
[34] But notably not including the UN.
[35] Emphasis supplied, at p. 15.
[36] P. 17.
[37] The Commission European Network and Information Security Agency (ENISA), the Computer Emergency Response Team, (CERT EU), national networks of competent authorities responsible for NIS, and "EP3R", the entity which partners the public and private sector (i.e. NIS globally), EC3, the European Police College (CEPOL) and Eurojust (i.e. law enforcement); the EEAS and the European Defence Agency (i.e. defence), CERT, NIS Competent Authorities (i.e. NIS), cybercrime units (i.e. national law enforcement) and National defence and security authorities (i.e. defence).

Prior to analyzing the substantive formulation of risk within the Strategy, the account turns next to examine the Directive introduced to support the Strategy.

I. 2. *Legal Tools of EU Rule-Making in cyber security: obligations upon market operators*

While the Strategy is partially-centred upon defence, it is based upon a minimum harmonisation Directive, which proposes to provide for a high common level of Network and Information Security across the Union (NIS).[38] It purports to establish a cooperative network mechanism for information exchange and to impose binding obligations upon public administrators and market operators of critical infrastructures. Competent national authorities are to be designated at national level,[39] which will be the focal point for cross-border cooperation, assisted by CERT teams in the Member States.[40] These authorities and the Commission will form a so-called permanent network for cooperation, exchanging and circulating information.[41] Moreover, national authorities will monitor the application of the Directive at national level and provide, similar to the Commission, early warnings on certain types of incidents, which may result in all competent authorities having to agree a coordinated response. Where an incident emerges, the Commission may adopt delegated acts.

The legal basis for the Directive is in Art. 114 TFEU, in the form of a minimum harmonisation Directive and this specific choice of legal basis merits attention. The Directive provides that divergences in NIS regulations in the Member States would constitute obstacles to trade in the event of no EU action being taken, resulting in the objectives being better achieved at EU level.[42] The NIS is thus connected to cross-border trade in so far as the Strategy contends that the resilience of information systems is essential to the smooth functioning of the internal market. Nonetheless, the nature of the legal obligations created for the national authorities in the Directive is 'light-touch' harmonisation, i.e. through information exchange networks.

The Directive places very onerous obligations upon national administrators and public network operators to identify and manage risk. Article 14(2) requires 'market operators' and public administrations to notify the NIS competent authority of 'incidents' which have a 'significant' impact on the security of the core services they provide.[43] However, as the European Data Protection Supervisor has stated, the definition of 'market operator' is insufficiently clear as expressed in Annex II, as is the definition of 'incident' and 'significant impact'.[44] Similarly, their obligations to respect EU data protection law appears equally

[38] Directive concerning measures to ensure a high common level of network and information security across the Union: COM(2013) 48 final.
[39] Art. 6.
[40] The latter pursuant to Art. 7, said to act under the supervision of the competent authority.
[41] Art. 8.
[42] COM(2013) 48, at pp. 8-9.
[43] Small and medium sized enterprises are excluded: Art. 14(8); the obligations only apply *within* the EU. See Annex II. This contrasts with the extensive *voluntary* programme provided for in the recent US Cybersecurity Executive Order: see Section III below.
[44] He criticises in particular its compliance with data protection obligations (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

uncertain. The use of Article 114 TFEU poses an interesting contrast with the EU's external rule-making with the US discussed in Section III, where neither obstacles to trade or trade conflicts nor obligations on market operators form any explicit relevance in the rule-making. On the one hand, this could be said to demonstrate the lack of symmetry between the internal and external rule-making. On the other hand, trade conflicts and obligations on market operators largely constitute questions relating to enforcement which are conducted at local level, rendering their absence from external rule-making justifiable.

Another legal tool of note used in the Cyber Security Strategy is the 'mainstreaming' of cyber-security policies into *inter alia* EU External Relations law and policy.[45] 'Mainstreaming' constitutes a complex fusion between a policy instrument, a rule-making strategy and norm embedded within EU law and policy.[46] Its actual success or relevance to all areas of EU policy is perhaps patchy after over a decade of its existence, given the unlikelihood of producing practical results if 'everything' must be taken into account. The deployment of mainstreaming as a legal tool is revealing as it constitutes an explicit effort to engage with the amorphous divide between external and internal aspects of security rule-making. In the end, however, it is difficult to view mainstreaming as anything other than a convoluted tool. One may say that this in fact exposes well the challenges of marrying the external and internal in rule-making, especially one based upon a commitment to the primacy of external norms.

The account next examines the content of EU internal rule-making in cybercrime.

I. 3. *Cybercrime: Third Generation EU Criminal law*

The substantive legal content of EU *cybercrime* law has evolved in a piecemeal form, amongst a plethora of legal instruments, actual and proposed, and has been conceived apart from cyber-security. EU cybercrime 'law' per se is a relatively recent legislative phenomenon, ostensibly beginning with the Framework Decision on attacks against information systems in 2005. [47] However, there is still no commonly agreed definition of cybercrime in EU law or no specific cybercrime Directive. Instead, the ratification of the Convention has been advocated by most EU institutions for some time, entailing that it has consistently prioritised external norms in its rule-making.[48] The Framework Decision

---

of personal data and on the free movement of such data) and the obligations incumbent upon microenterprises: Opinion *supra* note 22, 16-17.

[45] P. 15.

[46] Specifically in the area of EU Gender Equality law, whereby Art. 8 TFEU mandates the integration and promotion of equality between men and women in all areas of EU policy. See also the mainstreaming of basic values into the legislative process. It is a central tool of the European Pact for Gender Equality 2011-2020 and the Strategy for Equality between Women and Men 2010-2015. See Laurent Pech, "Rule of Law as a Guiding Principle of the European Union's External Action," 2012/3 CLEER Working Paper, available on the internet at <http://www.asser.nl/default.aspx?site_id=26&level1=14467&level2=14468&level3=&textid=40218> (last accessed on 25 November 2013).

[47] Council Framework Decision 2005/22/JHA of 24 February 2005 on attacks against information systems, OJ 2005 L 69/ 67.

[48] See for e.g., Report from the Commission to the Council based on Art. 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM(2008) 448 final; Council Conclusions

provided for the criminalisation of online and offline conduct, along with serious penalties and jurisdictional rules, focussing upon individual wrongdoing, but constituting only a minimal or limited harmonisation of laws, so much so that several Member States sought to rely upon existing legislation in place by way of satisfaction of the approximation requirements, yet generating some level of regulatory disparities which the Commission expressed its dissatisfaction with.[49] Later policy sought a broader policy framework for cybercrime including increased law enforcement cooperation, public-private partnerships and international cooperation, which eventually resulted in a proposal to repeal and update the provisions of the Framework Decision.

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.[50] It purports to criminalise access to systems, systems 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.[51] 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.[52] 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 risk 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 provision 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

concerning an Action Plan to implement the concerted strategy to combat cybercrime, 3010th General Affairs Council meeting (Luxembourg, 26 April 2010).

[49] See Valsamis Mitsilegas, "Area of Freedom, Security and Justice, including Information Society Issues" in Julia Laffranque (ed.), *FIDE Congress XXV Reports: General Report*, 40-41, (Talinn, Estonia, 2012); Commission Communication, "*Towards a general policy on the fight against cybercrime,"* COM(2007) 267 final

[50] Botnets are a network of computers infected by a virus which can be activated without the users knowledge to attack information systems on a large scale. See 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 2013, 2013 OJ 218/8. See its previous draft: COM(2010)517 final.

[51] The UK has stated that it will opt-into the Directive, on the basis that the Directive explicitly states that it will not to change existing EU competence. See "United Kingdom Report", in Mitsilegas (ed.) "Area of Freedom, Security and Justice", *supra* note 49 at 655-681. See also European Parliament LIBE briefing, June 2012 2010/0273;

[52] "Cybercrime: EU citizens concerned by security of personal information and online payments," IP/12/751, 9 July 2012. On so-called post-Lisbon Third Generation EU Criminal law and its relationship to the internal market, see Massimo Fichera, "Criminal Law beyond the State: The European Model," 19 *European Law Journal* (2013),174-200

formulation of cybercrime law which has yet to materialise and emphasises the non-holistic vision of risk, as regards its instruments.

Turning then to the infrastructure of EU cybercrime,[53] the establishment of a new dedicated Cybercrime Centre was later proposed by the Council and became a key component of the EU Internal Security Strategy and also the implementation of the Stockholm Programme.[54] An EU 'Cybercrime Centre' (the so-called 'EC3') was officially launched in 2013, which is based *within* Europol ostensibly as a 'desk' thereof.[55] It is a deliberate structural addition to the AFSJ *within* an agency, portrayed as desired by Europol itself, when much effort is being spent upon 'communautarising' AFSJ agencies, not least Europol itself.[56] This renders its purported 'quasi-institutionalisation' difficult to comprehend.[57] The Centre is stated to have four core functions, acting as a European focal point in fighting cybercrime, operationally fusing information and informing Member States of threats. The innovation of the Centre was intended to be as to the latter, that it would adopt a 'cross-community approach,' i.e. to exchange information beyond the law enforcement community, would develop a common standard for cybercrime reporting and would assume the collective voice of cybercrime investigation. However, these functions largely constitute 'information exchange', overlapping with Europol's current mandate.[58] Its establishment *prior* to the development of an overarching legal infrastructure in cybercrime and cyber-security provides evidence of the piecemeal evolution of EU internal policies to regulate cyber risk.

This leads to a more substantive discussion of the nature of risk within the EU's internal rule-making.

---

[53] The Council in 2008 began plans to institutionalise cybercrime in EU law with the development of so-called "platforms", a national alert "platform" and a European "platform", convergence points of national platforms within the competence of Europol: Justice and Home Affairs Council Conclusions, Council doc 14667/08, p. 8-10. See draft Council Conclusions on a Concerted Work Strategy and Practice Measures against cybercrime Council doc. 15569/08.

[54] See Action Plan Implementing the Stockholm Programme, COM(2010)171 final, at p. 34.

[55] See *supra* note 11, at pp. 3. See its website: <https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837> (last visited 25 November 2013). It is not a "functionally autonomous" body similar to the European External Action Service.

[56] For e.g. as to Europol, Eurojust, ENISA and a European Public Prosecutor's Office, pursuant to Articles 85 and 86 TFEU. See Madalina Busuioc, *European Agencies: Law and Practices of Accountability* (Oxford: Oxford University Press, 2013). The status of such entities is subject to change: See Draft Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final. To similar effect, see Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) COM(2013) 535 Others the subject of modernization include ENISA, established by Council Regulation (EC) 460/2004 and see. COM(2010) 521. See also the proposal for a European Public Prosecutors Office: COM(2013)0534 final.

[57] "Europol wants to host EU cybercrime centre," *EUObserver.com*, 14 November 2011. At the launch of the Centre, Europol was asserted to have previously lacked sufficient resources to gather information from a broad range of sources and to have lacked the capacity to deal with requests from law enforcements agencies, the judiciary and the private sector.

[58] A point not considered in much detail in the Feasibility Study for a European Cybercrime Centre, RAND Corporation, 2012, prepared for the European Commission. Notably, Interpol representatives with sit on its board and Interpol will reportedly launch its own Cybercentre in 2015. While non-duplication of EU rules with international rules are aims of the EU, international cooperation is a function of the Centre.

II. THE CHARACTER OF RISK IN INTERNAL EU RULE-MAKING

The regulation of risk in the Cyber Security Strategy, its related Directive and the Information Systems Directive present three distinct issues for consideration:- namely, the problematisation of EU 'cyber risk' and its management in cyber regulation, including its incidence to warrant regulation; secondly, its relationship to the multi-stakeholder construction of the regulatory paradigm in EU law and policy and, thirdly, the place of rights-based understandings of cyber regulation, for example, data protection and privacy.

First, the problematisation of cybercrime as a regulatory subject is more acutely disputed than cyber security, although they overlap considerably even in such literature. As Wall states, there is much confusion about the risks posed by cybercrime and the consensus that it exists.[59] Few national level prosecutions, fuelled 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. The rising incidence of both cybercrime and security risks are depicted in the Strategy as the reason to warrant regulation qua criminalisation. Such an assertion of 'incidence' relies heavily upon the thesis as made by, for example, ENISA arguing that cybercrime is rarely reported as a chronically underreported crime, with a significant impact upon individual uers.[60] It is an assertion as to risk regulation which appears empirically untestable and relies on this absence of knowledge for far-reaching regulatory choices. However, the knowledge relied upon in the EU Strategy and the Directive for the existence of risk emanates from an extremely limited and disparate range of asserted incidents, despite accepting a rising incidence of harm- so limited in fact, that little effort is made in the formulation of harm to actually distinguish acts of nature (eg flooding), external devices and actual attacks on IT infrastructures.[61] In its launch of the Strategy and Directive, the Commission described 'facts' about the existence cybersecurity drawn from *inter alia* Symantec and McAfee studies, two leading market actors in a specific sector with specific financial interests in the establishment of cyber harm, as well as a Eurobarometer poll, Eurostat figures and data from the World Economic Forum.[62] The Commission outlined as a factual assertion that there were an estimated 150,000 computer viruses in circulation every day, although not specifying the global nature of the harms or the relevance of the EU territory to the risk asserted to exist. Similarly, the data of the World Economic Forum or Symantec and McAfee do not in reality establish the existence of harm to warrant the *EU* to

[59] David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, 2007); See also David Wall, "Cybercrime and the Culture of Fear: Social Science fiction(s) and the production of knowledge about cybercrime," 11(6) *Information, Communications and Society* (2008), 861-884, writing of a "series of myths": at 862.

[60] "Cyber security incidents rarely reported: EU Agency" *Euractiv*, 27 August 2012, citing an ENISA report ('Cyber Incident Reporting (August 2012)), mentioning 51 notifications of "large" incidents by regulators. On ENISA, see *supra* note 56.

[61] "Cybersecurity incidents are increasing at an alarming pace": Strategy, p. 3; Impact Assessment Strasbourg, 7 February 2013, SWD(2013) 32 final, at 12-14. Cf Annegret Bendiek and Andrew Porter, "European Cyber Security Policy within a Global Multistakeholder Structure," 18 *European Foreign Affairs Review* (2013), 155-180.

[62] EU Cybersecurity plan to protect open internet and online freedom and opportunity, IP/13/94, 7 February 2013.

regulate and instead appear strikingly non-specific formulations of the incidence of risk. The LIBE Committee of the European Parliament has condemned the over-criminalisation of cybercrime, as much as its disproportionate over-criminalisation in the Cybercrime Directive, in light of its ineffectiveness.[63] Yet it is not a viewpoint shared across the institutions. For example, the character of cybercrime as a daily nuisance and potential threat has been invoked by the Commission to warrant higher cybercrime penalties.[64] The impetus towards criminalisation has been fuelled by those seeking urgent implementation of the Strategy's defensive components, still in the absence of a defined basis of the specific risk to be defended against. As a result, the problematisation of cyber risk appears inadequate, under-theorised and not ripe for a large-scale regulatory framework.

A second consideration as to the character of cyber risk is that the regulatory structure of the Strategy problematizes it as a multi-stakeholder exercise. It emphasises the emergent actor structure of cybersecurity, which transcends national, international, transnational and private actors, both internally *and* externally.[65] It is of course essential to have 'stakeholders' involved in the construction of this form of institutional design, given that industry, users and specialist stakeholders are often best placed to identify new risks. There are many means to enrol such actors within regulatory systems as part of management and service delivery, which reflects broader questions of the fragmentation and hybridity of governance.[66] It is cost-effective to enrol industry into the enforcement of low-risk forms of regulation. But whether it is adequate as a regulatory framework for higher-risk forms of regulation is not so certain. Such a framework may become opaque if the firms do not disclose their risk management regimes and may not reveal new risks. The need to have so many partners involved may be explained as part of the knowledge-building of rule-making in a complex field, although its complexity raises questions as to its efficacy, as much as its transparency and institutional design. Sharing powers and tasks across actors within risk regulatory regimes may reduce its effectiveness.[67] This remains an acute challenge for the formulation of risk within the Strategy and the NIS Directive. One may remark upon the surprisingly small number of stakeholders consulted by the Commission as to the NIS despite the legal obligations of the end product, which calls into question how 'multi-actor' the framework is in reality.[68]

The Strategy and NIS Directive appear to consider cyber regulation less systematically or holistically than comparable multi-stakeholder regulatory exercises, for example, in EU banking and finance regulation instruments, discussed further below. In this regard, regulation is proceeding in the absence of quantifiable harms or an empirically testable and consistent

[63] See *supra* note 51.
[64] DG Home Affairs, European Commission, on "Cybercrime", http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm
[65] See Bendiek and Porter "European Cyber Security Policy", *supra* note 61.
[66] E.g. Julia Black, 'Enrolling actors in regulatory systems: examples from UK financial services regulation," *Public Law* (2003), pp. 63-91.
[67] See generally Black & Baldwin, "Really responsive risk-regulation", *supra* note 2.
[68] See COM(2013) 48 final SWD(2013) 32 final, 2. "EP3R" (see *supra* note 37*)* is described as the device where the private sector was consulted and a public online and written consultation conducted yielded 179 responses, including from public authorities and NGO"s: p. 7. The manner of portraying this procedure is not particularly explicit or detailed.

definitions of cybercrime and cyber security. In turn, the dominance of the multi-stakeholder approach appears to lack less legitimacy and accountability. From the perspective of national authorities, Member State administrative bodies participating in EU-wide networks, with or without EU supervision are not a new phenomenon of EU law and policy, they are more prevalent in the area of utilities regulations, fundamental rights or data protection, where *precise* obligations have been imposed upon the Member States within an over-arching framework.[69] From the perspective of private actors, industry and/ or market operators, the use of Art. 114 TFEU here seems to be deployed disproportionately- i.e. oriented towards the regulatory objective of placing a significant burden upon private operators within a less than holistic framework.

The third substantive consideration as regards the character of risk is that the Strategy and its Directive expressly propose to create an open internet and online forum for freedom of expression. However, one can observe that their most telling omission in its regulatory infrastructure is in respect of data protection and citizen rights, both substantively and in its institutional infrastructure. It makes, for example, no provision for the role of Data Protection Authorities to control or police the use of data within the networks of actors collaborating in both the Strategy and Directive, as voiced by the European Data Protection Supervisor.[70] Similarly, one can note that information-sharing obligations are not couched explicitly in a 'citizen-centric' manner, instead acting as a relevant consideration 'after the fact'. In this regard, it is important to note that the Strategy was released prior to the NSA surveillance saga which has unfolded, which may yet ameliorate this concern and leads to the question of the relationship between the internal and external regulatory processes.

The account accordingly turns to examine the external rule-making of the EU with the US in the area of cybercrime and cyber security.

III. THE EU'S EXTERNAL CYBER RULE-MAKING: EU-US WORKING GROUP IN CYBERCRIME AND CYBER-SECURITY (WGCC)

Rule-making in the areas of cybercrime and cyber security between the EU and US constitutes the first major transatlantic cooperation in security a decade. It lacks the counterterrorism impetus attached to previous transatlantic cooperation.[71] It also takes place in the post-Lisbon context, after which the EU has been granted single legal personality for the EU and competence for its pursuit of the regulation of criminal law, pursuant to Article 82

[69] See Bruno De Witte, "New Institutions for Promoting Equality in Europe: Legal Transfers, National *Bricolage* and European Governance," 60 *American Journal of Comparative Law* (2013), 49, at pp. 58, fns. 28 and 29.
[70] Opinion of the European Data Protection Supervisor of 14 June 2013 on the Cyber Security Strategy and Directive, available at <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC> (last accessed 25 November 2013).
[71] See Elaine Fahey, "Law and Governance as checks and balances in Transatlantic Security," 32 *Yearbook of European Law* (2013), 1-21. See also on transatlantic rule-making, Elaine Fahey and Deirdre Curtin (eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US legal orders* (Cambridge University Press, 2014).

TFEU and Article 83 TFEU, operating as an entirely new legal background.[72] It forms a specific area of cooperation worthy of attention because of its particular relationship with internal EU rule-making in this area and its regulatory output.

While the EU-US WGCC group was established after the EU-US Summit in November 2010, the origins of this cooperation date back to the Joint EC-US Task Force on Critical Infrastructure Protection a decade earlier,[73] and at about the same time, the Council of Europe Cybercrime Convention was adopted, which now forms a central legal element of EU-US cooperation similar to the EU rule-making.[74] EU-US negotiations on a data protection framework agreement also begun in early 2010 but appear to have stalled for some time.[75] The EU-US cooperation goals are predominantly in four areas, including (1) the expansion of cyber incident management response capabilities jointly and globally, (2) to broadly engage the private sector using public-private partnerships, sharing good practices with industry and to launch a programme of joint awareness raising activities, (3) to remove child pornography from the internet and (4) to advance the international ratification of the Convention by the EU and Council of Europe Member States and to encourage pending non-European countries rapidly to become parties.[76] The first Cyber Atlantic exercise in 2011 kicked off a programme of joint cyber-attack exercises, to culminate in a fully-fledged EU-US cyber security exercise in 2014.[77] The activities of the WGCC were to be conducted in four expert sub-groups consistent with the four fields of work of the WGCC,[78] which include a broad network of governmental, agency and institutional actors. Public workshops and meetings have been conducted in 2011 and 2012 as part of the rule-making exercise and one of the hallmarks of this cooperation might be said to be its efforts to initiate transparency and public participation, despite the highly diverse range of stakeholders involved in cyber policies.[79]

The WGCC is expressed to be an 'outreach' model to other countries or international organisations with similar cyber issues and from the outset, it seems apparent that the WGCC had 'global' rule-making objectives, specifically the advancement of the Council of Europe

[72] See Ester Herlin-Karnell, *The Constitutional Dimension of European Criminal Law* (Oxford: Hart, 2012).
[73] "Creating a safer Information Society by improving the security of information infrastructures and combating computer related crime": COM(2000)890 final.
[74] See Section II. It entered into force on 1 July 2004 and was drafted by the Council of Europe Member States and Canada, Japan, South Africa and the US.
[75] Until recently. See "European Commission seeks high privacy standards in EU-US data protection agreement", IP/10/609 Brussels, 26 May 2010. See the Press Release from 4 April 2013 http://www.justice.gov/opa/pr/2013/April/13-ag-382.html, of discussions between the US Attorney General and Vice-Commissioner Reding. The LIBE committee of the European Parliament was debriefed on the negotiations in February 2013: LIBE(2013)0220_1.
[76] EU-US Working Group on cyber-security and cybercrime, Concept Paper, 13 April 2011. Annex I. It set a deadline for ratification before the 10th Anniversary celebration of the Convention in 2011.
[77] See Commissioner Malmstrom, "Next step in the EU - US cooperation on Cyber security and Cybercrime" SPEECH/13/380, 30 April 2013.
[78] Concept paper, p. 6.
[79] For example, holding open workshops for a broad range of private and public actors and publishing the lists of all of the participants: available on the internet on <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/eu-us-open-workshop> (last accessed on 25 November 2013).

Convention.[80] This is an objective of EU rule-making for some time. In 2008, the European Commission suggested that its redrafting or modernisation had become unachievable yet nonetheless since then promoted both international and EU ratification.[81] The WGCC Group mentions specific countries to be 'encouraged' to become parties to the Convention, countries within and outside the EU.[82] While during 2012 and 2013 several, there were still a number EU Member States still 'resisting' ratification on various grounds at the time of writing.[83] This context emphasises how the legal objectives the EU-US cooperation are globally-oriented. Similarly, another expected goal of the EU-US cooperation includes the endorsement of EU-US 'deliverables' in cybercrime by the Internet Corporation for Assigned Names and Numbers (ICANNs), the controversial US-based organization responsible for managing and coordinating the Domain Name System (DNS), engaging in significant postnational rule-making.[84] Further evidence of the nature of the 'global' objectives of the rule-making is provided by the minutes of a 2011 meeting of EU-US Senior JHA Officials, where it was stated that the EU and US would work together in the UN to avoid dilution of the body of international law on cybercrime.[85] One may remark that the European Commission was seeking global Cyber Security policies even before its own EU-level policy had been conceived.[86] Moreover, in advance of the adoption of the Cyber Security Strategy, the European Parliament in 2012 advocated an EU framework on cyber-security, with a view to the policy being 'brought up' at G8 and G20 level.[87] The goals of the WGCC suggest that they will lead eventually to the adoption of a global-like cyber policy or at the very least, global standard-setting, through their promotion of the primacy of external norms. The ambitious nature of the globally ambitious and externally-oriented rule-making *externally* contrasts with the policies pursued by the EU *internally*, as a far more modest rule-making process. By contrast, it can be said that this internal rule-making compares less than favourably with the EU's external rule-making, appearing instead piecemeal and less ambitious, in its failure to regulate holistically, transparently and systematically.

In the same period as the publication of the EU Cyber Security Strategy, the US President signed Executive orders providing for rules on cyber-security for the US, couched in a dense framework of administrative law which accords considerable discretion to officials of the

[80] Notably, the US is not a member of the Council of Europe but took part in the drafting of the Convention and has signed and ratified it domestically: see Elaine Fahey, "On the use of law in Transatlantic Relations: Legal Dialogues Between the EU and US," 19 *European Law Journal* (forthcoming).
[81] COM(2010) 517 final, p. 2.
[82] Concept Paper, p. 4.
[83] Cf the Commission's advocacy of the Convention, emphasising how the Convention had been signed by 25 out of the 27 Member States and ratified by 15 of them: *supra* note 66. See the ratification table at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> (last accessed on 25 November 2013).
[84] WGCC Concept paper, p. 3. However, IANN appears increasingly eager to interact publicly with the internet governance community: see <http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm> (last accessed on 25 November 2013).
[85] "Summary of Conclusions of the EU-US JHA Informal Senior Officials Meeting of 25-26 July," Council doc 13228/11, p. 3.
[86] Cf "Critical Information Infrastructure Protection- Achievements and next steps: towards global cyber-security," COM (2011)163 final.
[87] "Parliament demands single EU voice on cyber-security" *supra* note 12.

Department of Homeland Security.[88] The difference in cyber security approaches between the two legal orders has been suggested to create major regularity challenges for companies operating in the EU and US with the voluntary approach to the US alleging contrasting with the compulsory approach provided for by the EU.[89] The US cyber security approach instead involves private actors at all stages of rule-making and enforcement, although the comparative study of EU and US risk regulation is frequently cautious concerning the outcomes and explanations of policy convergence and divergence.[90] The WGCC does indeed appear eclipsed by such differences in regulatory developments in the respective legal orders, although such an analysis is premature in light of other regulatory developments discussed next.

This leads to the next section, which considers the substantive impact of the EU's external security rule-making

III.1. *The Regulatory Impact of the EU-US WGCC*

Contemporary events surrounding EU-US relations suggest that the regulatory impact of the EU-US cooperation is manifold, affecting EU-US rule-making in many areas, i.e. external security, but is also relevant to EU internal security. Thus it arguably has both direct and indirect impacts of significance. Its direct regulatory impact is set to be the broad adoption of global standards on cybercrime in the guise of a Council of European Convention. Equally, the deliverables of the EU-US cooperation on internet domains are set to be adopted by ICANN and possibly then globally. As a result, this would amount to a direct regulatory result. Of course, the extent to which transatlantic rule-making is viewed as normatively legitimate remains to be seen given that ICANN has recently attempted to increase or enhance participation and transparency in its rule-making practices.[91]

There are many regulatory benefits of the EU-US cooperation, not least the avoidance of trade conflict and inter-agency disputes. There are now a historically low number of trade conflicts pending before the EU and US at the WTO,[92] yet it remains a latent issue in all transatlantic rule-making. Moreover, a regulatory advantage of the WGCC would be to avoid ineffective

---

[88] Executive Order 13636, *Improving Critical Infrastructure cybersecurity*, Federal Register 78, No. 33 (19 February 2013). See the *Comprehensive National Cybersecurity Initiative*, which employs commercial and government technology to engage in threat-based decision-making, available at <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative> (last accessed 25 November, 2013). See also *The 2013 Cyber-security Executive Order: Overview and Considerations for Change*, Congressional Research Service 7-5700 R42984 (1 March 2013).

[89] See "EU, US go separate ways on cybersecurity" *Euractiv*, 5 March, 2013; Bendiek & Porter, "European Cyber Security Policy," *supra* note 61.

[90] See more generally, Jonathan Wiener, Brendon Swedlow, James Hammitt, Michael Rogers and Peter Sand, "Better Ways to Study Regulatory Elephants," 2 *European Journal of Risk Regulation* (2013), pp. 311-319.

[91] See, for e.g., significant emphasis on the ICANN website on transparency and accountability-related activities. See http://www.icann.org/.

[92] For a recent survey of the European Parliament, see Library of the European Parliament, "Principal EU-US disputes" (22 April 2013), http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130518/LDM_BRI(2013)130518_REV1_EN.pdf.

agency-level bilateral models. For example, consider the recent Memorandum of Understanding between the Irish Data Protection Commissioner, as the data protection agency of the Member State where most global social networking sites are head quartered,[93] with the US Federal Trade Commission on the operation of the EU-US Safe Harbour Agreement.[94] The recent NSA surveillance events demonstrate the obvious inadequacies of such a bilateral model and its failings to protect citizens data, albeit in respect of a voluntary or hybrid regulatory regime.

The formulation of EU external cyber regulation with the US must be conducted so as not to create 'blind spots' of areas not within the framework. Its manifold components and externalities suggest that it may readily generate blind spots in the regulatory process. For example, the WGCC output could also be of much significance for cloud computing as a regulatory enterprise in so far as it could impact broadly upon understandings of territory, legality and cyber markets.[95] An EU-US expert working group on cloud computing was established by the Transatlantic Economic Council in 2011 which met in early 2012 and has to report to the EU-US Information Society Dialogue. However, the NSA surveillance has been mooted by a European Commissioner as a reason for Europeans not to trust US clouds and instead to build their own.[96]

One may observe that EU-US rule-making is generally very sectoral or discrete and has a heavy dependence upon contemporary political affairs for its momentum. An EU Agreement on data protection for transfers of personal data for law enforcement purposes was still actively under negotiation in early 2013. The WGCC begun its work significantly prior to the outbreak of the NSA surveillance saga. This has since then called into question a broad range of EU-US data transfer agreements as well as the EU Data Protection Regulation negotiations. The European Parliament has voted to suspect all EU-US data transfer agreements on foot of its inquiry on mass surveillance by the US. By contrast, the EU-US Justice and Home Affairs Ministerial meeting in late 2013 stressed the importance of developing the EU-US negotiations on a data protection agreement, referencing the work of the EU-US ad hoc working group on the NSA surveillance saga.[97] Moreover, the regulatory impact of the EU-US WGCC is possibly of significance for and in turn is related to the on-going negotiations on an EU-US Data Protection Framework Regulation and an EU Data Protection Regulation. For example, the NSA surveillance affair has enhanced the controversy surrounding a draft provision of Article 42 of the draft Regulation which would give an EU court authority over

[93] E.g. Facebook, Google, Twitter.
[94] See http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf
[95] Cf media reports that the US Foreign Intelligence Surveillance Amendment Act (FISAAA) granted powers to grab EU data in US clouds: "US free to grab EU data on American clouds" *EUObserver.com*, 28 January 2013.
[96] "Europe pushes own digital "cloud" in wake of US spying scandal" *Euractiv*, 29 August 2013.
[97] Joint Press Statement following EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, Council 16418/13 (Brussels 18 November, 2013). See "Report on the Findings by the EU Co-chairs of the Ad Hoc EU-US Working Group on Data Protection", Council doc 16987/13, 27 November, 2013 and "Rebuilding Trust in EU-US Data Flows" COM(2013) 846 final. The latter references the role of the US within the Council of Europe Convention on Cybercrime as evidence of promotion of privacy standards internationally, at 9.

surveillance of EU citizen data pursuant to a foreign court order or other body.[98] Such provisions have the capacity to significantly alter the dynamic of the EU-US rule-making.

Nonetheless, the limited range of the WGCC mandate in the area of fundamental rights and data protection may need to be fundamentally revisited so as to acquire credibility and legitimacy. Moreover, its output seems increasingly eclipsed by EU and US internal rule-making developments. The European Parliament vote on the NSA surveillance and a European parliament inquiry, might have suggested a reduced impetus for the evolution of the regulation of cyberspace bilaterally, at least in the absence of a much stronger 'citizen-centric' component thereof. On the contrary, however, it has operated to spur the development of EU-US negotiations on a truly transnational instrument.

This leads to a more general assessment of the character of the EU's internal rule-making overall.

IV. THE CHARACTER OF EU RISK REGULATION

The EU's internal cyber regulation probably draws its closest parallels with another recent multi-stakeholder regulatory exercise:- in EU banking and finance regulation, in so far as it aims to regulate risk within a holistic international framework. The use of information-sharing networks and soft institutions possessing 'real' powers is a core feature of such a regulatory system.[99] The phenomenon of the formulation of *systemic* risk is a further key feature of the EU banking and financial regulation regime, somewhat similar to the cyber regime, built upon information-sharing and regularly published risk-reviews conducted by the European Banking Authority. It is notable that imprecision in the legal mandate of key bodies established recently in these regimes has generated questions of legal authority on account of the use of Article 114 TFEU.[100] These concerns of imprecision of legal mandate may be transferred *mutatis mutandis* to the EU cyber regulatory regime where it deploys Article 114 TFEU and emphasises its legal frailty.

[98] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final. Recent developments suggest that the adoption of a General Regulation will not occur until 2015, well after an outcome to the EU internal and external rule-making processes.

[99] See Eilis Ferran and Kern Alexander, Can Soft Law Bodies be Effective? Soft Systemic Risk Oversight Bodies and the Special Case of the European Systemic Risk Board *University of Cambridge Faculty of Law Research Paper* No. 36/2011; Annette Ottow, "Europeanization of the Supervision of Competitive Markets", 18(1) *European Public Law*, (2012), pp. 191-221; Niamh Moloney, Eilís Ferran, Jennifer Hill, John Coffee, *The Regulatory Aftermath of the Global Financial Crisis* (Cambridge: Cambridge University Press 2012); Elaine Fahey, "Does the Emperor Have Financial Crisis Clothes? Reflections on the legal Basis of the European Banking Authority", 74 *The Modern Law Review* (2011), pp. 581-595; Madalina Busuioc, 'Rulemaking by the European Financial Supervisory Authorities: Walking a Tight Rope," 19(1) *European Law Journal* (2013), pp. 111-125.

[100] Something which has been recently impugned with success in the Opinion of Advocate General Jääskinen in C-270/12, United Kingdom v Council and Parliament on 12 September, 2013 striking down the use of Article 114 TFEU in Article 28 of Regulation (EU) No 236/2012 of the European Parliament and of the Council of 14 March 2012 on short selling and certain aspects of credit default swaps, vesting powers in the European Securities and Markets Authority ("ESMA").

Mandatory disclosure of risk is a feature of many sectoral parts of the banking and finance regulatory regime for e.g. disclosure of capital requirements.[101] The invocation *and* regulation of market operators, by placing them under notification obligations in a harmonised regime is far from uncommon, as in the General EU Data Protection Regulation under negotiation and similarly, EU banking and financial services law or EU product safety.[102] One can discern two distinctive features of the banking and financial regulatory framework as regards risk and the obligations on actors within the framework. First, is the role of formal and proceduralised peer review in risk assessment, for e.g., in the implementation of stress testing.[103] This appears as an important different as regards the conceptualisation of actors acting within a framework of systemic risk in the cyber regime. Second, stakeholders are more explicitly the subjects and objects of the regulatory framework. For example, witness the more formalised procedural process under discussion by the European Banking Authority to identify those under reporting obligations, for e.g., Legal Identity Rules.[104] This is to be contrasted with the short legislative definitions of market operators within a minimum harmonisation Directive. In this regard, the EU's internal cyber regime could benefit from formalisation and proceduralisation.

What seems distinctive about risk within the cyber regulatory framework is the lack of a distinctive quantitative schema to detect and disseminate information or a lack of a real basis to make judgements about risk and nonetheless still place private actors under such obligations. One may contrast the place of private actors in US cyber regulation who are more strategically involved in the rule-making at the 'front' and 'back' end of the cyber rule-making processes.[105] Such a methodology seems to run the risk of institutionalising risk management at the expense of the actual societal risk through weak or inadequate IT systems operated by market operators. Furthermore, what is comparably distinctive is the scale of the obligations on so many market operators and their explicit place as the direct subjects and objects of the regulatory regime in the NIS Directive.[106] Placing obligations on those running high-risk entities such as nuclear plants is far from uncommon.[107] Yet the cyber regime differs

[101] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, 2013 L 176/338.

[102] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (2012)11, articles 31 and 32. See also the discussion of obligations on actors and institutional design in risk infrastructure, for example, as to product safety in respect of Article 114 TFEU, in Fahey, "Does the Emperor Have Financial Crisis Clothes," *supra* note 99.

[103] Pursuant to Article 30 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 (the European Banking Authority (EBA) Regulation). According to the EBA, peer review focusses on methods and examples of best practice, and considers (i) stress testing governance structures and their use, (ii) possible methodologies including the appropriate severity of scenarios and potential mitigating measures during stressed conditions, and (iii) the overall impact of risk on institution.

[104] Consultation on Draft Recommendation on the use of Legal Entity Identifier (LEI) (EBA/CP/2013/42, 28 October, 2013.

[105] Thaw, "The Efficacy of Cybersecurity Regulation" *supra* note 15.

[106] "EU Develops New Cybersecurity Rules," *Wall Street Journal*, 4 February 2013.

[107] E.g. Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations.

significantly from such entities but also from banking and financial supervision as a regulatory exercise for both its sheer scale and direct formulation of obligations on entities that may operate disproportionately on so many entities, for the reasons discussed here above. As a result, it seems difficult to contend that the EU's internal risk system as a rule-making process is either transparent, systematic or objectively defensible.

CONCLUSIONS

Risk regulation faces major challenges when conducted on a large-scale. The complexity of a regulatory process with many internal and external components raises the question as to its conceptual transparency, its functionality and systematic character. The casestudy of the rulemaking of the EU in cyber policies is an instructive one, concerning the contours of internal and external security, as well as providing an insight into their specific relationship in its regulation of risk. It has been argued here that the norm primacy accorded to the Council of Europe Convention has not yielded regulatory benefits. The account depicted here has demonstrated the primacy of external norms by the EU in its external and internal security making, as much as the overlapping and interlocking relationship between the internal and external dimensions thereof. Whilst similarly prioritising the primacy of external norms, the external rule-making of the EU with the US envisages a bolder vision of security rule-making on a global level. The process and content of the casestudy outlined here provides evidence of the openness of the EU to external norms. The character of EU internal regulation necessitates a scheme to formulate and regulate risk holistically yet appropriately, which does not appear to have been achieved in the rule-making conducted thus far.

This account has demonstrated how the internal/ external dichotomy in EU security is very real and apparent. Its evolution reveals particular relationships between the two, dependencies and trade-offs. It also reveals contrasting but closely dependent approaches to the internal and external components of EU security. The traditionally asserted 'fluidity' of external and internal security is arguably inadequate when seen from the perspective of this account. Instead, external security reveals many dependencies upon internal security. The temporal gap between legislating externally and the outcomes of internal processes may be surpassed by NSA surveillance and data protection negotiations ongoing. The latter represents distinctive regulatory sub-components that may radically impact upon such rule-making.