Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy

Axel ARNBAK[1]
Institute for Information Law, University of Amsterdam.
Berkman Center for Internet & Society, Harvard University.
Center for Information Technology Policy, Princeton University.

Abstract. This descriptive legal analysis maps and evaluates a four decade legacy of communications security conceptualizations in E.U. law and policy, including four legislative proposals launched in 2013. As the first comprehensive historical analysis of its kind, the paper forwards a range of new scientific contributions in a time secure electronic communications are of historically unparalleled societal, economic and political relevance. Five communications security policy cycles are identified, and their 'security' definitions and scope are described. These cycles are: network and information security, data protection, telecommunications, encryption and cybercrime. An evaluation of the current E.U. 'security' conceptualizations illuminates the underlying values at stake, the protection offered in current regulations, the formulation of six research themes and an agenda for computer science, political theory and legal research. Despite constitutional values at stake such as privacy and communications freedom and a robust computer science literature, the paper observes a deep lack of conceptual clarity and coherence in E.U. security policymaking. It then concludes that the observed conceptual ambiguity has allowed powerful stakeholders to capture, or paint E.U. network and information security policies in any colour they like.

The 2013 legislative proposals in the network and information security and – critically – their interdependence will be debated well into 2015 and provide a moment of truth for E.U. 'cybersecurity' policy. The outcome will reveal whether E.U. policymaking concentrates on securing electronic communications, or continues to foster political and economic interests of some of the more powerful 'cybersecurity' stakeholders. Given the increased relevance of, dependence on and attention for secure electronic communications, the coming year will illuminate what 'cybersecurity' policymaking really is about.

Keywords. Cybersecurity, network and information security, data protection, encryption, securitization, E.U. law, the c.i.a.-triad, constitutional values.

[1] See: http://www.ivir.nl/staff/arnbak.html. For the academic year 2013-14, Joint Fellow at the Berkman Center for Internet & Society, Harvard University and CITP, Princeton University. I am indebted to TPRC 2013 for accepting a very early stage draft of the paper on its program, and the 18 April 2014 IViR/Berkman Center workshop participants for their input. Natali Helberger, Nico van Eijk, Frederik Zuiderveen Borgesius and Caspar Bowden have given excellent comments on a previous draft.

1. Communications Security Conceptualizations in E.U. Law & Policy

Regulatory failure is often due to shortcomings in legal definitions.[2] This chapter critically reflects on the conceptualization of E.U. communications security law and policy. Section 1.1. identifies five communications security policy cycles, and offers what appears to be an exhaustive description – or at the very least a first attempt – of communications security conceptualizations in the E.U. regulatory framework. Spanning over four decades, the historical analysis shows that communications security regulation is nothing new, and that mapping the past proves critical in understanding current conceptualizations of 'security' and the underlying dynamic and interests in current policies: in all the identified subareas of communications security policymaking, new legislative proposals have been proposed and, some even adopted, in 2013. These proposals are set to influence global internet governance.

A holistic evaluation of these communications security policies is conducted in section 1.2., which subsequently develops six research themes on the intersection of computer science, political theory and legal studies. These research themes are still very much under construction, and input in the course of the thesis. From the evaluation, a research agenda is developed in section 1.3 on how to conceptualize communications security. This research agenda sets out the analytical framework of part I of the thesis.

[2] Baldwin et al. 2012, p.68.

1.1. ***The History of Five E.U. Policy Cycles***

It appears there is no comprehensive overview available of the current E.U. regulatory framework of 'network and information security', and how it is being shaped.[3] A recent policy study commissioned by the European Parliament calls the exercise 'undoubtedly highly complex', and in the end dodges the question at hand.[4] This section seeks to fill the gap, and to this end maps four decades of information and communications security conceptualizations in E.E.C., E.C. and E.U. policies, sketching the relevant regulatory framework in the process.

Five policy cycles can be distinguished: network and information security, data protection, telecommunications, encryption and cybercrime. The areas are presented more or less chronologically in terms of legislation adopted. The E.U. Treaties explicitly exclude 'national security from E.U. competence:

> *"[The E.U.] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State"*[5]

As such, 'national security' is a sole responsibility of E.U. Member States, and as such not a separate E.U. policy cycle. It will become clear that this often overlooked fact, most notably in the wake of the first Snowden revelations,[6] puts its mark on any effort to secure communications through E.U. regulation. Notably, the federal structure of the U.S. works exactly opposite; in the sense that national security is not dealt with at the state level, but rather 'a sole responsibility' of the federal government, particularly the U.S. Presidential Executive Authority.[7]

The sub-sections correspond with these five policy cycles, and start with providing the context of the policy cycle: the first instruments adopted, the policy rationales for doing so, and a short description of some of the prominent provisions. At the heart of the analysis of these policy cycle lies a description of the *definitions* of 'security' and their *scope*. Scope is understood as the policy area a particular instrument covers, which often means what stakeholders are subject of regulation, and what the rationale is for the regulatory instrument – securing information or networks, or if other interests have prevailed (such as national security or market structuring).

The definitions of 'security' that are mentioned in the legal instruments are analyzed against the well-known and broadly acknowledged "c.i.a.-triad" in computer science. In the Encyclopedia of Computer Science, Pfleeger defines them as follows:

- *Confidentiality* – assurance that data, programs, and other system resources are protected against disclosure to unauthorized persons, programs, or systems;
- *Integrity* – assurance that programs, or systems protect data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems;
- *Availability* – assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems. [8]

[3] Several policy documents contain brief outlines of the EU policy framework, however these contain gaps and hardly any analysis. See for example ENISA, *'National Cybersecurity Strategies – Practical Guide on Development and Execution'*, Dec. 2012, p. 2-5.
[4] Eg. N. Robinson et al., *'Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts'*, p. 80/96, report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament, Sept. 2013.
[5] Art. 4[2], Treaty on the Functioning of the European Union, OJ C 326 , 26 Oct. 2012.
[6] See section 1.1.2.
[7] Arnbak & Goldberg 2014.
[8] Cited from C.P. Pfleeger, 'Data security'. In *Encyclopedia of Computer Science* (4th ed.), Anthony Ralston, Edwin D. Reilly, and David Hemmendinger (Eds.). Chichester: Wiley 2003, p.504. See also Avizienis et al. 2004, p. 13, Pfitzman 2006, Haley et al 2006, Nissenbaum 2005, Pieters 2011. Mulligan & Schneider 2011, K. de Leeuw & J. Bergstra 2007, p.2.

In computer science, a rich literature further specifies and interprets the confidentiality, integrity and availability triad, its elements referred to as security goals.[9] It begs the question to what extent, in all those decades, policymakers have appreciated the insights from computer science, and how policies may, or may not have come to a clear grasp how to translate these security goals into sensible policies.

The year 2013 has seen legislative action in all five areas identified, either with proposals or legislation adopted. A separate section 1.1.6 is devoted to the 'Network and Information Security' Directive, proposed by the European Commission in February 2013 and currently debated by the E.U. Parliament and the E.U. Council of Ministers – the institution in which national governments find their E.U. seat. This new proposal speaks to all the policy cycles identified, and will give an actual indication of the ambitions of the E.U. institutions to augment information and network security. The confrontation of E.U. institutions in the space of information and network security in 1990 might be instructive in forecasting the outcome of that process.

1.1.1. *Information Systems & Critical Infrastructures*

The ambition of E.U. institutions to treat the security of 'information systems' as a separate policy area traces back, at least, to a 1992 Council Decision 'In the Field of Information Systems'.[10] The issue statement of the 1992 Decision reads like any opening statement of a policy document today:

> *"1.1. Issue - security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world."*

The issue statement observes that coordinated action at the E.U. level is the needed to avoid 'a fragmented approach'. That aim would not exactly be realized. To the contrary, E.U. policies would become highly fragmented and it would take over twenty years for substantial, coordinated *legislative* action to be introduced (see section 1.1.6.).[11] The legislative history of the 1992 Council Decision may explain why this is the case. The Council Decision itself contains little substance, but is a fascinating moment in information and communications security policymaking for its underlying institutional politics.

A 1990 proposal of the European Commission and several European Parliament resolutions preceded the 1992 Council Decision. In 1990, the Commission proposal expressed broad ambitions for information security policies at the E.U. level.[12] Its preambles gave considerable responsibilities to the European Commission, evoked the subsidiarity principle for E.U. action and mentioned that international coordination was necessary. A prominent justification read that information and communications security was not bound by traditional territorial notions of nation states. The document listed a broad set of underlying values to legitimize E.U. policymaking, such as 'protecting privacy, intellectual property, commercial confidentiality and national security.'[13]

In the Council text, however, such ambitions are toned down considerably. The document isolates facilitating a competitive business environment as the primary competence of E.U. level action in this area; information security should protect 'business applications, intellectual property and confidentiality'.[14] Other considerable changes in the Council Decision include the removal of the

[9] See section 2.1.
[10] Council Decision 92/242/EEC, OJ L 123/19, 8 May 1992.
[11] See section 1.1.6.
[12] COM(90) 314 final, OJ C 277/18, 5 Nov. 1990, p.18.
[13] COM(90) 314 final, Annex, Action line II, art. 2.1.7.
[14] Council Decision 92/242/EEC, Annex, Action line I, art. 2.1.

subsidiarity principle from the preambles; more representation of Member States in the expert group; the final say of the Council in cases of conflict, as well as the right of the to postpone actions suggested by the Commission (art. 8 Council Decision).[15] The Council, moreover, exactly determined the allocation of a tiny budget for European activities (2 million ECU per year, art. 3 Council Decision).[16] Excluding end user interest from the domain of critical infrastructure protection may have obscured the issue for other EU institutions, notably the European Parliament, in decades to come. The EEC Treaties in the 1990s did not prevent more ambitious approaches to augment the information and communications security of critical infrastructures to enhance public interests such as information and communications confidentiality or availability – similar to data protection or telecommunications provision.[17] With the 1992 Council Decision, Member States claimed control of network and information security policymaking.

The legislation on the tasks of the European Network and Information Security Agency ('ENISA') shows how that the institutional dynamic of the 1990s at the E.U. level still drives policymaking today. Art. 1[1] of the 2013 ENISA Regulation states that its task is to "raise awareness and promote a culture of network and information security (…) for the establishment and proper functioning of the internal market." Raising awareness and promoting a sense of urgency does not automatically give an institution actual authority. Among its other tasks are to support and contribute to voluntary efforts of other stakeholders (art. 3), without any explicit mandate of enforcement. Furthermore, national security and criminal law are explicitly excluded from its mandate in art. 1[2],[18] even though criminal law falls squarely within the competence of E.U. lawmaking since the 2009 adoption of the EU Treaty of Lisbon. The internal market focus, voluntary nature of ENISA policies and exclusion of criminal law strike as familiar to the 1992 Council Decision discussed above. Indeed, ENISA's impact has been analyzed as limited to providing 'policy advice', with a 'poor uptake' of its reports.[19]

Here, national governments strive for tight control of information and communications security policymaking. As we will see, this dynamic is indirectly challenged in several other policy cycles discussed throughout this chapter. And the current institutional power structure is challenged again, directly, with the 2013 Commission proposal for a 'Network and Information Security' Directive (section 1.1.6.).

Definition

'Security' is not defined in the 1992 Council Decision. Art. 1 jo. art. 2 call for the creation of an expert Committee ('Senior Officials Group') and contains calls for the development of action plans following six themes,[20] that are further outlined in an Annex and mostly describe a course of procedural action rather than relevant substantive details.

[15] The Commission proposal merely obliged it to send a report of its actions to other EU institutions (art. 5 Commission proposal).
[16] Contrasting with budgetary discretionary for the Commission as proposed by the Commission (art. 3 Commission proposal).
[17] Opting for a Council Decision rather than a Directive may, however, have been a strategic choice. The Council Decision is based in art. 235 of the EEC Treaty, which required a unanimous vote in the EU Council and a mere 'consultation' of the EU Parliament, rather than a majority vote in Parliament in the case of Directives. See generally: S. Prechal, *Directives in EC law*, Oxford: Oxford University Press 2005.
[18] Art. 1[2], Regulation 526/2013, art. 1[2], Regulation 460/2004.
[19] N. Robinson et al., *'Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts'*, p. 84 report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament at: http://www.europarl.europa.eu/delegations/fr/studiesdownload.html?languageDocument=EN&file=96230
[20] Outlined in art. 2[2]: "development of an information security strategy framework; identification of user and service provider requirements for the security of information systems; solutions for immediate and interim needs of users, suppliers and service providers; specifications, standardization and verification of information security; technological and operational developments for information security within a general strategy; provision of security of information systems."

The first definition of 'security' in this policy cycle can be traced back to a 2001 Commission Communication.[21] That 2001 definition has seen only slight modification over the years and is most recently codified in the 2013 ENISA regulation art. 1[3]: [22]

> *'network and information security' means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems.*

The definition seems directly inspired by the c.i.a. triad, but adds 'authenticity' to it. Unfortunately, additional argumentation or source material on why and how the Commission came to this definition is not provided. Subsequent EU documents that refer to this definition also lack further argumentation or source material.[23] Apparently, those later definitions have simply been copied from the 2001 definition. ENISA may have produced several reports and organized a range of workshops, but those are hardly taken seriously and do not have any binding force. The lack of guidance as to the meaning or intentions of the legislator is a cause of legal uncertainty and calls for further scrutiny.[24]

Scope: 'Network and Information Systems'

The 1992 Council Decision does not determine which entities are regulated. The 2013 ENISA Regulation offer only a reference to an incomplete description of 'network and information systems' in a 2006 Commission Communication.[25] That document is vague across the board; it also proposes policy action "based on dialogue, partnership and empowerment" involving "all stakeholders involved".[26] Such statements hardly provide guidance as to the scope of the instrument.

A 2001 Communication does mention that "all events that threaten security need to be covered", and provides an "overview of threats."[27] The examples are quite detailed and mostly still relevant, such as failure by websites to implement browsing over HTTPS, network disruption discussing DDoS attacks and malicious representation discussing identity fraud. The threats mentioned overlap with then already existing E.U. legislation in the areas of encryption, telecommunications and data protection.[28] In 2013, an ENISA Regulation would state that ENISA may only support, but not interfere, with telecommunications and data protection regimes and supervisory authorities.[29] Other threats mentioned in the Communication, such as the Echelon spying infrastructure, may fall within the definition of 'network and information security', but as subject matter national security is clearly exempted from the policy cycle in art. 1[2] ENISA Regulation.

Scope: 'Critical (Information) Infrastructures'

In 2005, the American political concepts of 'critical infrastructures' and 'cybersecurity' enter the E.U. policy arena. A Green Paper drafted by the Commission,[30] upon the request of the Council, eventually leads to the 2008 'Council Directive on European Critical Infrastructures'.[31] Again, the Council

[21] COM(2001) 298 final, 'Network and Information Security: Proposal for A European Policy Approach', 6 Jun. 2011, p. 3, p. 9.
[22] Regulation 526/2013, OJ L 165/41. The slight modification is the inclusion of 'unlawful'.
[23] ENISA Regulation 460/2004, art. 4[c]. COM(2006) 251 final.
[24] See section 1.2.
[25] The 2001 Communication contains an imprecise description of networks, 'systems on which data are stored, processed and through which they circulate' and an unfinished (!) sentence on applications and terminal equipment directly after it. COM(2006) 251 final, p. 9.
[26] "The Commission proposes a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment (…) in an open and inclusive multi-stakeholder dialogue." COM(2006) 150 final, p. 6.
[27] COM(2001) 298 final, p. 9.
[28] COM(2001) 298 final, para. 2.2.
[29] Rec. 37, Regulation 526/2013.
[30] 'Green Paper On A European Programme For Critical Infrastructure Protection', COM(2005) 576 final.
[31] Council Directive 2008/114/EC, 8 Dec. 2008, OJ L 345/75.

assumes control of the policy area and deems critical infrastructure protection primarily as an issue of Member States' national security (recital 4).

Apart from identifying new European Critical Infrastructures ('ECI') in the energy and transport sectors (Annex I), the Council Decision lays out a procedure to possible identify other sectors (Annex III). With regard to ICT, the Council is considering but not identifying the ICT sector as a Critical Infrastructure in of the 2008 Decision (recital 5). The consequence of being deemed an ECI, is that operators in those industries should have a security plan (art. 5 jo. Annex II) and a liaison officer for communication purposes (art. 6) in place, but it is up to Member States to determine most of the details and to enforce such obligations.

Adding to the confusion, in 2009 the Commission introduced a sub-class of Critical Infrastructures with regard to ICTs – so-called 'Critical Information Infrastructures'. Including internet backbone providers in its scope, this strand of policy is primarily concerned with encouraging the availability (or continuity) of communications through a host of newly erected voluntary public-private partnerships.[32] Both in critical infrastructure and critical information infrastructure policymaking, the voluntary nature of the regulatory measures is emphasized, and a sprawling web of organizations and working groups has emerged. That dynamic has been accelerating ever since, as recently new ones are being introduced on a seemingly monthly basis.[33]

Overall, policymaking in this field has not achieved to offer a clear picture of what 'network and information security' entails, nor what stakeholders fall within its reach. Meanwhile, policies often refer to several other cycles of E.U. policymaking. Indirectly, those other avenues of policy have had much more actual impact on the conceptualization of 'security' at the E.U. level. A close study of these related, and often overlapping, policy cycles is needed to comprehensively analyze the 2013 Commission proposal for a 'Network and Information Security' Directive (section 1.1.6.).

1.1.2. *Data Protection*

Since the inception of data protection, the security of personal data has been around as a concept.[34] In different definitions, and increasingly elaborate, data security was part of the earliest versions of the Fair Information Practice principles in 1973,[35] the U.S. Privacy Act of 1974,[36] the OECD Fair Information Practice Principles, and made it into the influential 1981 Council of Europe Convention no. 108.[37] That convention provides the basis for the 1995 E.U. Data Protection Directive, with its provision on 'data security' in art. 17.[38] That provision is still considered as one of the cornerstones of E.U. 'security' legislation and enforcement today.

Definition

Many E.U. legislative instruments follow the wording of the Data Protection Directive, that defines 'security of processing' in art. 17[1]:

> *'Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration,*

[32] COM(2009) 149 final.
[33] N. Robinson et al., *'Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts'*, p. 80, and reiterated by the authors on p. 96, report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament.
[34] See generally C. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, 1992. R. Gellman, *Fair Information Practices: A Basic History*, 2013.
[35] Great Britain, *Report of the Younger Committee on Privacy*, Home Office, 1972. See: http://epic.org/privacy/hew1973report/appenb.htm
[36] U.S. Privacy Act of 1974, 5 USC Sec. 552a(e)(10).
[37] Council of Europe, European Treaty Series No. 108, http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[38] Directive 95/46/EC ('Data Protection Directive'), OJ L 281, 23 Nov. 1995.

> *unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'* [39]

The first part of the definition closely follows art. 7 of the CoE Convention no. 108, but then the provision specifically adds a sentence on networked transmission on top of the original convention. That first part mirrors the c.i.a. triad, as disclosure or access appeal to *confidentiality*, alteration to *integrity* and destruction or loss to *availability*. It is a bit narrower than the c.i.a. triad, as it does not cover *temporary* loss of data availability.[40] Ensuring data availability in tense situations such as emergency healthcare is as such not covered by the Data Protection Directive.

The second part of the definition reveals that the provision may touch on both information and network security, given the addition of 'in particular where the processing involves the transmission of data over a network' to art. 17 Data Protection Directive. Recital 47 of the Directive explains, that 'telecommunications or electronic mail service' providers are deemed controllers for the traffic data generated by using those services. The 1997 predecessor of the E-Privacy Directive would further elaborate on these observations (both instruments discussed in section 1.1.3.).

The provision today still refers to network security, and there has been some action is this particular area by data protection authorities. The Dutch Data Protection Agency, for instance, started enforcement actions in July 2013 against 43 private doctors for not providing HTTPS-encrypted web communications to end users for forms on their websites.[41] The enforcement action was based on a sector specific standard[42] that finds its legal base in the Dutch implementation of art. 17 of the Directive, art. 13 of the Dutch Data Protection Act. Curiously, art. 13 of the Dutch Act has removed the network security sentence from its provision. Nonetheless, a network security enforcement action is taken by the data protection enforcer, when network and information, or data security are seen as interdependent. Such enforcement actions point to an uncertain and complex legal relationship between data security and network security (further discussed in section 1.2).

Scope

The 1995 Directive's 'security' provision is only applicable to organizations that control or process 'personal data'[43] – a key term in the Directive that captures those data that can directly or indirectly lead to the identification of a person.[44] The scope of 'personal data' has been expanding even since the adoption of the Directive in 1995 and remains the subject of intense political and scientific debate ever since.[45] But, as observed before with art. 17 of the Directive, Courts and Data Protection Authorities often interpret the term in light of new technological realities. For instance, IP-addresses are usually considered to be personal data. Regardless, certainly not all information and communications constitute 'personal data'. Corporate information, draft government policies or media reports stored on some server in the cloud are straightforward examples.

---

[39] Section VIII of the Data Protection Directive contains art. 17 and is titled: 'the confidentiality and security of processing', which in itself reveals that the c.i.a.-triad has not been followed.

[40] See Dutch Data Protection Authority guidelines on securing personal information. CBP, *'Richtsnoeren Beveiliging Persoonsgegevens'*, Feb. '13, p. 14.

[41] See CBP, 'Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek', May 2013, p. 3. http://www.cbpweb.nl/downloads_rapporten/rap_2013-beveiliging-online-herhaalrecepten.pdf

[42] NEN 7512:2005, *Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling*, p.15.

[43] Both 'controllers' (art. 17[1]) and organizations that 'process' personal data on their behalf (art. 17[2-4]) are covered in the Data Protection Directive. In outsourcing, for example, data security must be ensured through a private contract that assures a similar level of protection demanded from the 'controller' in art. 17[1] DPD.

[44] Defined in art. 2(a) Directive 95/46/EC: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

[45] Art. 29 WP, *'Opinion 2/2010 on Online Behavioural Advertising'* (WP 171), 22 June 2010, 9. See also Art. 29 WP, *'Opinion 4/2007 on the Concept of Personal Data'* (WP 136), 20 June 2007, 12-20. CJEU, 24 November 2011, C70/10, para. 51 (Sabam/Scarlet). For a thorough discussion of this particular issue, see F. Zuiderveen Borgesius, *'Behavioral Targeting: A European Legal Perspective'*, IEEE Security & Privacy, 2013-1, p. 82-85.

This simple observation that data protection policy only concerns situation in which 'personal data' is involved is however often overlooked, for instance in the initial European response to the Snowden revelations. Policymakers took to data protection, notable its safe harbor regime on international data transfers, for solving legal issues around ubiquitous surveillance. However, due to its definitions and scope, data protection as a solution is inherently limited. Only a small subset of the data in which intelligence agencies may be interested will be covered by data protection. Moreover, national security falls outside the material scope of data protection regulation for reasons of EU competence – national security is up to the Member States individually.[46]

Recent Legislative Action

The 1995 Directive is currently under review after the Commission proposed a Regulation in January 2012. The proposed General Data Protection Regulation ('GDPR'), if adopted, acquires immediate binding force across the EU without a need for implementation on the Member State level. The long awaited and quite massive legislative effort has led to a record amount of amendments filed in the European Parliament, but in March 2014 the Parliament nearly unanimously adopted a comprehensive legislative package.[47] While the incoming Greek E.U. Council Presidency had given priority to data protection,[48] for various reasons – the German government reluctant to lower standards, the UK defending business interests[49] – the Member States in the EU Council agreed at an October 2013 summit to move the deadline for adoption until 2015. With the heads of government openly debating data protection in the media, and amidst ongoing revelations on transnational intelligence gathering by all governments involved, data protection has become even more politicized than it already was when the Commission launched its initial proposal in 2012. Therefore, the implications of the entire process for the current arrangements around art. 17 are hard to assess at this point.

A crucial development is that Compromise position of the leading European Parliament Committee LIBE contains the introduction of a 'pseudonymous data' category, defined in art. 4[2a] of the Compromise proposal for the GDPR: "pseudonymous data means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution". A large body of research in computer science has meanwhile established that 'pseudonymous data' and 'anonymized data' can be re-identified using innovative inference techniques, recently even through writing style.[50] In March 2014, European Commissioner Reding has warned that the pseudonymous data category may become the "Trojan horse at the heart of the Regulation, allowing the non-application of its provisions."[51] If adopted, data considered pseudonymous data would not be regulated by art. 17 (art. 30 in the Compromise proposal for the GDPR),[52] which would imply further limits on the scope of the information and communication security provision through the EU data protection regime.

1.1.3. *The Telecoms Package*

The European regulatory framework for electronic communications originates in a long legacy of state-owned postal and telecommunications companies. The 1990 legislative package now known as the 'Open Network Provisions' aimed to liberalize the telecommunications market. Today still, the

[46] See Van Hoboken, Joris V. J., Arnbak, Axel and Van Eijk, Nico, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad (June 9, 2013), p. 27-29.
[47] A7-0402/2013, 22 nov. 2013, see: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//EN&language=en
[48] http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm?locale=en
[49] http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pac-news-531306
[50] A. Narayanan & V. Shmatikov, *Robust de-anonymization of large sparse datasets*, IEEE S&P Symposium 2008, p. 111-125; A. Narayanan et al. *On the feasibility of internet-scale author identification*, IEEE S&P Symposium 2012, p. 300-314.
[51] http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm?locale=en
[52] The information security provision itself in the proposed art. 30 appears to emerges materially strengthened, with a mandatory data protection impact assessment and security policy requirements.

main aim of the Telecoms Package, in the words of the European Commission, is 'to strengthen competition by making market entry easier and by stimulating investment in the sector.'[53] This legacy has real consequences for its security provisions, as we will see.

The 1997 'Telecommunications Data Protection and Privacy' Directive contained a general communications confidentiality requirement in art. 5.[54] Interestingly, the European Commission originally proposed a specific and robust network security requirement in its proposal for the Directive of 1990. Art. 8[2] of that proposal contained an explicit obligation for end-to-end encryption in telecommunications networks.[55] The end-to-end encryption proposal never made it into the final 1997 Directive. Today, many call for legal safeguards for strong end-to-end encryption in response to the Snowden revelations. Contemporary advocates of end-to-end encryption are probably unaware of those legislative debates on crypto in the Telecoms Package, already taking place over two decades ago against the background of liberalization of telecommunications. It is unclear why end-to-end encryption did not make it into the Directive. The explanation might lie in a combination of the priority of market liberalization and competition law over privacy, in a time when the crypto wars were waging primarily in the encryption policy cycle (see section 1.1.4.).[56]

The current relevant provisions can be found in the 2002 Framework and E-Privacy Directives,[57] respectively both amended in 2009.[58] The current art. 5 of the E-Privacy Directive still contains the same general confidentiality obligation as in 1997. Notable communications security measures introduced with the 2009 amendments are risk-assessment based 'security' obligations, [59] 'integrity' obligations to protect continuity,[60] a 'security' breach notification[61] and a personal data security breach notification.[62]

Definition

The 1990 Open Network Provisions included the 'Commission Liberalisation Directive'. It contains provisions on 'security' and 'integrity' in recital 9 that already point at underlying concerns at the time:[63]

> *"(9) the security of network operations means ensuring the availability of the public network in case of emergency. The technical integrity of the public network means ensuring its normal operation and the interconnection of public networks in the Community on the basis of common technical specifications. The concept of interoperability of services means complying with such technical specifications introduced to increase the provision of services and the choice available to users. Data protection means measures taken to warrant the confidentiality of communications and the protection of personal data."*

While introducing security measures, 'security' itself is not defined in that Directive. The c.i.a. triad remains not followed in its entirety until today. The definition of 'security' in 1990 emphasizes availability and interconnection, which points at liberalization of state monopolies and creating conditions for market entry as driving forces of the legislation. Data protection is subsequently seen as

[53] See: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm
[54] Directive 1997/66/EC, OJ L 24, 30 Jan. 1998. Note that this Directive traces back to a 1990 Commission proposal for a Council Directive in COM(1990) 314 final, SYN 299, p. 71.
[55] Art. 8[2], COM(90) 314 final, SYN 288 *Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks*, 27 Jul. 1990, 90/C 277/04.
[56] Reference?
[57] Directive 2002/21/EC (the 'Framework Directive', OJ L 108/33, 24 Apr. '02) and Directive 2002/58/EC (the 'E-Privacy Directive', OJ L 201/37, 31 Jul. '02).
[58] Directive 2009/140/EC ('Better Regulation Directive', OJ L 337/37, 18 Dec. '09) and Directive 2009/136/EC ('Citizen's Rights Directive', OJ L 337/11. 18 Dec. '09).
[59] Art. 13a[1] Better Regulation Directive.
[60] Art. 13a[2] Better Regulation Directive.
[61] Art. 13a[3] Better Regulation Directive.
[62] Art. 4[3] Citizen's Rights Directive.
[63] Art. 6 jo. art. 1 jo. rec. 9 Directive 1990/388/EC ('Commission Liberalisation Directive').

confidentiality of communications and data. Integrity is framed as 'normal operation', not at all the same as the integrity definition in computer science literature.

Over time, the conceptualization of 'security' in the 1990 Commission proposal and 1997 Directive would lead to confusing situations in the current Directives of the Telecoms Package. The confusion plays out on at least three levels. First, confidentiality enjoys broad protection under art. 5 E-Privacy Directive, which mentions both confidentiality of "communication" and "information". The E-Privacy Directive also mentions the ECHR and the Charter of Fundamental Rights of the E.U. in its opening recitals 2 and 3, as well as 24. For the other security attributes, art. 4 of the E-Privacy Directive implies that security is only of concern when personal data is involved, even though 'security' is about much more that personal data alone (section 1.1.2.).[64] Second, the Telecoms Package contains a general 'networks and services' security provision (art. 13a[1]) and a separate obligation for regulated entities to ensure the integrity of their networks (art. 13a[2]).[65] Had the Directives followed a more comprehensive definition of 'security' of the c.i.a. triad, art. 13a[1] would be more comprehensive and less confusing, while art. 13a[2] would have been superfluous. Thirdly, the integrity provision of art. 13a[2] ensures 'continuity of supply of services'. But that concerns *availability*, rather than *integrity*. Taken together, the interplay between 'security' in art. 13a[1] and integrity in art. 13a[2] is unclear, and not specified in recitals. It remains an open question whether the c.i.a.-triad attributes of the networks and information that are covered within the Telecom Package are covered by the legislation. If, and how network and information integrity as defined under the c.i.a.-triad are covered, is uncertain.

The legal uncertainty is exacerbated by the fact that, across the board, the legislator delegates determination of the details to the European Commission in art. 13a[4] Better Regulation Directive. The provision directs the Commission to follow 'international standards to the greatest extent possible', even though the provisions themselves do not align with international standards on such basic issues as terminology. International industry standards usually follow the c.i.a.-triad.

Furthermore, entrusting communications security to industrial standard setting procedures does not automatically yield optimal outcomes from a communications security perspective. It has been known for a long time among security experts that the GSM encryption standard A5 had been deliberately weakened through pressure by intelligence agencies.[66] This take on history has recently been confirmed amidst the Snowden disclosures, when four Norwegian engineers that took part in creating the GSM-standard process in the early 80's finally dared to speak up to and provide the details of the story. They pointed at the UK government for leading the effort in choosing weaker keys (54-bit instead of 128-bit) to enable intelligence gathering.[67] Strikingly, the weakened encryption standard adopted back then is still in wide use today, for instance in European 2G networks, leaving European mobile communications vulnerable to security breaches.

Such observations on standardization, as well as the failed attempt of the Commission to include end-to-end encryption as a security requirement in 1990 and beyond, spur the question how to determine 'acceptable' levels of security in light the general security obligations in art. 13a Better Regulation Directive. One can have a solid confidentiality provision with art. 5 E-Privacy Directive, but if the

[64] Art. 4 of the E-Privacy Directive and more explicitly recital 20 of the E-Privacy Directive mention that 'security is appraised in the light of Article 17 of Directive 95/46/EC', the Data Protection Directive.

[65] According to art. 13a[1], Member States must ensure that regulated entities 'prevent and minimize the impact of security incidents on users and interconnected networks'. Art. 13a[2] rules that Member States ensure that regulated entities 'guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks'.

[66] R. Anderson, *Security Engineering*, London: Wiley 2008, p. 615. In 1994, Anderson wrote a piece for UK Telecom, claiming that "there was a terrific row between the NATO signal intelligence agencies in the mid-1980s over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Warsaw Pact; but the other countries didn't feel this way, and the algorithm as now fielded is a French design." R. Anderson, *Hacking Digital Phones*, UK Telecom, 17 Jun. 1994.

[67] See: http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html

combination of art. 13a Better Regulation Directive and standardization allows to maintain a vulnerable encryption protocol for GSM over decades, a powerful adversary can get backdoor access to those communications regardless of confidentiality provisions in place.

Scope

The scope of the Telecoms Package is largely[68] limited to providers of 'electronic communications networks' and 'electronic communications services.'[69] Here, the market structuring legacy of the 1990 Open Network Provisions manifests itself directly. On the face of it, only conventional telecommunications and internet access providers fall within the scope of the Telecoms Package, being the 'transporteur' of communications primarily in the business of signals transmission.[70] Other communications providers, such as information society services[71] (think social network services and webmail providers), seem to fall outside its scope.[72] The fast observation could be made, that the Telecoms Package fails to appreciate crucial socio-technical developments in electronic communications since the 1990s, such as digitization and the convergence of communications. However, two examples provide a deeper understanding of that dominant view on the scope of the Telecoms Package: the regulation of i) data- and security breach notifications, and ii) Voice over IP ('VoIP') communications. The examples point at the underlying priorities of telecommunications regulation in Europe, how they are connected to the Open Network Provision legacy and how this affects security conceptualizations and policymaking.

The European Commission proposed a (personal) data- and security breach notification for electronic communications providers in 2007.[73] From the viewpoint of information and communications security, the most relevant intermediaries in this communications setting are the companies that create, store, process and monetize the data and infrastructure that the obligation seeks to protect – notably 'information society services'. These services provide most of the relevant functionality in a specific communications setting, where the conventional access provider merely connects its subscribers to the web. Following this reasoning, a majority in the European Parliament – with support from the art. 29 WP and the EDPS – sought to extend the data- and security breach notifications to information society service providers in 2008.[74] However, the Commission argued that the legal definitions of the Telecoms Package constrained to Parliament to pursue such an expansion in scope. Consequently, the notification measures remained in place, but only for conventional 'electronic communications providers'.[75] Hardly anyone noticed when the Commission provided the notification guidelines for these conventional electronic communications providers on 24 June 2013.[76] Meanwhile, 'information society services' have suffered a wide range of major security incidents – such as the leakage of millions of login credentials by e-mail newsletter provider Epsilon, Yahoo! and

[68] The cookie and spam provisions in the E-Privacy Directive regulate a broader set of relevant stakeholders, according to art. 5 and art. 13. Art. 29 WP 2009, WP 159, par. 2.1, note 7. See also F. Borgesuis, *'De meldplicht voor datalekken in de Telecommunicatiewet'*, Computerrecht, 2011-4, p. 211.
[69] See art. 2[a] jo. 2[c] Directive 2009/140/EC. Networks that fall within the scope of the definition in art. 2[a] are those "resources which permit the conveyance of signals irrespective of the type of information conveyed". Services are those "that consist wholly or mainly in the conveyance of signals on electronic communications networks, but exclude services providing content".
[70] Steenbergen 2009.
[71] See art. 1[2] Notification Directive 1998/48/EC: 'Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'
[72] Explanatory Memorandum, European Commission, Amended proposal, COM(2008)723 final, p. 20. See also recital 20, Directive 2002/21/EC.
[73] A personal data breach in the context of the Telecoms Package is defined similar to art. 17 Data Protection Directive in art. 2[h] Citizen's Rights Directive: '"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.' The security provisions in art. 7 of the Data Retention Directive (2006/24/EC) follow the same approach.
[74] European Parliament, amendment 136, 24 September 2008.
[75] F. Borgesuis, *'De meldplicht voor datalekken in de Telecommunicatiewet'*, Computerrecht, 2011-4, p. 211.
[76] See art. 1 Commission Regulation 611/2013.

LinkedIN – leaving the communications security and personal data of millions of users exposed.[77] In this example, the European legislator focused on the 'actor' rather than the function of the communication, and the Parliament saw itself constrained by the legislative definitions on scope in the Telecoms Package.

The second example, the regulation of VoIP, reveals a surprising contradiction. Following the Commissions reasoning with regard to breach notifications, VoIP providers would be regulated as information society service providers – falling outside the scope of the Telecoms Package. Following this line of reasoning, when Alice calls Bob using a fixed landline, the Directives apply. And when Alice uses VoIP technology to contact BoB, the providers of that communication, and thus its security, would go unregulated. The policies, however, are very different. According to the Commission, VoIP providers can fall under different regulatory regimes, and consequently with different regulatory obligations for communications security.[78] Here, the *market* with which the service competes is what matters. When a VoIP provider calls a phone number rather than a user account (say, SkypeOut rather than Skype-to-Skype) the Telecoms Package applies. But the average VoIP user that has the service installed on a smartphone and receives a call does not reasonably notice the difference between, say, SkypeOut and Skype-to-Skype. The user probably expects communications security provisions to apply to both VoIP communications settings.

The examples reveal that market considerations can stretch the scope of Telecoms Package, but communications security considerations cannot. The market structuring legacy of the Telecoms Package informs a communications security policy, where the economic fact that a software product competes with a 'analogue' service providers prevails, rather than the function of the communications setting. The E-Privacy Directive's scope has been stretched with regard to cookies and spam;[79] these provisions of the Telecoms Package target stakeholders beyond conventional telecommunications and internet access providers as well – such as websites and webhosting providers. In the Telecoms Package, communications security is approached on an ad hoc basis, in which market and political pressures prevail. A rigorous conceptualization of 'security' and its scope would inform an approach that would not leave substantial gaps in communications security protection for end users.

Recent Legislative Action

In September 2013, the European Commission proposed a Regulation amending several provisions of the 2002 and 2009 Directives.[80] The proposal and the proposed amendments to it in the Parliament don't affect the definitions, scope or the security provisions introduced in 2009. The aforementioned problems with regard to definitions and scope are not bound to be addressed anytime soon.

1.1.4. *Digital Signatures and Certificates*

Roughly until 1980, intelligence agencies closely guarded the means of production and use of encryption. Outside military and intelligence settings but within nations, relatively weak encryption was made available to provide some level of protection of communications, for instance to state-owned or controlled telecommunications companies (see section 1.1.2.). At the same time, strict restrictions on the export of encryption were (and remain) in place to control the spread of encryption across national borders.[81] In this way, intelligence agencies such as the NSA and GCHQ had close

[77] Zwartboek Datalekken: https://www.bof.nl/category/zwartboek-datalekken/
[78] "VoIP providers can be classified as providers of publicly available electronic communications services (…). This is however not the case for VoIP services that offer machine-to-machine communications essentially only consisting of the provision of a product." SWD/2013/032 final, Impact Assessment, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT
[79] Art. 5 and Art. 13 E-Privacy Directive. Art. 29 WP, WP159 2009, par. 2.1, note 7,.
[80] COM(2013) 627 final, 2013/0309 (COD), 'laying down measures concerning the European single market for electronic communications and to ,achieve a Connected Continent.
[81] B.J. Koops, *Crypto Law Survey*, at version 27.0, last update Feb. 2013, see http://www.cryptolaw.org/. The online survey of Koops maps encryption policies in a wide range of jurisdictions around the world. The survey focuses on export controls, encryption mandates and decryption orders for law enforcement. The E.U. section seems updated until 2002.

control over the adoption of encryption, while remaining capable of accessing weakly encrypted communications for surveillance and intelligence operations.[82]

Since the 1980's, however, more robust encryption was discovered and produced in private industry, academic and cypherpunk communities. Eventually, robust encryption became available for the average computer user. The development spurred a fierce public policy debate, popularly known as the 'crypto wars', on the regulation of encryption. Where civil liberties and business stakeholders see encryption as a central tool in protecting information and communications security central to human rights and business practice such as high-speed finance and E-Commerce, national security and law enforcement agencies voiced concern about access to communications. Mass adoption of electronic communications, easy access to open encryption tools such as PGP and SSL-certificates and the promise of E-Commerce intensified these debates in the mid '90s.

In 1997, the European Commission adopted a Communication on its encryption policy when the debates on its regulation reached a boiling point. The Communication titled 'Towards A European Framework for Digital Signatures And Encryption'[83] favored mass adoption of encryption.[84] Compared to the U.S. position on encryption, Andrews observes that the Commission took a relatively 'liberal approach'.[85] Andrews attributes the relatively friendly Commission position in part to the existence of art. 17 in the Data Protection Directive and the Telecoms Package, particularly art. 5 of Directive 97/66/EC (later the E-Privacy Directive).[86] In addition, Blanchette points to a strong but in the end unjustified belief among policymakers that electronic signature technology would change a centuries-old practice around the legal status of hand-signed paper documents.[87]

The 1997 Communication set the stage for the 1999 eSignatures Directive,[88] that provided a harmonized framework for the provision of digital signatures and certificates across the Europe. However, the national governments in the European Council succeeded in curtailing the ambitions of the European Commission on legislation at the E.U. level, leaving important specifics to the Member States. Throughout the 1990s, the European national governments had been leaving ample room for weakening cryptography in public statements by government bodies.[89] With the 1999 Directive – notably its omission of the prohibition for Trusted Service Providers to store private keys (discussed below) – the E.U. Council has achieved what it aimed for. This has led to enabling commerce to thrive by providing some integrity requirements and low regulatory burdens, but at the same time allowing for weak encryption and security requirements in E.U. legislation, both in the E-Signatures Directive, and in the E-Commerce Directive.[90] Obviously, the Snowden revelations – particularly the BULLRUN operation aimed at weakening encryption standards, technologies and implementations –

[82] W. Diffie & S. Landau, *Privacy on the Line*, Cambridge: MIT Press 2010. R. Anderson, *Security Engineering*, London: Wiley 2008.
[83] COM(1997) 503 final.
[84] COM(1997) 503 final, para. 2.2. In considering national security and law enforcement concerns, the Commission argued that regulating encryption would not stop targets of investigations from using it, signaling the attribution problem and steganography (information hiding) as tactics.
[85] For a comprehensive overview of the debate, see S. Andrews, *'Who Holds the Key? A Comparative Study of US and European Encryption Policies'*, The Journal of Information, Law and Technology, 29. Feb. 2000, see: http://encryption_policies.tripod.com/international/andrews_290200_key.htm
[86] S. Andrews, *'Who Holds the Key? A Comparative Study of US and European Encryption Policies'*, The Journal of Information, Law and Technology, 29. Feb. 2000, para. 5.2.
[87] J. Blanchette, *The Digital Signature Dilemma*, Annals of Telecommunications, vol. 61 no. 7-8, 2006, p. 903-918.
[88] Directive 1999/93/EC, OJ L 13, 19 Jan. 2000.
[89] For example, supporting the US-influenced OECD Guidelines at the Ministerial Declaration of European Ministers of the 1997 Global Information Networks Conference in Bonn, Germany, para. 36: http://www.echo.lu/bonn/final.html
[90] In the Commission proposal for the E-Commerce Directive, recital 15 contained an explicit reference to cryptography, mandating Member States to abstain from the restriction of its use. COM (1999) 247. That wording was later removed in the Council Common Position of 28 Feb. 2000, 14263/1/99 REV 1, p.7, see: http://register.consilium.europa.eu/pdf/en/99/st14/st14263-re01.en99.pdf.

provide new perspectives on the regulation of encryption and role of intelligence agencies beyond the crypto wars of the 1990s.[91]

Definition

'Security' is not defined in the eSignatures Directive. Art. 8 mandates that the provision of security products must comply with data protection measures of the Data Protection Directive and the Telecoms Package. The Annexes to the Directive contain several security requirements for regulated entities that mostly appeal to the integrity attribute of the c.i.a. triad, and that apply to a small set of stakeholders (see 'scope', below).

The omission of a definition has important consequences, that can be demonstrated by looking at alegislative development in the 90s. The 1997 Commission Proposal for the Directive prohibited private cryptographic keys to be stored by the trusted third parties that provide them, called Certificate Service Providers ('CSPs'; generally known as Certificate Authorities, 'CAs').[92] In the Council Common Position, however, and ultimately in the eSignatures Directive, this requirement was removed, ostensibly under fierce pressure from the U.K. and U.S. Government.[93]

The question of private key storage by the CA is an essential part of any *confidentiality* and *integrity* assessment. Private keys need to remain private for encryption to work, since a compromise of a private key entails a fundamental breach of trust and security. It enables encrypted information to be intercepted or modified by a man in the middle attacker.[94] Arrangements for private key recovery – such as key escrow and the 'Trusted Third Party' construction – are designed to enable surveillance and intelligence gathering. At the same time, attackers beyond intelligence and law enforcement agencies can exploit weaknesses in such arrangements.[95] A security definition in line with the c.i.a. triad would arguably spur a more explicit political debate about the omission of such a critical prohibition, rather than have it tucked away in one of its Annexes.

Scope

The Directive applies to CAs in general, but the important provisions, such as the security requirements, only apply to those CAs that issue so-called 'qualified certificates'.[96] The original Commission proposal applied to all CAs, regardless the type of certificate issued. But the scope was limited by the Council during its legislative process. The qualified certificates are a tiny subset of certificates issued, and used in specific contexts such as E-Government communications. The Council added the 'qualified certificate' category to the Annex, with the effect that the vast majority of CAs, and the vast majority of certificates issued in ordinary web browsing, do not have to comply with the specific (weakened) security requirements.

Recent Legislative Action

[91] See for example S. Levy, 'How the Code Rebels Beat the Government Saving Privacy in the Digital Age', New York: Penguin Books 2001. The book title is interesting. Understandably enthusiastic at the time, the NSA revelations have made clear that the book's main thesis is over-optimistic, and may only hold up with regard to a very small subset of technologies such as TOR.
[92] Annex II sub [h], COM(1998) 297 final.
[93] Common Postion (EC) NO 28/1999, 1999/C 243/02. S. Andrews, *'Who Holds the Key? A Comparative Study of US and European Encryption Policies'*, The Journal of Information, Law and Technology, 29. Feb. 2000, para. 2.1.
[94] Arnbak & Van Eijk 2012.
[95] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, B. Schneier, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, CDT Report, Revised 1998 version. The paper can be accessed here: https://www.schneier.com/paper-key-escrow.pdf
[96] Defined in art. 2[10] of the eSignatures Directive as: 'a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.'

The European Commission launched a revision of the 1999 eSignatures Directive in June 2012, with a proposal for a Regulation on 'Electronic Identification and Trust Services' ('eID Regulation').[97] Like the GDPR in data protection, an eID Regulation would acquire immediate binding force across the EU upon its adoption,[98] without a need for implementation in the legislation of Member States.[99] The updates addresses various developments since 1999. Generally, the use of encryption across electronic communications has seen an immense growth, and today is seen as minimum standard for processing information.[100] The deep security breach at Dutch CA DigiNotar in September 2011 has propelled the update of the 1999 legislation, with considerable effort from The Netherlands for legislative action at the E.U. level.[101] The outcome of the review process is uncertain,[102] but the Commission proposal can be analyzed.

The Commission proposal does not include a definition for 'security'. The one relevant connection to a conceptualization is made in art. 11, where the proposal refers to the Data Protection Directive when regulated entities process personal data. Without a definition of security, the legislator does not give any guidance how the c.i.a. triad operates with regard to trust service providers, and how to balance competing interests.

As to its scope, qualified and general 'trust service providers' (including CAs) are to be regulated – an approach similar to the original 1997 Commission proposal. Moreover, the proposal contains general security requirements, a security breach notification and liability provisions for both types of trust service providers,[103] with a stricter security requirements for qualified trust service providers such as more rigorous authentication of clients.

The technical and legal analytical depth of the accompanying documents is generally not convincing. The details of how trust service providers should assure communications security are to be determined by delegated acts of the European Commission. While the Commission includes both types of trust service providers, critical stakeholders in encrypted communications, such as web browser vendors or website operators are left untouched. Arguments in favor or against the policy choice are not provided, other than it is deemed 'too complicated at this point.'[104]

1.1.5. *Cybercrime*

A fourth area is the approximation of criminal law regarding security breaches. The history of cybercrime legislation provides useful insights into E.U. conceptualizations of communications security. It is one of the early avenues for policymakers in different institutional branches across a wide range of nation states – beyond Europe – to reach a seemingly broad consensus in the information and communications security policy area. Its definitions are copied in the proposed 'Network and Information Security' Directive (see section 1.1.6.).

[97] COM/2012/0238 final, procedural file 2012/0146 (COD).
[98] The US National Institute for Standards and Technology (NIST), on the other hand, is opting for a multi-stakeholder solution and organizing a workshops aimed at non-regulatory policy and technical resolutions to overcome the systemic vulnerabilities. See: See: http://www.nist.gov/itl/csd/ct/ca_workshop.cfm
[99] Indeed, numerous Member States have expressed concern with the choice of the legal instrument. As the instrument seeks to ensure a minimum level of security, and Member States are free to ensure higher levels of security, these concerns will primarily reflect positions of Member States that are concerned with high information and communications security levels, quite similar to the Council debates in 1998. See EU Council, 17269/12, 7 Dec. 2012, p.7, 2012/0146 (COD).
[100] For instance in the health sector, See CBP, 'Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek', May 2013, p. 3. http://www.cbpweb.nl/downloads_rapporten/rap_2013-beveiliging-online-herhaalrecepten.pdf The offering of HTTPS by default was becoming the state of the art for leading internet companies on client-server connections, and has received an impetus with the Snowden revelations.
[101] See Arnbak & Van Eijk 2012.
[102] The Commission proposal is being considered by both the EU Parliament and the EU Council since June 2012, see 2012/0146(COD).
[103] See Arnbak & Van Eijk 2012.
[104] A comprehensive analysis of the proposal can be found in: Asghari, Van Eeten, Arnbak & Van Eijk 2013.

Much of today's E.U. cybercrime legislation finds it substantial basis in the 2001 Council of Europe 'Cybercrime Convention'.[105] The Cybercrime Convention had been in preparation by an expert committee since 1996.[106] Many national legal systems had already criminalized 'computer crimes' in the 1980s, and a Convention of this kind had been envisioned at least since 1989.[107] Until this day, the Convention enjoys a status as the widest adopted legislative treaty in this space. Several countries outside Europe have become a party to the Treaty, notably the U.S., Australia, Japan, and the United States. Russian and China have not, expressing concerns over sovereignty.[108]

At the E.U. level, the 2005 Council Framework Decision on 'attacks against information systems'[109] was updated in August 2013 with a Directive.[110] Changes in the 2013 Directive include the implementation 'illegal interception' from the Cybercrime Convention, increasing penalties for large-scale attacks (primarily aimed at deterring the spread of 'botnets') and impersonation and criminalizing the use of 'tools' that enabled attacks.[111] The latter move has received much criticism from security researchers for criminalizing legitimate security research, such as penetration testing by security consultants as well as responsible disclosure by ethical hackers.[112] To address legitimate uses of hacking tools, a direct intent requirement has been introduced in the Directive and further explained in recital 16 and 17 of the final version. This intent requirement had already been part of art. 6 of the Cybercrime Convention from its very outset.

Definition

The preambles and provisions in the Cybercrime Convention contain some of the earliest comprehensive conceptualizations of 'security'. One of its central preambles reads:

> *"Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;"*

The c.i.a.-triad forms a central part of the preamble and the provisions of the Convention. Title 1 of Chapter II is named after it: "Offences against the confidentiality, integrity and availability of computer data and systems." Art. 2-5 contain the substantial criminal law provisions on 'illegal access', 'interception' and both 'data-' and 'system interference'. The explanatory memorandum makes clear that the provisions are directly linked to c.i.a.-triad theory,[113] and drafted in a technologically-neutral way to ensure the durability of the Convention.[114] In the subsequent E.U. cybercrime legislation, however, the c.i.a.-triad would hardly be part of the legislative mindset. The c.i.a.-triad is not mentioned in the 2005 or 2013 legislation and explanatory documents. In addition, the explicit mention of botnets in the 2013 Directive provisions reveals a less technology-neutral mindset of the legislator.

---

[105] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, see http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. The Cybercrime Convention came into force in 2004.
[106] CDPC/103/211196.
[107] Council of Europe, *Computer-related Crime*, Rec. R (89) 9, see http://www.oas.org/juridico/english/89-9&final%20Report.pdf
[108] I. Brown & P. Sommer, Reducing Systemic Cybersecurity Risks, OECD/IFP: London 2011, p.85-86, see: http://www.oecd.org/dataoecd/57/44/46889922.pdf
[109] Council Framework Decision 2005/222/JHA, 24 Feb. 2005.
[110] Directive 2013/40/EU 'on attacks against information systems', OJ L 218/8, 12 Aug. 2013.
[111] COM(2010) 517 final, p. 8.
[112] See for instance R. Singel, *Watch Out, White Hats! European Union Moves to Criminalize 'Hacking Tools'*, Wired Magazine, 4. June 2012, see: http://www.wired.com/threatlevel/2012/04/hacking-tools/
[113] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, para. 43. See: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm
[114] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, para. 36. See: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

As mentioned before, art. 3 of the 2001 CoE Convention on the 'interception of communications' did not make it into the 2005 E.U. Cybercrime Directive, only into the 2013 version over a decade later. The interception article of the CoE Convention is one of the central provisions aimed at assuring confidentiality of communications of end users, and it had already been proposed in the 1989 Recommendation as deserving protection.[115] Moreover, it was addressed in the 1997 ECtHR *Halford v. The United Kingdom* case, that concerned illegal wiretapping of an employee of the U.K. police by her employer.[116] The explanatory memorandum of the Convention explicitly mentions *Halford*, and further mentions five ECtHR court cases to point at the constitutional dimension of the c.i.a.-triad and criminal law approximation in this space.[117]

In its 2002 proposal for a Council Decision implementing the Convention, the Commission copies several 'threats to information systems' from a Commission Communication in the 'network and information systems' cycle.[118] 'Interception' is mentioned, but is considered to be dealt with in electronic communications law (see section 1.1.3.).[119] But that particular policy cycle only deals with conventional telecommunications providers as stakeholders, and is of a public law nature, not criminal law. The Council, nor the Parliament report further raised the issue.[120] Later, in 2010, the Commission includes the provision without any further explanation in a proposal that would eventually become the 2013 E.U. Directive.[121] Whether or not the criminalization of such actions is desirable, the public documentation of the E.U. institutions doesn't even start to develop a vision what it sought to criminalize in 2005, and why 'interception' was not part of it. An understanding of the c.i.a.-triad could have made the omission of the interception provision in the 2005 Directive, and its inclusion in 2013, a topic of public debate.

The Cybercrime Convention preamble names 'deterrence' as a main rationale for the instrument. 'Deterrence' aims at sending credible signals to possible adversaries that attack is futile, because it spurs serious retaliation. The doctrine has been inspired by game theory and international relations studies, and was of decisive influence in Cold War diplomacy and beyond. [122]

The deterrence logic inherent in cybercrime policymaking may explain a puzzling prominence in the 2005 E.U. Council Decision of the threat of terrorist attacks on information systems, which apparently calls for strict cybercrime legislation at the E.U. level. But counterterrorism is the exclusive area of national security, and as such exempt from E.U. competence. Moreover, the effectiveness of counter-terrorism through deterrence in cybercrime legislation is contentious and warrants further examination (see section 1.2.).

---

[115] Council of Europe, *Computer-related Crime*, Rec. R (89) 9, 1989, p.53, see http://www.oas.org/juridico/english/89-9&final%20Report.pdf.
[116] ECHR Halford v. United Kingdom, Reports 1997 – III, 25/06/1997.
[117] ECHR Klass and others v. Germany, A28, 06/09/1978. ECHR Kruslin v. France, 176-A, 24/04/1990. ECHR Huvig v. France, 176-B, 24/04/1990. ECHR Malone v. United Kingdom, A82, 02/08/1984. ECHR Lambert v. France, Reports 1998 – V, 24/08/1998
[118] COM(2001) 298 final, p. 9.
[119] COM(2002) 173 final, p. 3.
[120] A5-0328/2002. The Parliament advocated a less strict regime, warned for the criminalization of legitimate actions, and amended the Commission Proposal to include fundamental rights safeguards across the text. The report was effectively neglected by the Council and in the adopted Decision. With the institutional structure of the time, the Parliament only needed to be consulted, rather than have the right to vote, with regard to matters of law enforcement policy in the Third Pillar of European Union policymaking.
[121] The legislative history of the 2013 Directive can be tracked through procedural number 2010/0273 (COD). The 2005 Council Decision through CNS(2002)0086. The interception article had been proposed in the European Commission proposal in
[122] T. Schelling, *The Diplomacy of Violence*, New Haven: Yale University Press 1966. Schelling shared a Nobel Prize in Economics with R. Aumann for "having enhanced our understanding of conflict and cooperation through game-theory analysis". His work on deterrence has had major influence in foreign policy and popular culture; conversations with film director Stanley Kubrick inspired the latter to make a film about deterrence theory, called Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb. See: http://www.hks.harvard.edu/news-events/news/articles/schelling-kubrick-strangelove

Conversely, the 2001 CoE Convention explanatory memorandum states that appropriate security measures themselves are "the most effective means" to prevent security breaches, rather than criminal law.[123] The 2013 E.U. Directive does the same in recitals 26-27, and even hints at imposing liability on providers that do not meet proportionate information security levels. Decades onwards in the cybercrime policy cycle, such comprehensive policy action has not materialized. The 'Network and Information Security' Directive proposed in 2013 aims to address this (see section 1.1.6.). The relationship between deterrence and actual effective network and information security policy deserves further attention (see section 1.2.).

Scope

The scope of the cybercrime policy cycle has been broad from the very outset. The Cybercrime Convention preamble, cited above, distinguishes a number of concepts that encapsulate the scope of cybercrime legislation. These concepts are further defined in art. 1 of the Convention:

> *a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;*
>
> *b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*
>
> *c) "service provider" means:*
> *i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and*
> *ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.*

The definitions seek to capture any device, data or provider imaginable in the electronic environment. Devices can be both stand-alone machines as well as networked, in whatever form. The definition of service providers covers the entire range of providers: telecoms, information society services, and all other service providers conceivable in the electronic environment fall within the scope of the legislation. These definitions have not substantially changed over time, and are again part of the 2013 Directive. So along with a broad range of policy issues beyond information security, comes the broadest set of stakeholders imaginable. In today's information-mediated society, the cybercrime policy cycle thus encapsulates nearly everything, every time.

Apart from attacks *against* information systems, the measures also address actions "where computer and telecommunication systems are used as a means to attack certain legal interests."[124] These actions are outlined in artt. 2-10 of the 2001 CoE Convention. Of note are the criminalization of child abuse and intellectual property infringements.[125] In doing so, the Convention enable a possibility to conflate cybercrime with a wide range of other interests, that are not directly related to the network and information 'security'. This can be witnessed in the myriad of cybercrime and cybersecurity strategies seen across the E.U. in recent years.[126]

[123] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, para. 45. See: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm
[124] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, para. 36. See: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm
[125] The explanatory memorandum also points at 'hate speech', but notes that a consensus could not be reached because of freedom of expression concerns – hate speech was to be treated in an additional protocol to the Convention, which would be adopted in 2003. Council of Europe Convention on Cybercrime, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, CETS 189, Budapest 28 Jan. 2003, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
[126] See section 1.2.6.

1.1.6. *The Proposed 'Network and Information Security' Directive*

In February 2013, the European Commission proposed a 'Network and Information Security Directive' (NIS Directive).[127] The proposal is the main policy action of the 'European Cybersecurity Strategy',[128] jointly prepared by the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy. The European Cybersecurity Strategy expresses ambitions and some commitments about raising awareness, research agenda's and promoting a market for cybersecurity largely similar to the 1992 Council Decision (section 1.1.1.).

The Directive, however, would be the first comprehensive legislative instrument in the broader area of 'network and information security'. If adopted in the form the Commission proposes, the Directive would significantly break with the voluntary and E.U. Council dominated approach that has been in place since the 1992 Council Decision. 'Network and information security' policies would after more than two decades be addressed in binding EU legislation.

The proposed Directive contains legislative obligations for Member States to adopt national strategies and action plans and to set up CERTs (Chapter II, art. 4-7), as well as cooperate with one another by sharing risk and incident information and installing early warning systems, coordinated by ENISA (Chapter III, art. 8-13). In addition, the proposal imposes minimum security requirements, security breach notifications and enforcement on 'market operators' (Chapter IV, art. 14-16).[129] These obligations are without prejudice to those arising from the data protection regime (art. 1[5]). Determining the details of a range of these provisions is often delegated to implementing acts adopted by the Commission. The Commission grants itself substantial authority: implementing acts have binding force unless Council or Parliament opposes (art. 18[2-5]).

Definition

The definition in art. 3[2] of the Directive is nearly identical to the definition formulated the ENISA Regulation 2013 mentioned before (section 1.1.1.):

> *"security" means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;*

The recitals, explanatory memorandum and other accompanying documents do not provide any argumentation as to why the definition is chosen, or what it implies. Neither does the documentation explain why the definition has been slightly adapted compared to the definition of the ENISA Regulation: 'unlawful' has been removed from the definition, while 'events' and 'actions' have been changed into 'action'.[130] In that sense, the Commission still fails to provide guidance how to balance the security attributes of the c.i.a.-triad. But the fact that the c.i.a.-triad, is, as a first, comprehensively adopted in a E.U. Directive with considerable network and information security provisions provides an opportunity to develop a vision of what security means, and how its underlying values should be balanced against one another.

Scope

The scope of the proposal is determined by two different definitions, i.e. 'network and information system' and 'market operator'. The 'market operator' category contains several exemptions that exclude critical stakeholders from the security provisions of the Directive. Taken together, what

[127] COM(2013) 48 final, 7 Feb. 2013, legislative procedure 2013/0027(COD). Impact Assessment to the proposed Directive: {SWD(2013) 31-32 final}.
[128] JOIN(2013) 1 final, 2 Feb. 2013.
[129] According to recital 25, the concept of security by design is clearly excluded from the regulatory measures in art. 14.
[130] Perhaps, 'unlawful' was removed to make clear that the Directive would not have any impact on legislative action in the field of cybercrime. The proposal clearly excludes criminal law from its scope in art. 1[4].

remains is a regulatory patchwork that both fails to provide legal certainty to providers, and to meaningfully address end-user interests.

Chapter II and Chapter III of the Directive cover 'network and information system' policy, and contain regulation on a.o. national strategies, capabilities and international cooperation. The Commission proposal contains a definition for 'network and information system' in art. 3[1]:

> *"network and information system" means:*
> *(a) an electronic communications network within the meaning of Directive 2002/21/EC, and*
> *(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as*
> *(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.*

Again, the proposal and its accompanying documents do not provide any guidance on the definition itself. Sub a directs that the term is broader than networks regulated under the Telecoms Package (see section 1.1.3.). But sub b and c rip the issue open. The concepts of 'devices' and 'computer data' seek to capture data in electronic form – as opposed to non-electronic data (such as paper filesystems). While not motivated by the Commission, the choice to copy the definitions from the 2013 Cybercrime Directive implies that the provisions of Chapter II and Chapter III on national strategies, capabilities and international cooperation cover as broad a ground as 'cybercrime' law; all electronic systems and data (see section 1.1.5.).

For Chapter IV, however, the Directive also creates subset of stakeholders under the definition of 'market operator'. Along with public authorities, the security obligations of Chapter IV of the proposal would only apply to this set of stakeholders. The term 'market operator' is defined in art. 3[8a] and art. 3[8b], with a non-exhaustive list in Annex II:

> *(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;*
> *(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.*

The definition of 'market operator' identifies two groups. Firstly, the proposal specifically identifies several critical infrastructure sectors in Annex II (sub b). It bypasses the Council and Member State control of the designation of European Critical Infrastructures (see section 2.2.4). This is probably an unrealistic aim for the final Directive, as the E.U. Council has already voiced critique.[131]

The second group covered by the 'market operator' definition are the so-called "information society service providers"[132] that "enable the provision of other information society services" (sub a – discussed in section 1.1.3.).[133] Annex II and the Impact Assessment of the proposal point at which providers would fall under the definition: e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores. According to the Commission, stakeholders that perform similar functions in communications, such as providers of smartphone apps and some VoIP providers,[134] don't fall under the definition.[135]

---

[131] In its first debate of the proposal, the Council has already criticized why some sectors had been included and others not, and what the impact of the definition would be on the competitiveness of industry and innovation. 2013/0027(COD), Debate in Council, 6 Jun. 2013.

[132] See art. 1[2] Notification Directive 1998/48/EC: 'Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'

[133] The element of "enabling" was probably inserted to focus on negative consequences of one service for another service, perhaps in the spirit of critical infrastructures. Recital 24 is quite unclear in its wording, but the term 'disruption' in the recital might point at a focus on availability interests, when one service depends on another. The Impact Assessment seems to confirm this reading: "we consider relevant those actors whose services, delivered through the Internet, are empowering key economic and social activities and which have a significant impact in case their activities are suspended for a couple of hours." SWD/2013/032 final, Impact Assessment, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT

[134] See section 1.1.3. for a detailed analysis of VoIP providers under the Telecoms Package.

The 'market operator' definition and the explanation of the Commission are problematic for several reasons. If one strictly follows the definition of an "information society service", many apps would also fall under it, rendering the explanation of the Commission incorrect.[136] Moreover, from an end user perspective, there is direct interaction with the information society services at the edge of the information value-chain – such as apps. Users directly depend on app security measures and obligations to protect their confidentiality and integrity interests. For a user, there is no difference between accessing Facebook via your browser or via the app, or chatting with a friend via the Facebook app or any other instant messaging app. A functional and user-centric approach would apply the security requirements and breach notifications of art. 14-16 to all information society services. The proposal seeks to cover user interests with the data protection and telecoms package references in art. 1[5], but fails to appreciate that these policy cycles leave large gaps in end-user protection. The Commission does not contemplate on the full range of the c.i.a.-triad, and how to balance these interests. In this policy cycle, at least, such a comprehensive approach would be consistent with its definition of 'security' articulated in art. 1[3].

Even *within* the limited 'market operator' definition, a large number of stakeholders are actually exempted from the security measures of art. 14. Three exemptions are relevant to communications security. First, according to art. 1[3], 'electronic communications' and trust service providers are exempted from the relevant security provisions and referred to their respective regulatory regimes in the Telecoms Package (see section 1.1.3.) and encryption regulations (see section 1.1.4.). Especially with regard to the latter, the current regulatory regime does not provide similar security measures, and it remains to be seen whether the 2012 Commission proposal for an eID Regulation will contain such measures after the legislative battle in the Council and Parliament.

Second, art. 14(8) exempts micro-enterprises with a personnel of 10 or below and an annual turnover or balance sheet of less than 2 million Euro.[137] Recital 27 and the explanatory memorandum provides no additional explanation. The Impact Assessment contains one sentence that again points at prioritising continuity of service provision for other businesses, rather than confidentiality or integrity interests of end-users.[138] Balancing the regulatory burden on start-ups with the persistent problem that security only comes as an afterthought in product and service development is one of the pressing challenges in communications security policymaking, but the Commission does not start with setting out a vision how to address it.

Third, and most importantly, soft- and hardware developers do not fall within the scope of the Directive altogether, and are explicitly exempted in recital 24. This goes to the heart of security policymaking, as all information and communications practices depend on soft- and hardware. Their persistent vulnerabilities are a fundamental problem in information and communications security. Even in the survey conducted by the Commission for its Impact Assessment, 36.1% of the most frequent incidents are reportedly caused by soft/hardware failures.[139] The field of security economics illustrates that software vulnerabilities are not so much a technical problem, but are caused by deep market failures in the industry; information asymmetry, liability dumping, 'winner take all' and network externalities all apply.[140] Correcting market failures may call for legislative intervention, or in

---

[135] Impact Assessment - SWD(2013)32 final - 7/2/2013

[136] Any app store lists thousands of apps that are a "service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." The definition is discussed in section 1.1.3.

[137] Commission Recommendation 2003/361/EC, OJ L 124/39, Annex I, art. 2[3].

[138] "On the other hand, micro companies are less critical for the overall continuity of the services given that incidents affecting them may not have a sufficiently wide reaching impact on society as those incidents affecting larger businesses." SWD/2013/032 final, Impact Assessment, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT

[139] SWD/2013/032 final, Impact Assessment, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT

[140] One of the first papers to address the security economics of software vulnerabilities is R. Anderson, 'Why Information Security is Hard — An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications Conference, pp. 358-65. Software vulnerabilities on p. 359. A recent helpful survey paper comes from T. Moore & R. Anderson, *'Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioural Research'*, Harvard CRCS Technical Report, March 2011. The report presents an overview the field of internet security economics, and points to

any event its consideration. Exempting these stakeholders from the Directive altogether seems indefensible, but the Commission fails to even elaborate upon its choice, merely stating that "software developers and hardware manufacturers are not providers of information society services and are therefore excluded".[141]

Recent Legislative Action

The legislative action around the proposed Directive will be the essential indicator of the ambitions of the EU legislator in the field of communications security. The proposal is currently under consideration by the Parliament and Council; both seem critical. The Council seems to advocate voluntary approaches for coordination on the EU level and the possibility of (bilateral) legislative action at the Member State level,[142] the same approach that has been advocated since 1990 (see section 1.1.1.). The European Parliament amendments of 13 March 2014 already exclude information society services altogether.[143] At the time of writing, the proposal is still at the E.U. Council for is first reading, so the outcome of the proposed Directive is uncertain at this point. But at the face of it, robust conceptualizations of 'security' or substantial security measures seem far away from adoption.

1.2. ***Evaluation: 6 Conceptualization Research Themes***

It is commonplace that networked communications challenge existing concepts, and that network and information security is a top policy concern. With such commonplaces, it may come as a surprise that so little research has been conducted on the actual conceptualizations in E.U. 'security' policy. The descriptive, internal legal analysis of the previous sections enables an evaluation of current 'security' conceptualizations in the E.U. regulatory framework. What insights has the historical analysis generated about current state of information and communications 'security' legislation, its definitions and its scope?

The historical analysis of the previous section enables the identification of five distinguishable policy cycles in E.U. network and information security policymaking: data protection, the telecoms package, encryption, cybercrime and network and information security. The definitions of 'security' in these cycles were mapped and analyzed against the c.i.a.-triad, a consensus conceptualization of 'security' in computer science literature. The following figure summarizes the current state of affairs in E.U. 'security' policymaking, as of March 2014:

E.U. 'Security' Conceptualizations	***Confidentiality***	***Integrity***	***Availability***	***Scope***
Data Protection	Personal data, may include network	Personal data, may include network	Personal data, may include network*	Controllers and Processors 'personal data'
Telecoms Package	communications and information**	unclear, probably only personal data	priority issue, but phrased as 'integrity'	Network and Service Providers in Telco Markets
Encryption	undefined, linked to data protection	undefined, prioritized in Annexes	undefined, not covered in provisions	Qualified Trust Service Providers
Cybercrime	undefined, but covered in provisions	undefined, but covered in provisions	undefined, but covered in provisions	Any system, device, all computer data
Critical infra. and "NIS" proposal	not yet, but explicitly in Directive proposal	not yet, explictly in Directive proposal, adds 'authentiticity'	not yet, but explicitly in Directive proposal	network and information system', 'market operators'

* does not cover temporary availability
** 'information' in terminal equipment ('cookie provision')

dozens of relevant references explaining market failures in internet security. On p. 3 and p. 4, market dynamics causing persistent software vulnerabilities are explained.

[141] Recital 24.

[142] 2013/0027(COD), Debate in Council, 6 Jun. 2013. This has also been expressed in Council Resolution 2009/C 312/01, Conclusion Council and European Parliament, 27 May 2011.

[143] Decision by Parliament, 1st reading/single reading, T7-0244/2014, 13 Mar. 2014.

The conceptualizations of 'security' vastly differ per policy cycle. The result is a complex patchwork of conceptualizations, legal protections and enforcement mechanisms across today's five policy cycles. When it comes to scope, legislation is rather informed by opportunistic economic and political motives and a market structuring legacy than the actual function of a specific communications setting and insights from security economics. Another general observation is how the crypto-wars of the mid 1990s still cast their shadow over today's 'security' conceptualizations. Many a sensible 'security' measure was proposed by the European Commission over two decades ago, but not adopted because of resistance of several Member States in E.U. Council – and perhaps forgotten today.

From the historical analysis six cross-cutting network and information security 'themes' have emerged that warrant further research. These research themes are further developed in the next sections.

1.2.1. *The Guiding Force of the c.i.a.-Triad?*

The regulatory initieatives of the '80s and early '90s connect their 'security' conceptualizations to the consensus definition of the c.i.a.-triad in computer science literature. These connections to the c.i.a.-triad – and how to interpret confidentiality, integrity and availability – are made throughout the first influential 'security' laws of those early years: the CoE data protection convention, the CoE cybercrime convention, and most explicitly in the 1990 European Commission proposal for a Council Decision 'In the Field of Information Systems'.

E.U. legislation, on the other hand, has not followed the c.i.a.-triad uniformly from its very outset, save for indirect references in the Data Protection Directive. The Telecoms Package adopts its own vocabulary, encryption policies refer to data protection for terminology, while cybercrime legislation of the E.U. does not follow the c.i.a.-triad at all. The more recent 'network and information security' policy cycle is the only one to refer explicitly to the c.i.a.-triad, but its laws and policies have created a weak legislative and institutional framework in which ENISA policy advice is hardly followed.

It seems that copying definitions from earlier documents has become standard practice. In doing so, no guidance is provided as to the meaning or intentions of the legislator in a particular instrument; for instance, on how to interpret 'network' against existing definitions in telecommunications law, or how 'authenticity' differs from 'integrity' or how to balance confidentiality, integrity and availability interests when these security attributes conflict.[144] Such guidance is essential, because it creates the necessary framework for interpreting subsequent policy actions of the legislator and other regulatory authorities, notably when formulating delegated acts or negotiating standards. Contrary to best practices in data protection,[145] the details of 'security' policies are, mostly, delegated to the executive branch of the E.U. or to standards bodies without normative input, generating legal uncertainty and sometimes technologically insecure outcomes (see section 1.1.3. and below). When the devil is in the details, delegating them make the conceptualization of 'security' at the E.U. level somewhat of an empty vessel.

Current policies leave significant gaps in network and information security protection, rather than protecting the confidentiality, integrity and availability regardless of the type of information that traverses a certain network. It spurs the research question if, and how the c.i.a.-triad constitutes a useful conceptual framework for policymaking, and whether its inclusion in 'security' definitions would make a difference in actual policymaking. Does, or should, the c.i.a.-triad stimulate or force policymakers to assess whether confidentiality, integrity and availability goals are met? Can a

[144] Arnbak & Van Eijk 2012. See section 2.
[145] For example, the Data Protection Directive has provided critical normative input to negotiating an international Do Not Track Standard. See Art. 29 WP, WP 188, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, para. 10; R. Madelin, Letter to World Wide Web Consortium Tracking Prot. Working Group, 21 June 2012, http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0604/Letter_to_W3C_Tracking_Protection_Working_Group.210612.pdf .

stronger theoretical understanding of what 'security' actually is help legislators and enforcement to focus on critical security issues?

As an example to illustrate the relevance these questions, one can point at the omission of private key storage that has not been subject of any public scrutiny in legislative debates around the 1999 eSignatures Directive. One possible explanation is a lack of technical understanding of legislators, not realizing how the c.i.a.-triad had provided the conceptual framework in earlier security policies. Another, more pragmatist possibility is that the prohibition was conveniently omitted in the final text and rushed through E.U. institutions by a pre-Lisbon E.U. Council. The latter possibility is not that speculative, as the text was negotiated at the height of the crypto wars in the second half of the 1990s. In any event, the recently proposed update of the 1999 Directive will provide a fresh opportunity to analyze the guiding force of the c.i.a.-triad, as well as the priorities of the E.U. legislator when it comes to encryption policy.

1.2.2. *The Constitutional Dimension of the c.i.a.-Triad*

The security attributes confidentiality, integrity and availability have a clear connection with constitutional values such as communications secrecy, privacy, data protection and communications freedom. The concept of 'correspondence' does include the integrity and confidentiality of electronic communications in art. 17 of the UN International Covenant on Civil and Political Rights and art. 8 of the European Convention on Human Rights (ECHR).[146] Integrity has a connection with data subject rights under data protection, a separate constitutional value in art. 8 of the relatively recently adopted E.U. Charter of Fundamental Rights. And in a networked communications environment in which bulk metadata surveillance seems to be the rule rather than the exception, network and information security may become, or is already instrumental in the enjoyment of a broader range of fundamental rights, such as freedom of religion and freedom of association.[147]

From the very inception of the ECHR, its fundamental rights protection adopts a functional approach with regard to the main provisions. Steenbruggen has observed this as the root cause for the flexibility of the ECHR and the ability of its Court to provide protection regardless of the technological reality of tomorrow. Indeed, case-law of the ECtHR is already responding to the socio-technical changes and increased dependence of networked electronic communications.[148] In 2008, the Court established that ensuring the technical security of medical health records through information security legislation is a constitutional obligation for all Member States of the Council of Europe. The positive right to information security, according to the Court, explicitly includes such safeguards as access controls and access logging.[149] A July 2013 ruling of the ECtHR in the context of cloud communications expanded the scope of the constitutional protection of the Convention to "all data on a server", regardless of whether that data is 'personal data' that identifies a (legal) person.[150] As such, the positive obligation to ensure technical security may extend to, for example, confidential corporate information.

While communications confidentiality has a long tradition of protection under the ECHR, rulings are case-specific. The specific constitutional interpretation of the c.i.a.-triad may therefore depend on the specific communications setting at hand. These observations serve to illustrate that the interplay between network and information security and its c.i.a.-triad and constitutional values of the E.U. is a complex matter and a crucial topic for further research.

[146] CCPR art. 17, General Comment 16/32, §8. In depth: M. Nowak, 'Privacy: Art. 17 CCPR', p. 403, in: M. Nowak, 'U.N. Covenant on Civil and Political Rights: CCPR commentary', Kehl am Rhein: Engel 1998
[147] See K. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*. Boston College Law Review, Vol. 49, No. 741, 2008.
[148] Steenbruggen has observed the open wording of the ECHR as the root cause for the flexibility of the ECtHR and its ability to provide protection regardless of the technological reality of tomorrow. Steenbruggen 2009, p. 54.
[149] I. v. Finland, App. No. 25011/03, 17 Jul. 2008, para. 47. De Hert 2010, p. 49.
[150] para. 106 BERNH LARSEN HOLDING AS AND OTHERS v. NORWAY 14/03/2013

With such a clear connection, E.U. policies need to observe the normative guidance offered by its constitutional regime. Fundamental rights circumscribe the leeway for policymaking. But E.U. policies hardly ever elaborate upon it, other than including a short reference to fundamental rights in a recital or explanatory document. The explanatory memorandum of the Cybercrime Convention of the CoE, on the other hand, mentions five ECtHR court cases that regulate any cybercrime policy.[151] In addition, European Commissioners for the first time took an oath to uphold the E.U. Charter of Fundamental Rights in 2010,[152] and the E.U. is on its way to accede to the Council of Europe as a full member.[153] These important legal and political developments exacerbate the lack of normative vision in E.U. 'security' policymaking as an alarming observation, and add to the relevance of the constitutional dimension of the c.i.a.-triad as an important topic for further study.

1.2.3. *Data Protection Path Dependency*

The data protection policy cycle is highly influential across the other policy cycles: its security provision is referred to, and thus determines how 'security' is understood in E.U. 'encryption' policy as well as for a substantial part of the Telecoms Package. The recently proposed 'Network and Information Security' Directive itself excludes data protection from its 'security' competence; instead it creates another cross-reference in E.U. 'security' policymaking to data protection. In other words, network and information security policy and enforcement in these policy cycles will largely depend on how 'security' is conceptualized in light of the 'personal data' conceptualization, and enforced in its policy cycle. Conversely, a change in the data protection policy cycle will have immense impact in 'security' policymaking in the other policy cycles.

The data protection path dependency of the other policy cycles creates gaps in legal protection for communications security. As observed in section 1.1.2., personal data are only a subset of the information and communications that deserve to be secured. Path-dependency with 'personal data' leaves a wide range of data – such as government or corporate data – unprotected. In addition, the definition of 'personal data' is subject to intense debate in the ongoing revision of the data protection framework. The possible introduction of a new category of 'pseudonymous data' risks leaving more data traversing electronic communications networks unprotected. Not only in data protection law, but in 'encryption' policy and a large part of the Telecoms Package as well. Data protection legislators may not be aware of the impact of their decisions beyond data protection because of these links to those other policy cycles. And related to the constitutional dimension of the c.i.a.-triad, is the possibility that policymakers believe constitutional values have been 'covered' because of the existence of data protection law. These developments beg the question to what extent network and information security policymaking needs to disconnect itself from its foundation in the data protection policy cycle going forward.

In the encryption policy cycle, for example, the silent disappearance of the private key storage prohibition for CAs, a critical security requirement in the 1997 Commission proposal that in the end did not make the 1999 eSignatures Directive, is a case in point (see section 1.1.4.). Because of the omission, the law as it stands makes no point of prohibiting private key storage or, in other words, enabling key escrow. A serious risk of key escrow includes exposing encrypted communications to the destruction, loss, alteration, disclosure or access that art. 17 of the Data Protection Directive claims to prevent.

On the face of it, the 'personal data' path-dependency may have made the relevance of the omission less obvious. Understood as a data protection issue, private key storage has become 'lawful' by removing its prohibition from the signatures legislation; as such it is merely an issue of 'consent' or

[151] ECHR Klass and others v. Germany, A28, 06/09/1978. ECHR Kruslin v. France, 176-A, 24/04/1990. ECHR Huvig v. France, 176-B, 24/04/1990. ECHR Malone v. United Kingdom, A82, 02/08/1984. ECHR Lambert v. France, Reports 1998 – V, 24/08/1998

[152] 'European Commission swears oath to respect the EU Treaties', IP/10/487, Luxembourg, 3 May 2010.

[153] See for the up-to-date status quo of the negotiations: http://hub.coe.int/web/coe-portal/what-we-do/human-rights/eu-accession-to-the-convention

'legal obligation' as a legal ground for data processing that can be dealt with in a CAs terms & conditions. But as a network and information security issue, private key storage is the ultimate backdoor, a red flag, a glaring vulnerability. In the current legislative debates around its successor, the eID Regulation, the proposals still refer to the data protection policy cycle, and fail to include the c.i.a.-triad itself. As such, the data protection path dependency has a perverse effect on communications security, that is currently not at all understood or even addressed in research and policy.

1.2.4. *Scope: Re-orient Actor-Based Policies Towards a Focus on Functionality?*

In two of the essential policy cycles, the Telecoms Package and 'encryption', the scope of the leading legislative instrument is determined by whether or not a stakeholder falls within a certain definition of an 'actor'. Stakeholders offering the same communications functions can be regulated (or not) in completely different ways, because the stakeholder happens to be (or not) a 'qualified trust service provider', 'information society service' or a 'public electronic communications service'. The data breach notification in the Telecoms Package is a case in point (see section 1.1.3.).

Going forward, the current actor-based scoping in 'security' policy is a problematic approach. It leaves increasing gaps in legal protection, for reasons including technological turbulence, convergence and conflicting underlying policy rationales. In recent years, the electronic communications environment has seen rapid change with digitization, convergence and wide user adoption of networked electronic communications in desktop and mobile environments. Threat landscapes are constantly evolving. New companies that provide services that nobody could have imagined yesterday, have already become multi-million enterprises. Basing a regulatory effort on a particular actor may have lost its relevance completely as soon as an instrument is adopted.

Actor-based scope definitions are sometimes crafted with different policy rationales in mind, most prominently the harmonization of the internal market of the E.U. In the case of VoIP providers, the Telecoms package merely includes new manifestations of networked communications when they operate in similar markets that are regulated to counter the risk of significant market power; so VoIP falls within the Telecoms Package when it directly competes with fixed telephony (in case of SkypeOut, see section 1.1.3.). The vast majority of VoIP communications that do not compete on the market, but offer nearly identical functionality (voice communications) go unregulated. In an internal market mindset that is usual to E.U. law, market considerations can stretch the scope of the Telecoms Package, but communications security considerations cannot. It points towards the current priorities in these policy cycles. But a rigorous conceptualization of 'security' could inform an approach that would depend less on regulatory or political legacies, and more on addressing today's gaps in communications security protection for end users.

While the European Commission seems to have signaled that the current limited scope of 'security' regulation is too limited, its proposals still focuses on actors. And the newly proposed Network and Information Security Directive appears to have the same weaknesses. As noted in section 1.1.1. and 1.1.6., its definition of 'network and information system' concerns all stakeholders involved, but the proposal leans heavily on a new definition of 'market operator' that exempts a wide range of critical stakeholders. Notable examples are software and hardware businesses, while security economics explicitly informs that especially soft- and hardware businesses should be subject to regulation that designed to address market failures (see section 1.1.6.). Information society services may not be included in the scope of the Directive altogether, as the Parliament has excluded these stakeholders from the Directive's scope. The actor-approach is, indeed, vulnerable to industry lobbying. The strength of the software lobby in Brussels and Strasbourg is well-known and over decades old.[154]

[154] The Business Software Alliance has been critical of the proposed Directive. Now that 'information society services' have been excluded from its scope, BSA members are no longer regulated under the proposal. Now, the BSA welcomes the legislation on its website: 'BSA Welcomes European Parliament Vote on Proposed Network and Information Security Directive', Strasbourg 13 March 2014, see: http://www.bsa.org/news-and-events/news/2014/june/eu06062014eusecurityrules

There are other ways to scope 'security' policies; constitutional law, data protection and cybercrime adopt different approaches in their policies. As noted in section 1.2.2., the ECHR has since 1948 adopted a flexible, functional approach towards fundamental rights conceptualizations – rather than one strictly depending on a technology or stakeholder. Cybercrime is of the broadest scope imaginable. Rather than focusing on actors, it seeks to augment security through criminalization. The effectiveness and underlying political nature of the cybercrime approach is further discussed in section 1.2.6.

The scope of data protection does not primarily depend on the actor involved, but on the definition of 'personal data' as noted above. Moreover, it is stretched when network security is instrumental for certain types of (sensitive) personal data. This path dependency has its limits, but sometimes it may work for specific communications settings. The HTTPS enforcement actions by Data Protection Authorities mentioned in section 1.1.2. come to mind. Here, the pragmatic approach was informed by public interest and expectation, in which data protection indirectly solves a particular network security issue that in fact directly connects with the encryption policy cycle. This is network and information security policy by proxy: it only occurs because the more appropriate policy cycle has a weak enforcement structure and only includes security requirements for 'qualified trust service providers', not general CAs. Data protection may have come to save the day in this example, but gaps in legal protection remain more generally.

Current E.U. security conceptualizations fail to capture similar communications functions (voice, chat, text, etc.), offered by different stakeholders. The quite imminent pressure on the conventional actor-based scope conceptualizations and different approaches in other policy cycles render the following research question: do we need a comprehensive conceptualization of network and information security, perhaps even in an integral legal instrument? Should such a holistic security conceptualization be informed by fundamental rights, cybercrime and/or data protection conceptualizations? An integral instrument could overcome the conceptual scoping weaknesses of the current five policy cycles, and provide a holistic approach to network and information policy – both in definition (possibly along the c.i.a.-triad) and in scope. Such an instrument could scope policy along functional lines, rather than the actor-based approach that currently impedes E.U. network and information security policy. On the political level, it seems impossible that anything happens anytime soon.

What would a functional approach towards scope look like? If Alice were to send Bob an e-mail using a webmail provider such as Gmail, the list of intermediaries involved in securing their private communications could include Google, Alice or Bob's internet access providers, a range of routing intermediaries at internet exchanges in between, the open Wi-Fi network Alice has joined in her favorite coffee place, their operating systems manufacturers, their devices (smartphone, computer, tablet, etc.), web browser and router vendors – and the list may go on. At all these intermittent points between Alice and Bob, communications security can be implicated. But most of them do not fall within by the current actor-based E.U. regulatory framework. A functional approach would inform that it does not matter much whether Alice contacts Bob through e-mail offered by their internet access provider, or Google – similar to fundamental rights and cybercrime regulations are offered across the board (for example prohibiting interception), regardless of a particular actor.

Another informative area of scholarship is security economics.[155] Security economics posits that security fails when organizations or users that defend the systems lack an incentive to do so. Through its incentive-based analysis, security economics has explained various persistent security failures throughout the electronic communications environment using economic concepts, such as information asymmetries, externalities and liability dumping. In earlier work on HTTPS governance, we have

[155] See section 1.1.6. A good overview is given in T. Moore, R. Anderson, 2011. Internet Security. In: Peitz, M., Waldfogel, J. (Eds.), The Oxford Handbook of the Digital Economy, Oxford University Press. See: ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

called the combination of functional conceptualization and security economics analysis a 'value chain' approach.[156] The combination of a functional approach to conceptualization and the application of security economics analysis does, however, come with complexities. Broad and functional 'security' conceptualizations need to be aligned with detailed regulatory interventions that are designed to address the technical specificities of a particular communications setting and its market incentive structure. This dynamic – broad conceptualization, specific regulatory application – surely necessitates further technical, economic and legal research.

1.2.5. *E.U. Regulatory Competence: Structural National Security Capture*

In the start of the 1990s, and across most of the policy cycles, the European Commission suggested c.i.a.-triad inspired network and information security conceptualizations and robust policies. The E.U. Council, however, has been consistently evoking national security as an obstacle to E.U. competence in the 'network and information security' policy cycle. The Council Decision of 1992 was a critical moment in that regard, leaving the main competence in the area of information and network security for European Member States ever since (see section 1.1.1.). In other policy cycles, legal provisions have been substantially weakened. Examples include removing end-to-end encryption as a security requirement in the predecessor of the E-Privacy Directive in the early 1990s (see section 1.1.3.) and removing a prohibition for CAs to store private keys of SSL-certificate customers in the final version of the 1999 eSignatures Directive (see section 1.1.4.). The deliberate weakening of encryption standards in GSM in the 1990s that impacted mobile communications security ever since is another case in point (see section 1.1.3).

Extrapolating from these cases, we can observe that the national security capture manifests in various forms: *explicitly* in E.U. Council deliberations and statements by government representatives, *implicitly* in E.U. Council amendments to Commission and Parliament proposals for legislation that omit critical provisions, and *secretly* in the actual implementation process of legislation by subtly subverting standards and encryption policies. The latter strategy falls under the category of "kleptography", a centuries old practice that is defined as "persuading the party to be intercepted to use a form of cryptography that the attacker knows they can break."[157] The aforementioned GSM case is an example of this approach, and a case to further explore for its striking similarities with the NSA Bullrun and GCHQ Edgehill operations, disclosed by Edward Snowden.

The historical analysis generates research questions about the relationship between national security capture and regulatory competence at the E.U. level. On the one hand, history instructs that whenever robust policies are about to be adopted at the E.U. level, national governments joined in the E.U. Council capture those policies referring to national security, or to surveillance more generally. National security falls under the exclusive competence of national governments – or 'sole responsibility' as the E.U. Treaties have it (see introduction to section 1.1. and section 1.1.1.). This could be seen as a fundamental weakness in the E.U. institutional structure to meaningfully regulate network and information security. On the other hand, the nature of network and information security is changing rapidly, and policymaking increasingly concerns issues far beyond national security. Rationales for regulatory intervention that come to mind are enhancing the digital economy, harmonizing the internal market, consumer protection and fundamental rights. These are all issues that fall well within E.U. competence. Considering the increasing weight of other interests involved, not having competence in national security may prove to be an opportunity to actually strengthen security when policymaking concentrates on meaningfully augmenting communications security and harmonize the E.U. internal market to that end. In comparison, on the U.S. federal regulatory level, national security is an inherent part of all steps in the legislative process, exacerbated by a near exclusive regulatory authority within the Executive branch based on art. II of the U.S. Constitution.[158]

[156] See Arnbak & Van Eijk 2012; Asghari, Van Eeten, Arnbak & Van Eijk 2013.
[157] P. Hallam-Baker, 'PRISM-Proof Security Considerations', Internet Engineering Task Force (IETF) Internet–Draft, 11 September 2013, s. 3.4, p.6-7, see: http://tools.ietf.org/html/draft-hallambaker-prismproof-req-00
[158] See Arnbak & Goldberg, 2014.

History certainly suggest national security strategies will remain a potent factor in this debate, for instance as witnessed in the GSM case. And that a national security agenda weakens incentives for meaningfully strengthening network and information on the E.U. level. Many countries may strategize towards more robust 'national cybersecurity' at home, while seeking to foster its ability to engage in intelligence gathering and cyber-attacks in another E.U. country. E.U. level action may impair that ability. Another perspective comes from game theory, highly influential in nation state strategic planning, especially with regard to timing offensive cyber-attacks. Game theory seems suggests several counter-intuitive incentives with regard network and information security: securing communications, the theory holds, leads to an escalation of nation state cyber-attacks.[159]

Recent months have seen considerable legislative action on all five E.U. policy cycles. Since the 1990s, dependence on network and information security in its technical conception has significantly increased on a social, economic and political level. And the post 9/11 obsession with national security appears to be fading to some extent in Europe, at least in the public debate, with the Snowden revelations adding a different policy dynamic to the fold. In other words, the political landscape has changed and the stakes to secure communications for all end-users, rather than keeping communications vulnerable for all attackers, are higher and felt by more voters than before. The coming years will prove insightful in understanding the competence, political leeway and the ambition of the E.U. vis-à-vis national security.

1.2.6. *The 'Cyber' Threat: Deterrence vis-à-vis Protection*

As observed in section 1.1.5., deterrence is a central element in the definition and conceptualizations in cybercrime – and in cyber warfare for that matter. For over two decades deterrence has been the doctrine to drive much of the policy action in the cybercrime policy cycle. Deterrence was the central rationale behind the influential CoE Cybercrime Convention of 2001. Cybercrime policy as a network and information security measure can thus be understood as a preventative measure by leveraging a threat of punishment through criminal law – or the law of armed conflict[160] – after the occurrence of an attack.

Deterrence policymaking concentrates on sending credible signals to adversaries to refrain from an attack, because your possible retaliation will cause considerable or devastating harm. But conventional deterrence models are only marginally effective in the field of network and information security. It is often impossible to attribute a specific attack to a certain actor ('the attribution problem'). Moreover, punishing crimes locally is impractical in a global environment. Several crucial nations – including Russia and China – will not join the Cybercrime Convention or any other global cybercrime policy regime anytime soon. And perhaps most obvious and important, systems actually don't get more secure by talking tough on punishment and retaliation.[161]

The Cybercrime Convention recognized already in 2001 that deterrence is a limited doctrine for cybersecurity. The Convention stated in its explanatory memorandum that actual network and information security measures are "the most effective means" to prevent security breaches, rather than criminal law.[162] Back then, a broad consensus could be reached with over 50 countries around the Cybercrime Convention and within the E.U. around the approximation of criminal law, but that broad

[159] R. Axelrod & R. Illiev, *Timing of cyber conflict*, PNAS, vol. 111, no. 4, Jan. 28, 2014. Weak defences decrease the probability that capabilities for exploiting zero-day vulnerabilities will be deployed, the paper concludes. Increasing overall cybersecurity will lead nation state attackers to rationally strategize towards immediately exploiting zero-days rather than holding on to them in the possible event that 'business as usual' escalates into to actual military action.

[160] Citing from a 2010 NATO report of a Group of Experts, chaired by M. Albright, former U.S. Secretary of State: "cyber attacks [..] could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5." NATO Public Diplomacy Division, *NATO 2020: assured security; dynamic engagement*, 0753-10, p. 45 & p. 17.

[161] D. Mulligan & F. Schneider, 'Doctrine for Cybersecurity', Dædalus, the Journal of the American Academy of Arts & Sciences 140 (4) 2011. D. Clark & S. Landau, Untangling Attribution, in: Proceedings of a Workshop on Deterring CyberAttacks, National Research Council: Washington 2010. N. Sales, Regulating Cybersecurity, Northwestern University Law Review, Vol. 107, No. 4, 2013.

[162] Council of Europe Convention on Cybercrime, CETS 185, Budapest 31 Nov. 2001, para. 45. See: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm

users protections offered through network and information security legislation still has to materialize. Meanwhile, the proposed Network and Information Security Directive is struggling for meaningful survival. Today, the deterrence doctrine dominates policy agendas, even though on itself it fall short of providing actual user protection.

The current political dynamic begs the question if the protection of network and information security is the ultimate goal of such policies. Instead, we might be witnessing the dynamics of 'securitization', a practice of political speech to frame certain threats as imminent to a significant collective or set of values (such as the nation state) by powerful stakeholders, in order to prioritize certain policy and funding agendas.[163] For the U.S. political arena, Hansen & Nissenbaum suggest that the introduction of the terms 'cyber security' and 'critical infrastructures' in the 1990s has enabled a now successful securitization of the networked environment.[164]

Indeed, the concept of 'cybersecurity' today seems to have provided leeway to further politicize, and securitize, the legal governance of communications security: as security incidents have reached the mainstream news, policymakers have started to frame security vulnerabilities as existential threats for social, political and economic life. Cybersecurity has been connected to acts of terrorism, child abuse, human trafficking and even downloading music and movies.[165]

What is really at stake in E.U. 'security' conceptualizations and politics? In recent years, the U.S. political terminology, and a similar aggressive language, can be witnessed on the E.U. level. Then again, the lack of national security competence may limit the window of opportunity for successful securitizations of cyberspace at the 'federal' level of E.U. policy. Apart from technical and legal research, the political science of 'security' conceptualizations and policymaking at the E.U. level is a necessary subject of further research in the coming years.

1.3. ***Conclusion and Research Agenda***

The historical analysis of four decades of policymaking has rendered new insights into E.U. security conceptualizations and policymaking. Five policy cycles have been distinguished in this paper: data protection, the telecoms package, encryption, cybercrime and network and information security. The historical analysis of these cycles has been synthesized in section 1.2., resulting in themes that deepen insight into how the European regulatory framework should protect network and information security of end users.

The historical analysis informs us how 'security' definitions are incomplete and left unexplained by the legislator. There is no coherent understanding at the E.U. level how to define 'security', and how its underlying values operate, relate or should be interpreted. Whenever a substantial security breach has occurred, legal protection as well as enforcement structures in data protection and telecommunications – policy cycles that in themselves leave considerable areas of network and information confidentiality, integrity and availability untouched – have been re-wired or stretched to address political or economic concerns. Often, in ways that are understandable from a realistic view of the opportunism embedded in policy- and lawmaking, but with conceptually questionable, as well as sub-optimal or outright damaging outcomes.

[163] See section 3.2. for a discussion of securitization theory.
[164] L. Hansen, H. Nissenbaum, *Digital Disaster, Cyber Security and the Copenhagen School*, International Studies Quarterly, 2009:53, p. 1157.
[165] For example, see the European Commission press release announcing the EU Cybersecurity strategy: http://europa.eu/rapid/press-release_IP-13-94_en.htm. The estimates of loss incurred due to cybercrime are highly unreliable, and usually include figures provided by the entertainment industry. See also Anderson et. al., 'Measuring the Costs of Cybercrime', WEIS 2012, p.14, see: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf. See more generally: I. Brown & P. Sommer, Reducing Systemic Cybersecurity Risks, OECD/IFP: London 2011, http://www.oecd.org/dataoecd/57/44/46889922.pdf, M. Mueller, Networks and States, MIT Press: Cambridge 2010., D. Bambauer, Conundrum, Minn. L. Rev., vol. 96, 2012, p. 7, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1807076.

Between the policy cycles there exist substantial gaps in the application of the c.i.a.-triad in itself, and how its elements should be understood in the various 'security' policies adopted in legislation. The obvious connection of the c.i.a.-triad with constitutional values – and a long tradition of ECtHR case law – has only been made in the earliest CoE Cybercrime policies, but never since been further elaborated on at the E.U. level. Furthermore, the institutional ecosystem in the field of network and information security – embodied by ENISA – has quite deliberately not been graced with a competence to work out a coherent vision on network and information security policy. Meanwhile, the five policy cycles have not been 'scoped' with network and information security in mind, but rather confronted with a myriad of interests, ranging from market structuring in telecommunications, via data protection, to cybercrime and especially national security as powerful policy aims that have overshadowed communications security. The E.U. regulatory framework contains, in sum, a large amount of legislative arrangements on network and information security, but both a coherent vision on part of the legislator as well as a clear view of what laws exist and how to apply them is lacking. Legal uncertainty permeates E.U. network and information security law.

A legislative habit seems to exist in which 'security' conceptualizations are copied from previous documents, with little argumentation and elaboration on what impact a particular conception of 'security' has on the actual policies furthered in these instruments. Regardless of constitutional values at stake and a robust computer science literature, the critical details are often delegated to the European Commission or standardization processes, rather than negotiated between Council and Parliament. Perhaps conceptual copy-pasting is not that surprising, as loss of institutional memory on a technical and complex policy issue seems an inherent drawback for 'good' communications security regulation at the E.U. level. Nonetheless, the lack of clarity and coherence when it comes to E.U. security conceptualizations has allowed powerful stakeholder to paint network and information security in any colour they like.

The 'network and information security' policy cycle is a case in point (section 1.1.1. and 1.1.6.). Starting already in 1990, in 2014 E.U. level network and information security and critical infrastructure policy by and large remains voluntary, and under the control of the Member States in the E.U. Council. A complex policy surface has emerged: many Member States see network and information security as synonymous to national security policies. From the outset, an implicit aim has been to obstruct E.U. institutions from active involvement and coordination, as 'national security' is explicitly excluded from E.U. competence under its Treaties. A patchwork of mostly voluntary action plans and public-private partnerships has emerged, while critical stakeholders such as software vendors are exempted from regulatory instruments. In practice, nobody has a clear overview of what policies are in place, who is effected, and stakeholders hardly follow-up on ENISA policy advice.

The issue statement of the 1992 Council Decision is worth citing again, both because its aims have clearly not been reached and because it reads like any policy document today:

> *"1.1. Issue - security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world."*

A policy priority for network and information security comes in bursts. Two time-frames of note are the 1990s – amidst data protection and encryption policy reform (the so-called crypto-wars) – as well as 2013 and beyond. Many of the security measures most security experts call for today (end-to-end encryption obligations, private key storage prohibitions obscuring key escrow for CAs), were also proposed back then by the European Commission, only to be removed from E.U. legislation by the E.U. Council's national governments. In the middle of these two time-frames sits a decade of national security and cybercrime securitization practices, intensified by post-9/11, Madrid and London terrorist attack politics.

The year 2013 has seen considerable legislative action in all five policy cycles, which points at the momentum and concerns over network and information security at the E.U. level. Particularly, the 'Network and Information Security' Directive presents an opportunity to work out how to conceptualize 'security' in E.U. law and policy. Most, if not all of these initiatives will be discussed well into 2015. It is still unclear what coalitions will be formed on this subject after the European Union elections of May 2014. On the one hand, the recent attention for network and information security will undoubtedly be exacerbated by the Snowden revelations. On the other hand, the recently proposed Network and Information Security Directive appears to already have been captured by powerful security interests both on the state and corporate side: software vendors are left outside its scope, specific security measures have been weakened by both Parliament and Council and politicians across parties have voiced a desire to delay the legislation for the foreseeable future, hardly responding to widespread concern and media reporting on insecure communications.

However, the social dynamics of networked communications, the political situation in the E.U. and the continuing Snowden revelations create an urgent societal relevance for further research. The current status quo of conceptual ambiguity is untenable. The importance of, and dependence on, networked communications in economic, social and political life is increasing. At the same time, the weaknesses of these communications are exposed on a daily basis by media reports on poor security practices at service providers or pervasive surveillance practices by nation states all across the world. With regard to the latter, we are only starting to develop a more thorough understanding of the national security dimension in surveillance practices as well as network and information security policymaking, enabled through the leaks of Mr. Snowden. Surely, more leaks exposing insecure communications will follow in the coming years.

Section 1.2. has developed six research themes which will form the basis of the further research in Part I of this thesis:

1) The guiding force of the c.i.a.-triad;
2) The constitutional dimension of the c.i.a.-triad;
3) Data protection path dependency;
4) Scope: re-orient actor-based policies towards a focus on functionality;
5) National security capture of E.U. policymaking;
6) Cybercrime and cybersecurity: deterrence vis-à-vis protection.

These themes are further explored in the following chapters. Technical perspectives are offered in chapter 3, political science perspectives in chapter 4 and constitutional and legal perspectives in chapter 5. Chapter 6 develops a conceptualization of 'security' that will form the basis of the case studies in Part II of the thesis on HTTPS governance and the disclosures around the NSA/GCHQ BULLRUN and EDGEHILL operations. Part III will develop a normative theory and specific regulatory recommendations on if, and if so how the European regulatory framework should protect network and information security for end users.