UvA-DARE (Digital Academic Repository)

Conceptualizing Communications Security: A value chain approach

Arnbak, A.

DOI

[10.2139/ssrn.2242542](https://doi.org/10.2139/ssrn.2242542)

Publication date

2013

Document Version

Submitted manuscript

Published in

TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy: September 27-29, 2013: George Mason University School of Law, Arlington, VA

[Link to publication](#)

Citation for published version (APA):

Arnbak, A. (2013). Conceptualizing Communications Security: A value chain approach. In *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy: September 27-29, 2013: George Mason University School of Law, Arlington, VA* Social Science Research Network (SSRN). <https://doi.org/10.2139/ssrn.2242542>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)

CONCEPTUALIZING COMMUNICATIONS SECURITY: A VALUE CHAIN APPROACH

Axel ARNBAK¹

Institute for Information Law, University of Amsterdam.

Abstract. Cybersecurity has become a top priority for policymakers these days, but as the engineering saying goes: “if you don’t know what you want, it’s hard to do it right.” This paper finds considerable shortcomings in current conceptual and legal frameworks for communications security policymaking. The misleading concept of cybersecurity incorporates a wide range of social issues under its umbrella, such as child protection, foreign policy and intellectual property protection. Cybersecurity distracts communications security conceptualizations and policies from the technical conception that should be at their core, i.e. ensuring confidentiality, integrity and availability of communications to authorized entities. The paper develops a value chain approach for the conceptualization and legal governance of communications security. This value chain approach is informed by an empirical case study into HTTPS governance and multilateral security engineering methods SQUARE and MSRA. It offers a 9-step framework for granular, functional communications security conceptualizations, tailored to specific communications settings. The framework enables policymakers to devise technical security goals, apprise constitutional values, confront stakeholders interests and balance associated public and private interests. The value chain approach should assist policymakers in deciding what they want, and to know whether they are the appropriate actor to get it right.

Keywords. Communications security, cybersecurity, HTTPS, governance, constitutional values, value chain approach.

“We must do something. This is something. Therefore we must do it.”²

- ‘The Politician’s Logic’, Sir Humphrey Appleby (1988)

WORK IN PROGRESS – CONTACT AUTHOR FOR LATEST VERSION

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 the Telecommunications Policy Research Conference 2013 organization for the opportunity to present this is earliest-stage research. This is a very first draft on the subject, and I expect to add an updated version on 6 September 2013, well before TPRC, and to continue updating the paper in the coming months based on the participants input. The paper should be much more precise on terminology, especially given the subject. Any comments, literature suggestions and critique are equally gratefully received at a.m.arnbak@uva.nl.

² Syllogism identified by fictional character Sir Humphrey Appleby in TV-Series ‘Yes, Prime Minister’ in the episode ‘Power to the People’, 1988. See: <http://youtu.be/vidzkYnaf6Y>

Table of Contents

Introduction.....	2
1. Communications Security Definitions.....	5
1.1. ‘Security’? A Technical Conception.....	5
1.2. ‘Communications’ Security? A Value Chain Approach.....	8
2. Security Requirements Engineering	12
2.1. From General Goals to Specific Requirements	13
2.2. Multilateral Security: Addressing Conflicting Stakeholder Interests	14
3. Conceptualizing Communications Security.....	15
3.1. Step by Step Engineering Methods: SQUARE and MSRA.....	16
3.2. Governance: Communications Security Value Chains	18
4. Concluding Remarks	21
Appendix: Overview Security Requirements Engineering Framework	22

Introduction

Secure communications trace back to the Roman Era, when letters reporting the latest from the battlefield were encrypted with the Caesar Cipher to protect their confidentiality and integrity. Ever since, communications security has been an ambition and security requirements have been mediated through adopting the appropriate mix of technical, organizational and legal measures. These measures have always reflected the socio-technical context, stakeholder interests and the underlying values of the time and the specific communications setting. In today’s ‘infosphere’,³ in which information communications technologies (‘ICTs’) increasingly mediate our informational, personal, economical en political interactions, realizing secure communications is important for a wide range of stakeholders. The increasing attention across the globe for realizing communications security, and its legal governance, gives rise to a basic question: what is communications security?

Definitions determine the scope and may reflect the objectives of any governance effort. Conceptual clarity is a “precondition ... to interpersonally

³ L. Floridi, *The Philosophy of Information*, Oxford University Press, 2011.

and unambiguously communicate ideas, analysis and policy options”,⁴ while shortcomings in definitions are an important source for regulatory failure.⁵ The question, and continuous iteration, on the legal definition of communications security is however hardly addressed; rather it is a critical question policymakers shy away from.

Apart from the shortcomings in current legal definitions for ‘communications’ in a rapidly changing socio-technical environment (see section 1.2), the plurality of the concept of ‘security’ is another source for conceptual ambiguity. Nissenbaum noted in 2005 that two distinct conceptions of security emerged in policy discussions on securing communications. ‘Technical (computer) security’ is rooted in computer science and engineering and protects the security attributes confidentiality, integrity and availability. ‘Cyber-security’, on the other hand, is mostly employed by governmental and corporate actors⁶ and seems to incorporate all social issues that are in any way TCP/IP mediated. Indeed, cybersecurity has provided leeway to further politicize, and securitize, the legal governance of communications security: vulnerabilities are framed as existential threats for social, political and economic life. The technical security conception is mixed up with public safety and social and national security issues, such as child protection, human trafficking, foreign policy and downloading of music and movies.⁷ It reminds one of Sir Humphrey Appleby’s Politician’s Logic: “something must be done. This is something. Therefore, we must do it.”

The current legal governance of communications security, meanwhile, receives its fair share of criticism for its problematic relationship with constitutional values and contradicting the realization of security in its technical conception. Legislative proposals to introduce internet kill-switches in the U.S., hacking powers for law enforcement agencies in the Netherlands and to regulate web browsing security in the EU reinforce or expose communications to well-known security vulnerabilities, rather than resolving

⁴ A. Schmidt, *Conceptualizing Internet Security Governance*, GIGANET 2009, p.2, see: <http://netdefences.com/wp-content/uploads/Schmidt-2009-Conceptualizing-Internet-Security-Governance.pdf>

⁵ Baldwin et al., ‘Understanding Regulation’, Oxford University Press, 2013, p.68.

⁶ H. Nissenbaum, “Where *Computer Security* Meets *National Security*,” *Ethics and Information Technology*, Vol. 7, No. 2, June 2005, p. 63.

⁷ 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. 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.

them.⁸ Paradoxically, some of the same security vulnerabilities that are cause for existential concern are at the same time secretly exploited, apparently to further state interests. In this way, cybersecurity has served as a Trojan horse that it purportedly should protect against. Furthermore, the credibility of the aforementioned existential claims has been put under serious pressure by the recent revelations about transnational surveillance, on both sides of the Atlantic. Wide and unchecked surveillance of networked communications is conducted for a wide range of objectives – national security, foreign policy, economic espionage and indeed offensive cybersecurity – under codenames such as PRISM, xKeyscore and Tempora. The programs run by Western intelligence agencies, that until a few months ago had been obscured by the cloud,⁹ arguably constitute the most serious breaches of communications security in recent history.

This paper argues that countering the current conceptual ambiguity is a necessary precondition for sensible communications security policymaking. The paper aims to contribute to reorienting communications security conceptualizations towards the technical conception of security. The central research question of the paper is, how to conceptualize ‘communications security’ for its legal governance. More specifically; how should the security attributes of communications confidentiality, integrity and availability be integrated into its legal governance?

The research is primarily of a descriptive nature, and employs desk research as principal method. Primary legal sources, soft law and literature are reviewed from both the U.S. and European legal frameworks, along with internationally recognized technological standards and computer science, legal, information theory and public policy literature. The theoretical analysis in this paper builds upon and expands the empirical analysis conducted in a case study on HTTPS governance presented at TPRC 2012 (‘Certificate Authority Collapse’). The paper is early-phase research and a first draft in a longer series of papers on the same subject. In this first draft, the analysis focuses on the European legal framework. In the future, the paper should be complemented with an assessment of communications security conceptualizations in other legal systems – notably the U.S. The paper should eventually become the analytical cornerstone of a four-year research project on communications security governance.

⁸ D. Opderbeck, *Cybersecurity and Executive Power*, 89 *Washington Law Review* 795, January 2012. Arnbak, Axel and Van Eijk, Nico, *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain* (August 15, 2012). 2012 TRPC. Available at SSRN: <http://ssrn.com/abstract=2031409>. 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). Available at SSRN: <http://ssrn.com/abstract=2276103>.

⁹ Van Hoboken, Arnbak & Van Eijk 2013. Rauhofer, Judith and Bowden, Caspar, *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* (June 21, 2013). Edinburgh School of Law Research Paper No. 2013/28. Available at SSRN: <http://ssrn.com/abstract=2283175> or <http://dx.doi.org/10.2139/ssrn.2283175>

The first section of the paper analyses existing ‘security’ and ‘communications’ conceptualizations. In the second section, multilateral security requirements engineering is explored as a source of inspiration for communications security conceptualizations, and the value chain approach is introduced. Section 3 is a modest first attempt on developing the value chain approach for communications security conceptualizations.

1. Communications Security Definitions

This section presents an overview of the technical conception of ‘security’ (section 1.1.) and analyses the limits to the legal definitions of ‘communications’ (section 1.2). It proposes a granular and functional value chain approach to communications security conceptualizations.

1.1. ‘Security’? A Technical Conception

In technical communities, a consensus appears to have been reached over the last decades on the classification of the main attributes of ‘security’ definitions: *confidentiality*, *integrity* and *availability*.¹⁰ While slight differences in the exact definition of these three main attributes appears across the literature, they can generally be defined as follows:¹¹

- *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;
- *Availability* – assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems.

¹⁰ K. de Leeuw & J. Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook*, Elsevier: Amsterdam 2007, p. 2/3.

¹¹ Cited from Pfleeger 2003, p. 504. See also Pfitzman 2006, Haley et al 2006, Nissenbaum 2005, Pieters 2011. K. de Leeuw & J. Bergstra 2007, p.2. The CIA-triad can also be found across influential technical standards documents: Refs. <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html> ISO/IEC 27000:2012, para. 2.30. Assurance is defined by the U.S. National Institute of Standards and Technology as “grounds for confidence that other security goals have been adequately met” by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. See: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

Some authors have extended this well-known ‘CIA-triad’ with concepts such as anonymity (non-identifiable data subject), accountability (availability and integrity of a person who performed an operation), non-repudiation (assurance of the accurate sender) and authentication (accurate identification by a computer system).¹² At the same time, these attributes can be subsumed under the CIA-triad. Fabian et al. observe: “accountability and non-repudiation can be classified as integrity goals, authentication as a design mechanism to achieve confidentiality or integrity, and anonymity or un-observability may be subsumed under confidentiality goals.”¹³ The threats to the attributes of this technical conception of ‘security’ have been evolving over the years, but the surveyed literature shows that the CIA-triad remains robust.

The security attributes interact with each other in complex ways and may complement or conflict with each other, depending on the communications setting. As an example to illustrate this point, let us look at certificate-mediated web browsing security (HTTPS, the padlock in the browser). In particular, the incident response dynamics in the aftermath of the widely reported breaches at certificate authority (‘CA’) Diginotar and CA Comodo are informative. Trust revocation of a CA by web browser vendors renders the websites running certificates signed by these CAs inaccessible (breach of ‘availability’), while refraining from trust revocation of the breached CAs could maintain an insecure status quo. This substantially increases the vulnerability of end-users to eavesdropping (breach of ‘confidentiality’) or alteration of transmitted information (breach of ‘integrity’) through a man in the middle attack.¹⁴ Trust revocation of relatively small CA such as Diginotar renders some websites unavailable. Therefore, this is an easier decision for browser vendors than revoking trust in large CAs, even though the breach at such a large CA (in the case of Comodo, a market leading CA) implicates the confidentiality interests of end-users by several orders of magnitude. Large CAs thus benefit from the systemic security vulnerabilities in the SSL/TLS encryption protocol, because they face a small risk of actually being punished by browser vendors. Browsers are left with the difficult choice – often based on limited information provided by the CA and some external pressure of tech communities – whether to prioritize availability or confidentiality interests of end-users that seek secure communications with the websites of their bank, social network or webmail provider.¹⁵ Returning to the conceptualization of ‘security’, the example shows that not only the security attributes interact, but other specific circumstances matter as well. Stakeholder interests (browser vendors vis-à-vis websites and CAs) and market structure (large market share vis-à-vis small market share) are

¹² Pfitzmann 2006. Pfleeger 2003.

¹³ Fabian et al, ‘A Comparison of Security Requirements Engineering Methods’, *Requirements Eng* (2010), 15:7-40, p.12.

¹⁴ Arnbak & Van Eijk 2012.

¹⁵ Asghari, Hadi, Van Eeten, Michel, Arnbak, Axel and Van Eijk, Nico, *Security Economics in the HTTPS Value Chain* (June 12, 2013), WEIS 2013, Available at SSRN: <http://ssrn.com/abstract=2277806>.

just two of the many factors that may impact how security is produced in a specific communications setting.

The concept of ‘authorization’ is strikingly central in the technical conceptions of ‘security’. Confidentiality is breached as soon as an *unauthorized* entity can access a secured asset, integrity when an *unauthorised* entity can modify it, and availability when the *authorized* entity is barred from it. The centrality of authorization becomes even more clear from the unified definition of ‘security’ in Avizienis et al: ‘security is the absence of unauthorized access to, or handling of, a system state’.¹⁶

From the perspective of policy and regulation, the immediate question that arises is how authorization is operationalized. Who is this ‘authorised entity’, how did she get authorized, by whom, Who enforces and supervises these crucial decisions? The operationalization of authorization is vital in determining the value of the security attributes, and how they should be balanced in specific communications settings.

‘Authorization’ needs to be conferred and subsequently verified through a reliable structure.¹⁷ This structure can take many different shapes, such as the design of access control mechanisms, contracts, consent and the legislative process. In the interaction between authorization and the three main security attributes, regulation plays an essential role. Both in conferring and in verifying authorization, applicable laws and standards may be an important source for determining authorization.¹⁸ The European Data Protection Directive has an extensive section on the security of personal data, and so do sector-specific laws in the United States such as HIPAA on health data. Both instruments set security requirements and determine ‘authorization’ in specific communications security (see section 3.2.).

In addition, the security attributes confidentiality, integrity and availability connect to constitutional values such as communications secrecy, privacy and freedom of expression. In art. 17 of the UN International Covenant on Civil and Political Rights (CCPR) and art. 8 of the European Convention on Human Rights (ECHR), the concept of ‘correspondence’ does include the integrity and confidentiality of electronic communications.¹⁹ A 2008 ruling of the European Court of Human Rights (ECtHR) concerning sensitive health data²⁰ establishes that ensuring technical security through the law is not merely an ethical or political obligation, but a constitutional obligation for all Member States of the Council of Europe: ²¹ states should both refrain from violating the security attributes without an extensive justification (a negative obligation not to

¹⁶ Avizienis 2004, p. 23.

¹⁷ Pfleeger 2003, p. 505.

¹⁸ FIPS 200; SP 800-53; SP 800-53A; SP 800-37; CNSSI-4009.

¹⁹ 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

²⁰ I. v. Finland, App. No. 25011/03, 17 Jul. 2008.

²¹ De Hert 2010, p. 49.

interfere). States should also ensure and enforce the technical conception of security through ex ante legislation (a positive obligation to ensure). Merely having legislation in place that provides ex post compensation after a breach of security is insufficient.²² Laws have to provide meaningful technical security in vertical (citizen – public entity) and horizontal (citizen – private entity) relationships such as ‘to police strictly access of and disclosure of health records’.²³ If such specific access controls and logging functions are not in place, the systems owner is liable for possible damages.²⁴

A July 2013 ruling of the ECtHR in the context of cloud communications expands the scope of the constitutional protection of the Convention to “all data on a server”, regardless of whether that data in effect identifies a (legal) person or not.²⁵ As such, the positive obligation to ensure technical security may extend beyond personal data to, for example, confidential corporate information. It is important to note that these recent rulings are case specific. Constitutional criteria for an adequate level of technical security depend on the values, interests, stakeholders and circumstances under consideration.

In computer science literature, this definition of ‘security’ is given regardless of its prefix (network, information, communications, systems). As we will see in the next section, the prefix of communications impacts, and constrains, the legal conceptualization substantially.

1.2. ‘Communications’ Security? A Value Chain Approach

Communication²⁶ is classically defined in the legal literature as the exchange of information,²⁷ the transmission of information from a sender to a receiver through a communications channel.²⁸ These conventional legal definitions point to the communications channel, or ‘transporteur’, in private communications as the object of ‘communications security’. The data transmitted and the end-points of the communication are not the object of communications security in these classical legal definitions. If Alice calls Bob using a fixed landline, communications security concerns itself with the connection from Alice’s horn to Bob’s, in other words with securing the wire and switching arrangements of telecommunications providers.

In the European regulatory framework, ‘electronic communications’ refers to the situation in which the transmission or exchange of data between sender and receiver is conducted by an electronic communications provider – an entity primarily in the business of signals transmission – such as conventional

²² ECtHR I. v. Finland., para. 47.

²³ ECtHR I. v. Finland., para. 40.

²⁴ ECtHR I. v. Finland., para. 44.

²⁵ para. 106 BERNH LARSEN HOLDING AS AND OTHERS v. NORWAY 14/03/2013

²⁶ Here, we are concerned with private communications, rather than public communications.

²⁷ Steenbruggen 2009, p. 53.

²⁸ Dommering 2000, p. 465, referring to Van Cuilenborg & Noomen 1988.

telecommunications and internet access providers.²⁹ Information society services,³⁰ such as providers of social network services and webmail, fall outside the legal definition of ‘communication’³¹ and thus outside the scope of the vast majority of current communications security obligations in the European legal framework.

The conventional communications environment has seen rapid change with digitization, convergence and the explosion of networked electronic communications (mostly through the ‘internet’). Moreover, there is the emergence of information society services that practically perform similar communications functions as the conventional ‘electronic communications providers’. Not to mention the evolving threat landscape of communications security. These developments put pressure on the straightforward spatial and conceptual boundaries of the ‘communications security’ concept. For example, if Alice were to contact Bob again, this time via e-mail, the list of intermediaries involved in securing their private communications could include their e-mail providers, Alice or Bob’s internet access providers, a range of routing intermediaries between, the insecure open Wi-Fi network Alice has joined in her favorite coffee place, their operating systems manufacturers, their devices (smartphone, computer, tablet, etc.), perhaps their web browser vendors – the list may go on. The message, moreover, would be divided in many packets, distributed through as many different routes over the network, only to be assembled again at the end-point of the message. At all these intermittent points between Alice and Bob, communications security can be implicated.

In the European legal framework, the concept of ‘communications security’ is tied to technologies of the 90’s. A case in point of how the current legal conceptualization of ‘communications’ is constraining meaningful communications security policies is the introduction of a personal data breach notification for electronic communications providers in 2007.³² Even then, it was clear that limiting a data breach notification obligations to the classical telecommunications providers was too narrow. These stakeholders transport the data and should not to its contents, let alone store and process them. The more relevant intermediaries in this communications setting are the companies that actually store, process and monetize the personal data the obligation seeks to protect.

A majority in the European Parliament tried to extend the data breach notification to these intermediaries in 2008,³³ but found itself constrained by

²⁹ See art. 2[c] Framework Directive 2009/140/EC.

³⁰ See art. 1[2] 1998/48/EC Richtlijn informatieprocedure II: ‘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.’

³¹ European Commission, Amended proposal, COM(2008)723 final, p. 20.

³² For a detailed account, see F. Borgesuis, *De meldplicht voor datalekken in de Telecommunicatiewet, Computerrecht*, 2011-4, p. 209-218.

³³ European Parliament, amendement 136, 24 September 2008.

the (European Commissions' interpretation of) the legal definitions of the E-Privacy Directive. Four years after the E-Privacy Directive was adopted, on 24 June 2013, the European Commission introduced a Regulation on the notification of data breaches that only covers electronic communications providers – hardly anyone noticed.³⁴ Even though a personal data breach was first proposed by the European Commission in 2007,³⁵ a general data breach notification requirement for information society services still remains to be signed into law. A case of regulatory failure due to shortcomings in a legal definition.³⁶

Instead of relying on conventional legal conceptualizations, a functional conceptualization would focus on what constitutes communication in specific settings. Instead of concentrating on communications providers in a legal sense, the intermediaries that partake in Alice and Bob's communications chain should be included as relevant stakeholders. From a functional perspective, this can be a number too large to handle. Indeed, dynamics in communications transmission have given rise to the adoption of SSL/TLS encryption to provide end-to-end security in web-mediated communications, preventing all those intermediaries between Alice and Bob communications providers to listen in to their communications.³⁷

As an analytical concept, 'communications' and 'communications security' remain relevant, but the relevance of the current legal conceptualization of 'communications' is diminishing. This technology dependent approach to communications policy conceptualizations is legacy to the European legal framework and the consequence of a long history of state involvement in telecommunications provision before the market liberalization of the 90's. The Open Network Provisions of the 90's were always meant to be an ex ante sector-specific market structuring instrument, not an avenue to cure all the problems of networked communications. It remains to be seen whether the current review of the electronic communications framework takes this point into account.

A refreshing perspective comes from art. 8 of the ECHR, and art. 17 CCPR likewise. These Charters contain a fundamental right to 'respect for correspondence', rather than a technology dependent conceptualization, and include communications security and its attributes, no matter how rapidly its underlying technologies or intermediaries change. The ECHR from 1948 adopts a functional approach, where recent laws and regulations on the EU level don't. The case law discussed in the previous section illustrate this

³⁴ See art. 1 Commission Regulation 611/2013.

³⁵ European Commission, Impact Assessment, 13 nov. 2007, SEC(2007)1472, p. 102-103.

³⁶ Baldwin et al. 2012, p.68. See introduction.

³⁷ The SSL/TLS protocol and its implementation have many security problems of its own, notably the area of integrity given the systematically weak certificate-based authentication model on which all security goals depend. See Arnbak & Van Eijk 2012; Asghari, Van Eeten, Arnbak & Van Eijk, 2013.

perfectly well. From the outset, the dependence of end-users' communications on the intermediary has always constituted the principal rationale for the respect for correspondence. Steenbruggen has observed this as the root cause for the flexibility of the ECHR and its ability to provide protection regardless of the technological reality of tomorrow.³⁸

The EU 'Network and Information Security Directive' (NIS Directive) that also refers to cybersecurity across its provisions, proposed in February 2013 to target 'information society services' rather than 'electronic communications providers' alone. The European Commission seems to have understood that the current legal conceptualization of 'communications' is too narrow given today's networked communications environment. In an explanatory document, the Commission states that it would be 'absurd' not to include these 'information society providers' within the scope of this instrument.³⁹ The accompanying document of the NIS Directive points at cloud providers, social networks and e-commerce providers to fall under the scope of the instrument, but surprisingly would not cover stakeholders just as relevant in the communications security sphere, such as providers of smartphone apps.⁴⁰ A functional approach would inform that it does not matter much whether Alice contacts Bob through Facebook or the highly popular communications service What's App. Moreover, the legal definition of 'information society services' doesn't include web browsers, content management systems such as Wordpress, nor does the definition cover hardware and software developers – even though these stakeholders have received their fair share of criticism lately over communications backdoors – that could all be part of the chain of intermediaries enabling private communications. The European Commission might have its reasons, but refrains from explaining why this focus on 'information society services' isn't 'absurd' going forward. A similar analysis can be made of the recently proposed EU Regulation on Trust Services, that for legacy reasons includes one stakeholder in the communications process, the Certificate Authority, but not the other critical stakeholders such as websites and browser vendors.⁴¹ Under the functionally robust 'respect for correspondence' of art. 8 ECHR these would all be considered relevant intermediaries, but not in the European Commission's legislation. One wonders whether the Commission has really learnt its lesson.

These increasingly rapid socio-technical developments in networked communications render the realization of secure communications through legislation increasingly complex. However, it is not a trivial task that legislatures can shy away from: it may be a positive constitutional obligation to ensure communications security through legislation (section 1.1. and section 3). Legislatures must take note that sensible communications security policies

³⁸ Steenbruggen 2009, p. 54.

³⁹ http://europa.eu/rapid/press-release_MEMO-13-71_en.htm

⁴⁰ Impact Assessment - SWD(2013)32 final - 7/2/2013

⁴¹ Arnbak & Van Eijk 2012.

depend a highly dynamic set of stakeholders and that for any given specific communications setting, a different and rapidly changing set of stakeholders can, should or cannot assume responsibility. Moreover, forms of ad hoc networked governance with a variety of private stakeholders without much involvement from public authorities have been considerably successful in augmenting communications security in recent years – in the cases of routing security and the Conficker botnet mitigation.⁴² Legislatures need to adapt to the reality that not only ‘communications’, but also the modalities of communications security governance are rapid in flux, and their regulatory cycles are hardly keeping up.

Those responsible should be aware of these socio-technical realities, and adopt granular and functional approaches towards communications security conceptualizations and policies. In earlier work, we have suggested a “value chain approach” as one possible method for the legal governance of communications security.⁴³ A value chain approach suggests that governance conceptualizes ‘communications security’ *values*, and then identifies stakeholders, their interests and interactions (*chain*). That framework lets the regulator determine if interventions are needed to align the incentives for delivering communications security outcomes in the specific communications setting under consideration.

In section 3, we will develop this value chain approach and explore how it can inform the conceptualization of communications security. In the next section, we look at the methods in ‘security requirements engineering’ and ‘multilateral security’ to provide a more thorough analytical framework for the value chain approach.

2. Security Requirements Engineering

‘Security requirements engineering’ is a method in computer science to elicit the security requirements of a particular communications setting based on the CIA-triad – it is described in section 2.1. In such settings, various stakeholders can have quite different interests. The concept of ‘multilateral security’ helps confronting these interests with one another, and possibly resolving them (section 2.2.).

⁴² Mueller, Schmidt & Kuerbis 2012 provide a quite detailed account of these cases in ‘Internet Security and Networked Governance in International Relations’, *International Studies Review*, 15 86-104, 2003.

⁴³ See Arnbak & Van Eijk 2012. To a lesser extent, see Asghari, Van Eeten, Arnbak & Van Eijk 2013.

2.1. From General Goals to Specific Requirements

The CIA-triad discussed earlier consists of the security attributes confidentiality, integrity and availability. Security goals provide a bit more detail, and are defined across the literature as ‘general statements about the security of an asset’, and ‘aims to protect assets from harm’.⁴⁴ An example of a security goal would be: “the government has the integrity goal that financial transactions in a country do not change the total amount of circulating money.”⁴⁵

In security engineering, merely stating that security attributes or goals are important is not sufficient. The security attributes are not verifiable in themselves and do not give a direction towards the regulated stakeholders how the attributes should be balanced, notably when security goals or stakeholder interests conflict (section 2.2.).⁴⁶

Security requirements in engineering are defined by Haley et al. as ‘constraints on the functions of the system, where these constraints operationalize one or more security goals.’⁴⁷ Fabian et al distinguish three aspects of security requirements: i) they capture security goals in more detail; ii) they indicate a stakeholder and a counter-stakeholder; iii) they describe the applicable laws or other circumstances in which they operate, such as the threat landscape, to which the requirement refers.⁴⁸ Security requirements can originate from the security goals of the developer of a system, as well as from its environment. The aspects of security requirements engineering also correspond well with the aforementioned value chain approach.

Even though the concept of security requirements primarily is concerned with engineering systems, its conceptualization holds useful insights for the (legal) governance of secure communications. The most essential insight is this: recent regulatory instruments and policy documents on the EU level state some security attributes in the definitions sections or preambles, but do not provide guidance on their relationship with what is regulated in the instrument, or how the attributes should be balanced in specific communications settings. Policy makers can learn from security requirements engineers, that their conceptualizations have become too static, and that merely proclaiming security attributes from other legislative texts fails to address the specificity of the communications setting that is regulated, the associated threats or vulnerabilities, and to map stakeholder interests.⁴⁹ As the saying in engineering

⁴⁴ Fabian et al 2010, p. 8. Haley 2006, p. 37.

⁴⁵ Fabian et al 2010, p. 8.

⁴⁶ Fabian et al 2010, p. 8. See also Arnbak & Van Eijk 2012, where we note this omission in the new EU eIDAS Regulation proposal.

⁴⁷ Haley et al 2006, p. 37. Fabian et al conclude that “there is no established terminology in the field of security requirements engineering”, Fabian et al 2010, p. 38.

⁴⁸ Fabian et al 2010, p. 12. Gürses & Santen 2006.

⁴⁹ A schematic overview of the conceptual framework for security requirements engineering of Fabian et al 2010 has been included in the appendix of this paper as it provides a useful insight

goes: “if you don’t know what you want, it’s hard to do it right”.⁵⁰ In addition, it does not address the modalities of authorization.

The balancing of security goals indeed depends on the specific communications setting or application under consideration.⁵¹ Submitting sensitive medical data to a pharmacy requires strict communications confidentiality guarantees,⁵² while watching to a live webcasted concert of your favorite band is more connected to availability and underlying attributes (such as reliability). In security engineering, the specificity of security attributes increases from general attributes, to goals, to requirements, and finally to specifications.⁵³ The question what level of specificity a regulatory instrument should contain depends on many factors, not in the least the type of regulatory instrument, and will be addressed in section 3. First, the situation of conflicting stakeholder interests is discussed.

2.2. Multilateral Security: Addressing Conflicting Stakeholder Interests

In their comparison of several security engineering methods, Fabian et al criticize the widely used methods (such as the ‘Common Criteria’) for assuming that the only stakeholder in a security system is its owner.⁵⁴ But apart from the owner, many stakeholders can have an interest in an asset and it is quite common that these interests do not align. The concept of multilateral security addresses these conflicting interests.

Multilateral security is defined as “providing security for all parties concerned, requiring each party to only minimally trust in the honesty of others:

- Each party has its particular protection goals;
- Each party can formulate its protection goals;
- Security conflicts are recognized and compromises negotiated;
- Each party can enforce its protection goals within the agreed compromise.”⁵⁵

Multilateral security “supports engineers in identifying security goals of the security stakeholders, and in resolving conflicts among them – and in the reconciliation of security goals and other, notably functional, requirements.”⁵⁶ It has “the potential to free users of IT systems from a lack of self-

for policymakers into the relationship of the various concepts and how security requirements are formulated.

⁵⁰ Fabian et al 2010, p. 7.

⁵¹ Avizienis 2004, p. 23.

⁵² CBP 2013.

⁵³ Fabian et al 2010, p. 12.

⁵⁴ Fabian et al 2010, p. 8.

⁵⁵ Pfitzmann 2006.

⁵⁶ Fabian et al 2010, p. 8.

determination concerning their (in)security.”⁵⁷ Several methods (such as the 7-step MSRA method, section 3.1) for eliciting these requirements from multilateral security analysis have been described by Fabian et al 2010 and have been operationalized by a range of authors, such as Gürses & Santen in a case study of multilateral security requirements for an Intranet environment for PhD students.⁵⁸

Just as positive and negative stakeholder interests are “necessary and fruitful” for a requirements engineering team, so can it be for policymakers in secure communications.⁵⁹ The interaction of stakeholder interests is an essential insight into determining how to balance the security attributes in a specific setting. The example of web security browsing of section 1.1 illustrates, that in the HTTPS communications value chain, certificate authorities, websites, browser vendors and end-users have conflicting interests in terms of the security attributes confidentiality, integrity and availability.⁶⁰

The concept of multilateral security again points towards granular and functional approaches towards the conceptualization and governance of communications security. These insights in value chain dynamics, such as conflicting stakeholder interests, are essential in conceptualizing communications security for its legal governance. The next section examines how this value chain approach might inform the conceptualization of communications security and its governance, and in particular the operationalization of the key concept of ‘authorization’ identified in section 1.1.

3. Conceptualizing Communications Security

Conceptualizing communications security is not an easy task. In the areas of software and security engineering, many models exist for engineering security. Fabian et al note that until this date, “no established terminology exists in the field of security requirements engineering” and recommend to combine some of the strengths of these methods in both the design and the development phases of systems.⁶¹ Even in this forward thinking technical community, the conceptualization and realization of security is very much under construction.

Thus, the following development of a value chain approach for communications security conceptualizations still has important gaps. Nonetheless, some insights from security engineering and legal analysis can be merged into one framework. This section sets out to outline and analyze two multilateral security requirements engineering methods, and then synthesizes

⁵⁷ Pfitzmann 2006.

⁵⁸ Gürses & Santen 2006.

⁵⁹ Fabian et al 2010, p. 12.

⁶⁰ Arnbak & Van Eijk 2012.

⁶¹ Fabian et al 2010, p. 38.

the insights in this paper to construct a value chain approach for conceptualizing communications security.⁶²

3.1. Step by Step Engineering Methods: SQUARE and MSRA

Security Quality Requirements Engineering (SQUARE) is a nine-step process developed at the Software Engineering Institute of Carnegie Mellon University.⁶³ It helps organizations to build security into the early stages of the production life cycle.⁶⁴ The main objective of SQUARE is to elicit and document security requirements, which should also be a main objective in policymaking. Both security engineers and stakeholders participate in the nine-step process, which is designed as follows:⁶⁵

1. *Agree on definitions.*
2. *Identify assets and security goals.*
3. *Develop artefacts to support security requirements definition.*
4. *Perform risk assessment.*
5. *Select elicitation technique(s).*
6. *Elicit security requirements.*
7. *Categorize requirements.*
8. *Prioritize requirements.*
9. *Inspect requirements.*

Each of these steps has a range of inputs, techniques, specific participants and outputs. A tool that guides the participants through the process can be downloaded from the SQUARE website.⁶⁶

The first step is to agree on definitions, because different stakeholders have different ideas on what general concepts mean. This lessons should be heeded by policymakers, as the current conceptual ambiguity shows that many people operate similar terms, but attach different values and meanings to those terms – cybersecurity being the obvious example in this regard (see introduction). Interestingly, the second step is considered vital in the SQUARE process: “without overall security goals for the project, it is impossible to identify the priority and relevance of any security requirements that are generated.”⁶⁷ Towards the end of the process, security requirements are categorized and prioritized. It should be noted that SQUARE generates as specific requirements as possible: ‘the call center website mode should be available to at least 300 connections at any given time’ is an example of such a requirement, where “the

⁶² A detailed description falls outside the scope of this paper, but can be found in Fabian et al 2010, Gürses 2010 and Haley 2006.

⁶³ Fabian et al. 2010 compare SQUARE with different other methods.

⁶⁴ See: <https://www.cert.org/sse/square/>

⁶⁵ See: <https://www.cert.org/sse/square/square-ninesteps.html>.

⁶⁶ See: <https://www.cert.org/sse/square/square-tool.html>

⁶⁷ See: <https://www.cert.org/sse/square/square-faq.html>

system shall improve the availability of the existing customer service center” is a security goal. The outcome of the SQUARE process is a set of prioritized goals and requirements which can then inform the design of the system.

Several authors argue that upon finishing a security engineering process, such as SQUARE, it should be complemented with multilateral security engineering to illuminate and consolidate stakeholder interactions and conflicts. Fabian et al. describe one influential method, the Multilateral Security Requirements Analysis (MSRA):

1. *Identify stakeholders.*
2. *Identify episodes.*
3. *Elaborate security goals.*
4. *Identify facts and assumptions.*
5. *Refine stakeholder views on episodes.*
6. *Reconcile security goals.*
7. *Reconcile security and functional requirements.*

In both models, the security goals are derived from the CIA-triad.⁶⁸ A particularly valuable insight for policy conceptualizations in the multilateral approach, is that stakeholders not only have conflicting interests in terms of the security goals (some might prioritize confidentiality, others availability), but also that stakeholders might have similar interests that conflict in relation to another stakeholder. Multilateral security engineering therefore ties a counter-stakeholder to a stakeholder with an interest in a particular security requirement. For example, a user may have a confidentiality interest in a social network towards the social network, an attacker, other users and/or the government. The interesting point is, that in multilateral security engineering this is not problematic, but it is an assumption that provides necessary input to elaborate, negotiate, balance and enforce the conflicting stakeholder interests. In the process, multilateral security “requires each party to only minimally trust in the honesty of others,”⁶⁹ as the process is meant to illuminate these conflicts. In a world of PRISMs, in which not only government authorities but the largest internet companies seem to have been systematically giving incomplete information on their collaboration with surveillance practices, it might just be a very sensible approach anyway.

In the next section, we will flesh out insights multilateral security requirements engineering holds for developing a value chain approach to communications security conceptualizations.

⁶⁸ Fabian et al. 2010, p.16-18.

⁶⁹ Pfitzmann 2006.

3.2. Governance: Communications Security Value Chains

What insights can be extrapolated from the analysis in the previous sections? In the spirit of the steps devised in the SQAURE and MSRA methods and in a modest attempt to further developing the value chain approach to communications security conceptualizations, the following steps may be identified:

1. *Identify the specific communications setting.*
2. *Agree on security definitions.*
3. *Identify communications security goals and authorizations.*
4. *Identify stakeholders (intermediaries), incentives and interactions.*
5. *Apprise relevant constitutional values.*
6. *Balance security goals, reconcile with broader values.*
7. *Perform risk assessment of outcomes.*
8. *Consider policy intervention.*
9. *Inspect outcomes.*

While acknowledging this is early-stage research, several points can be made at this point. Any conceptualization of communications security should start with identifying the specific communications setting under consideration. Communications security operates differently in a HTTPS setting than in fixed landline mediated communications. This first step of ‘Identifying the communications setting’ adopts a functional, granular perspective. The value chain approach thus sets out to force governance actors to map how the actual communications setting operates. The functional perspective informs us that there is no reason in principle why What’s App mediated text messages should be treated differently from a communications security perspective than SMS text messages through your telecommunications provider or performing a Skype chat.

The next step is to agree on the security definitions. This step adopts the technical conception of security outlined in section 1.1. and integrates the CIA-triad in the value chain approach. It also focuses those involved in the governance of communications security on the key concept of authorization. Governance actors are also confronted with the many different sources of authorization, such as a private contract, consent or authorizations that arise from general public law. These sources should be taken into account when determining security goals.

In identifying communications security goals, a normative assessment can be made what goals are desired for the communications setting under consideration. These will be generally framed along the lines of the CIA-triad and the concept of authorization. For example, ‘end-users should be guaranteed a high level of trust in the confidentiality of HTTPS communications, and be provided with end-to-end protection from a man in the middle attack’.

Upon identifying the goals in a specific communications setting, the chain of intermediaries can be mapped in more detail. Who are the relevant stakeholders in the communications setting under consideration, what are their characteristics and interests? What are their incentives for security, and how does the chain of intermediaries interact? Security economics analysis may prove very helpful in this step.⁷⁰

Then, the relevant constitutional values need to be identified. These serve as a baseline, or as the legal criteria, for the governance of communications security in the specific setting. The constitutional values can correct security goals that may give unrestricted access to confidential communications. In Europe, the recent case law discussed in section 1.1. points at strong positive constitutional obligations to ensure communications security in a form of governance that provides meaningful protection. The extent of these constitutional obligations depends on the specific circumstances of the communications setting under consideration. End-users receive stronger protection than legal persons, but the latter also have legitimate claims to these values. The constitutional criteria of course differ across regions. In the current set-up of the value chain approach, the specific circumstances relevant for identifying the constitutional criteria have been mapped before this step.

The critical next step is to balance the set of security goals and reconcile them with broader values endogenous to the communications setting, such as usability and functionality, as well as exogenous to it, such as policing cybercrime, stimulating the digital economy.⁷¹

At this point, a risk assessment can be performed of the incentives for security in the specific communications setting. What are the probabilities that the market, networked communities or ad hoc governance networks in the specific setting achieve the desired security goals devised in the previous step? Is there an unacceptable risk that the appropriate balance of security goals and broader values concerned cannot be reached? Risk may not be the right concept, however, as risk assessments are increasingly difficult in complex environments.⁷² The concept of assurance may be more appropriate at this stage of the value chain approach, defined as the “measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.”⁷³

If an informed analysis points to the fact that this may be the case, governance response may be warranted. Governance responses can take many forms, the various instruments vary per region. The level of specificity and the modalities of governance are interesting questions for further research, and is one of the many issues to be addressed in future work connected to this project.

⁷⁰ Anderson et al. Asghari, Van Eeten, Arnbak & Van Eijk 2013.

⁷¹ Haley 2006.

⁷² Mulligan & Schneider. "Doctrine for Cybersecurity". *Dædalus, the Journal of the American Academy of Arts & Sciences*, 140(4), 2011.

⁷³ CNSSI-4009; SP 800-39.

Finally, mechanisms for inspecting whether a communications setting sustains to perform according to the stated security goals should be in place. Many communications settings or regions will already have such governance structures in place.⁷⁴

Future work will further develop the value chain approach and assess how it works out in practise through several case studies.⁷⁵ While far from complete or perfect, this first attempt at a general value chain approach for communications security conceptualizations has several promising features: it allows for granular and functional conceptualizations of communications security and its legal governance. It can be tailored not only to specific communications settings, but it can also be applied across jurisdictions. The approach synthesizes important insights from (multilateral) security requirements engineering and translates them into the policy arena. It reorients security policies towards their technical conception, rather than conflating them with a range of other policy issues. These only come into account in the final steps of the approach, which should allow for solving the root causes of security issues first, and only then looking at the residual policy problems that remain. The value chain approach is also a counterweight to mixing unrelated social problems with one another under the umbrella of cybersecurity policymaking. Moreover, it provides a framework for balancing underlying security goals, interests of stakeholders and public values in a complex policy area of communications security, on which we all increasingly depend all day, every day.

At the E.U. level, policies generally shy away from forward thinking approaches. Insights such as the ones touched upon in this paper, let alone comprehensive assessments, remain absent from communications security policymaking. In E.U. instruments, usually some general claims will be made about security, but the details – even the security goals – are left wide open and to be discussed in delegated acts that appear years after the initial publication of a regulatory instrument (see section 1.2). New instruments, such as the E.U. Regulation on Electronic Identification and Trusted Services proposed by the European Commission in the aftermath of the Diginotar incident, never start with identifying security goals nor the relevant intermediaries, nor do they tailor their conceptualization of ‘communication security’ to the specific setting under consideration, let alone how the underlying values, interests and constitutional obligations of the associated stakeholders interact.⁷⁶

The current confrontation with complexity and dependence requires creative thinking and a certain amount of courage – one might even call it a white hat hacker spirit – of those responsible for the legal governance of secure

⁷⁴ Mueller 2010.

⁷⁵ A paragraph 3.3 will be added to upcoming versions of the paper, titled ‘3.3. Adopting the Approach in Practise: HTTPS Governance’.

⁷⁶ Arnbak & Van Eijk 2012.

communications. The time is as good as any to challenge ourselves, to welcome constructive critique and open the debate on how to address the conceptualization and governance of communications security.

4. Concluding Remarks

Communications security conceptualizations rely too heavily on static definitions in legal frameworks and the conceptual ambiguity of the ‘cybersecurity’ frame. Instead, one of the conclusions of this paper is that the conceptualization of communications security needs granular and functional approaches, tailored to specific communications settings. This facilitates adaptable policies in the dynamic socio-technical networked communications environment of today. Furthermore, the conceptualization of ‘security’ is in dire need of reorientation towards its technical conception: protecting communications confidentiality, integrity and availability for authorized entities.

Inspired by multilateral security engineering methods, this paper has suggested a 9-step plan to conceptualize security in communications value chains: 1) *Identify the specific communications setting*; 2) *Agree on security definitions*; 3) *Identify communications security goals and authorizations*; 4) *Identify stakeholders (intermediaries), incentives and interactions*; 5) *Apprise relevant constitutional values*; 6) *Balance security goals, reconcile with broader values*. 7) *Perform risk assessment of outcomes*; 8) *Consider policy intervention*; 9) *Inspect outcomes*. A value chain approach enables policymakers, both at the E.U. level and beyond, to adapt to the current socio-technical realities and realize communications security in a way that apprises constitutional values, balances the interests of the stakeholders involved and opts for the technical conception of security.

This paper is in an early-research phase. As part of a four-year research project, future work will further develop the value chain approach suggested here and research the positive obligations, or constitutional criteria, ensuring for communications security. Several case studies will be conducted to explore the usefulness of the value chain approach in various communications settings, such as HTTPS communications and addressing governmental access to cloud data from abroad. The scope of the analysis will be broadened to cover the U.S. legal framework.

Appendix: Overview Security Requirements Engineering Framework⁷⁷

Fig. 1 Conceptual framework for SRE

⁷⁷ Fabian et al 2010, p. 10.