UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií, Katedra mezinárodních vztahů

Diplomová práce

2014 **Jakub Rozsypal**

UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut politologických studií**, Katedra mezinárodních vztahů**

Jakub Rozsypal

The Conundrum of Cybersecurity: Concepts, Modalities and Threat Framing of the European Union

Diplomová práce

Praha 2014

Autor práce: **Bc. Jakub Rozsypal**

Vedoucí práce: **PhDr. Vít Střítecký, M.Phil., Ph.D.**

Rok obhajoby: 2014

Bibliografický záznam

ROZSYPAL, Jakub. *The Conundrum of Cybersecurity: Concepts, Modalities and Threat Narrative of the European Union.* Praha, 2014. 85 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut politologických studií. Katedra mezinárodních vztahů. Vedoucí diplomové práce PhDr. Vít Střítecký, M.Phil., Ph.D.

Abstrakt

Tato práce se zabývá komplexním tématem kybernetické bezpečnosti v mezinárodních vztazích, specifiky kyberprostoru vzhledem k jeho vzniku a technické povaze a přístupu k bezpečnosti informačních a komunikačních technologií očima Evropské unie. Ačkoliv se kybernetická bezpečnost jako kategorie dostává v posledních dvaceti letech stále častěji do uvažování o bezpečnosti a související politické debatě, některé základní koncepty jsou stále nedostatečně uchopené. První část práce se proto zabývá kybernetickým prostorem a jeho specifiky a poukáže na některé inherentní rozpory mezi světem tradičních westfálských států a fluidním charakterem digitálního světa. Analýzou dosavadních incidentů v kyberprostoru a také absencí zásadních „digitálních katastrof" bude poukázáno na rozpor mezi teorií a realitou. Celá práce vychází z konstruktivistického metodologického rámce pracujícího s intersubjektivitou. V závěrečné části zabývající se Evropskou unií je to přístup tzv. formulace hrozby (*threat framing)* skrze který je analyzována narativ EU v záležitostech kybernetické bezpečnosti. Tento je identifikován jako „fundamentální stavební blok společnosti" s tendencí dostávat se do hlavního proudu politiky prostřednictvím několika kanálů: kybernetická kriminalita, kybernetická obrana, ochrana kritické infrastruktury, protiteroristická politika a širší normativní pohled pod názvem Digitální agenda.

Abstract

This thesis deals with the complex issue of cyber security in international relations, specifics of cyber realm due to its technical nature and particular circumstances of its development as well as with the way how the EU deals with information and communication technologies. Even though cyber security as a category appears with increasing frequency and intensity in the thinking on security and related political debate in the past twenty years, some of its basic tenets are still insufficiently understood. First part of the thesis deals with cyber realm and its specifics as such with effort to pinpoint some of the inherent contradictions between the traditional Westphalian nation states and the fluid character of the digital world. Through analysis of selected relevant incidents as well convincing absence of the "digital-doom" scenarios the peculiar expectation-reality discrepancy will be analysed. The overarching method departs from intersubjective securitization framework. In the last part analysing the EU it is the concept of *threat framing* that is applied to study and trace the narrative of the EU in these matters. Here a gradual construction of a narrative termed ICT as "fundamental societal building block" reveals itself with cyber related issues making its way into top policy levels through various channels: Cyber-crime, Cyber-defense, Critical Infrastructure Protection, Counter-Terrorism and overarching normative effort termed Digital Agenda.

Klíčová slova

Kybernetická bezpečnost, formulace hrozby, Evropská unie, epistemické komunity, étos internetu, sekuritizace, informační a komunikační technologie

Keywords

Cybersecurity, threat framing, European Union, epistemic communities, ethos of the internet, securitization, information and communication technologies

Rozsah práce: 130 111 znaků

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracoval/a samostatně a použil/a jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne …30. 07. 2014 Jakub Rozsypal

Poděkování:

Na tomto místě bych rád poděkoval svému vedoucímu PhDr. Vítu Stříteckému za cenné rady, Jonathanovi Soderbergovi z firmy Protection Group International, Laurentu Bernatovi z OECD taktéž za užitečné vhledy do problematiky. Zejména bych chtěl poděkovat svým rodičům, kteří mě po celou dobu studia podporovali.

Here I would like to thank my supervisor PhDr. Vít Střítecký for valuable leadership and insight, to Jonathan Soderberg from Protection Group International and Laurent Bernat of OECD for useful advice in these matters. Especially, I would like to thank my parents who have been supporting me throughout my studies.

UNIVERZITA KARLOVA V PRAZE
FAKULTA SOCIÁLNÍCH VĚD
INSTITUT POLITOLOGICKÝCH STUDIÍ

Bezpečnostní studia

projekt diplomové práce

The Conundrum of Cyber security: What role for the EU?

LS 2013

Vedoucí práce: PhDr. Vít Střítecký, M.Phil., Ph.D.

Cyber security became a prominent aspect in the security discourse at least since the end of the Cold War. Together with technological advancements a policy window was opened that allowed for the securitisation of IT mostly as a new weapon in potential war but not a qualitative change in the nature of security(Eriksson, 2001, pp. 218-219). Moreover, focus on highly vulnerable infrastructures and their protection emerged as the norm within broader securitization of the cyberspace (Cavelty 2012). Disastrous scenarios of massive cyber-war or cyber-terrorism occurrences failed to materialize and the phenomenon of Y2K served as a reality check and went to show how much can perception and reality differ. Yet there is broad consensus that security in the virtual space poses a strategic risk and most recently the EU has tied security of ICT technologies to such core values as *freedom and prosperity* in its Cybersecurity strategy (European Commission 2013a). In addition to this apparent mismatch between discourse of fear and reality of prevalent positive development a peculiar lack of scholarship that is able to connect the technical side of ICT and the more general theories in Security studies catches one's attention (Eriksson, Giacomello 2006).

The dynamics of the Cyber sector

The proposed thesis will try to capture the specific dynamics of the cyber sector and the way it differs from other aspects of security in general. It has been argued that *hypersecuritization* (threats are relevant to all referent objects due to network nature of the environment) as well as *technification* (the problem is highly sophisticated and changes rapidly overtime, which makes it difficult to create meaningful policy) (Hansen, Nissenbaum 2009). From market and economic point of view security in virtual space resembles environmental security and makes for a good example of a public good – overwhelmingly privately owned sector lacks the incentives to invest in security and thus it is desirable for the public sector to step in (Cavelty, 2008, pp 30-31). Anonymity of current open-architecture of the web allows for intense asymmetry of threats, this is in part because the TCP/IP protocol was never built with security in mind. New technologies such as IPv6 could radically fix this shortcoming (K Geers 2011). Additionally, *collapse of time and distance* within the virtual sphere (Der Derian 2003) makes traditional territory-based approaches rather obsolete. Cyber security has

no founding history of defining events and has to find analogies to conventional events in mobilizing audiences (Hansen, Nissenbaum 2009). It seems plausible to argue, that threats in the cyber domain can only be overcome by intersectoral and international cooperation (Świątkowska 2012).

The method

The thesis will employ a perspective of *threat framing* (Eriksson 2001a)(Cavelty 2008a) (Eriksson, Noreen 2002b). This framework can be understood as an extension of the Copenhagen School approach (Buzan, Wæver, Wilde 1998) beyond mere *speech act* to a more holistic approach. Framing is a struggle over the social meaning of what the issue consists of and what is to be done. The framework consists of:

- the framing actor (the EU)
- type of referent object (network, information assurance, critical infrastructure)
- frame characteristics (elaborated – subject to change and contested)

The frame forms our understanding of how and why certain issues gain salience on the political agenda. The model comes close to agenda-setting theories(Kingdon 2003; Princen 2009; Princen, Rhinard 2006), yet is dynamic and allows explanation in change due to policy diffusion, interpretation of new threats in established institutions, which fits neatly in the realm of cyber and allows for multi-causal explanations. Figure 1 shows how a frame is constructed and in what way it influences agenda. In the next step the effects provide feedback to the cognitive part and the process reproduces itself.

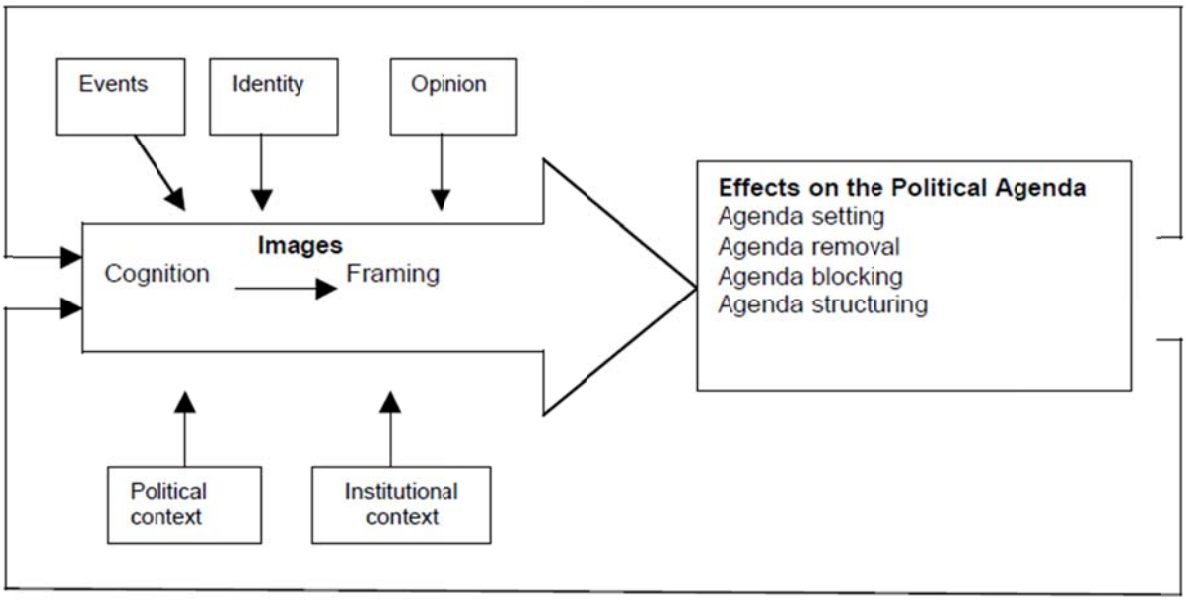

FIGURE 1 (ERIKSSON, NOREEN 2002 P. 19)

The case

The EU was chosen on the basis of the nature of the cyber-sector, the thesis will argue that the type of actor the EU is (international/supranational) puts it in a better position to deal with these insecurities than traditional smaller units such as individual states. Since the consensus holds that ICT technologies are beneficial and help societies develop the notion that a state can deal with providing security in its own territory is not feasible due to the open-architecture network characteristic. Additionally, the EU can be viewed as having a wide perspective on security as such and thus aim for providing *information assurance* in a broad sense.

The aim

The aim of this thesis will be to analyse the landscape of cyber security and provide insight into how agenda regarding cyber sector is set at the EU level. Constructivist threat framing framework will be used to gain understanding into processes that drive the securitization of ICT technologies in the EU. It will aim to explain change of how cyberthreats are perceived from the beginnings of the WWW up till now. Finally, the previous steps will allow for a critical examination of the EU role within the cyber

security sector and open up space for author's own recommendations. The main argument will build on the notion that the EU can employ its comprehensive multilayered approach to Cybersecurity and create adequate and effective strategy to secure the cyber domain.

Questions that will be answered within the thesis include:

- What are the dynamics of Cybersector? How does it differ from the offline world?
- How does the EU frame Cybersecurity? What are the securitizing moves employed in order to achieve this?
- What role should the EU play? Why does it make more sense to provide security through international/supranational institution?

The structure

Literature

Non-periodical:

BAYUK, Jennifer L., HEALEY, Jason, ROHMEYER, Paul, SACHS, Marcus H., SCHMIDT, Jeffrey and WEISS, Joseph, 2012. *Cyber Security Policy Guidebook* Hoboken: John Wiley & Sons. ISBN 1118027809.

BUZAN, Barry, WÆVER, Ole and WILDE, Jaap De, 1998. *Security: A New Framework For Analysis* [online]. S.l.: Lynne Rienner Publishers. [Accessed 25 October 2012]. ISBN 1555877842. Available from: http://books.google.com/books?hl=en&lr=&id=j4BGr-Elsp8C&pgis=1.

CASTELLS, Manuel, 2004. *The rise of the network society*. Oxford: Blackwell Publishing Ltd.

CAVELTY, Myriam Dunn, 2008a. *Cyber-security and Threat Politics: US Efforts to Secure the Information Age* [online]. S.l.: Routledge. [Accessed 21 May 2013]. ISBN 0415429811. Available from: http://books.google.com/books?id=QEjX-pv0_PcC&pgis=1.

CAVELTY, Myriam Dunn, 2012. The militarisation of cyber security as a source of global tension. In: MÖCKLI, Daniel (ed.), *Strategic Trends 2012* [online]. Zurich: Center for Security Studies, ETH Zurich. ISBN 978-3-905696-36-3. Available from: http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012-Cyber.pdf.

DINNISS, Heather Harrison, 2012. *Cyber Warfare and the Laws of War* [online]. S.l.: Cambridge University Press. [Accessed 2 June 2013]. ISBN 1107011086. Available from: http://books.google.com/books?id=ubgAOmSHbAoC&pgis=1.

ERIKSSON, Johan and GIACOMELLO, Giampiero, 2007. *International relations and security in the digital age* [online]. New York: Routledge.

GEERS, K, 2011. *Strategic cyber security*, Tallinn: CCD COE Publication. ISBN 9789949904051.

GORI, Umberto, 2009. Modelling cyber security. In: *NATO Advanced Research Workshop on Operational Network Intelligence: Today and Tomorrow*. Washington, D.C.: Ios Press. 2009. pp. 215.

KINGDON, John W., 2003. *Agendas, alternatives, and public policies* [online]. 2nd. New York: Longman. [Accessed 31 May 2013]. ISBN 0321121856. Available from: http://books.google.com/books?id=hSolAQAAIAAJ&pgis=1.
LEWIS, James Andrew.2003, Cyber Security: Turning National Solutions Into International Cooperation, Center for Strategic and International Studies, Washington D.C., 2003, 144 s. ISBN 0892064269
PRINCEN, Sebastiaan, 2009. *Agenda-setting in the European Union* [online]. S.l.: Palgrave Macmillan. [Accessed 29 May 2013]. ISBN 0230220533.
ROBINSON, Neil, Emma DISLEY, Dimitris POTOGLOU, Anais REDING, Deirdre May CULLEY, Maryse PENNY, Maarten BOTTERMAN, Gwendolyn CARPENTER, Colin BLACKMAN and Jeremy MILLARD,2012, Feasibility Study for a European Cybercrime Centre, Santa Monica, Calif: RAND Corporation, TR-1218-EC, 2012
SOMMER, Peter a BROWN, Ian, 2011 Reducing Systemic Cybersecurity Risk. Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. Available at: http://ssrn.com/abstract=1743384
ŚWIĄTKOWSKA, Joanna, 2012. Cyberthreats as a Challenge to the Security of the Contemporary World. In: ŚWIĄTKOWSKA, Joanna (ed.), *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations*. Krakow: The Kosciuszko Institute. pp. 47. ISBN 9788393109364.
WAEVER, O. 1993, Securitization and Desecuritization, Copenhagen : Centre for Peace and Conflict Research, 1993, (COPRI Working Papers ; No.5)
WESTBY, Jody R.2004, International Guide to Cyber Security, American Bar Association, 2004, 330s. ISBN 1590313321

Periodical:

BISOGNI Fabio, CAVALLINI Simona, DI TROCCHIO Sara, 2011, Cybersecurity at European Level: The Role of Information Availability, Communications & Strategies, 81, 1st Q. 2011, p. 105.
ERIKSSON, Johan, 2001a. Cyberplagues, IT, and security: Threat politics in the information age. In: *Journal of Contingencies and Crisis Management* [online]. December 2001. Vol. 9, no. 4, pp. 200–210. [Accessed 11 May 2013]. DOI 10.1111/1468-5973.00171. Available from: http://www.blackwell-synergy.com/links/doi/10.1111/1468-5973.00171.
ERIKSSON, Johan, 2001b. Cyberplagues, IT, and Security: Threat Politics in the Information Age. In: *Journal of Contingencies and Crisis Management* [online]. December 2001. Vol. 9, no. 4, pp. 200–210. DOI 10.1111/1468-5973.00171. Available from: http://www.blackwell-synergy.com/links/doi/10.1111%2F1468-5973.00171.
ERIKSSON, Johan, 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? In: *International Political Science Review/ Revue internationale de science politique* [online]. 2006. Vol. 27, no. 3, pp. 221–244. [Accessed 28 February 2013]. DOI 10.1177/0192512106064462. Available from: http://ips.sagepub.com/cgi/doi/10.1177/0192512106064462.
ERIKSSON, Johan and GIACOMELLO, Giampiero, 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? In: *International Political Science Review/ Revue internationale de science politique* [online]. 2006. Vol. 27, no. 3, pp. 221–244. [Accessed 23 May 2013]. DOI 10.1177/0192512106064462. Available from: http://ips.sagepub.com/cgi/doi/10.1177/0192512106064462.
CAVELTY, Myriam Dunn, 2008b. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. In: *Journal of Information Technology & Politics* [online]. 2008. Vol. 4, no. 1, pp. 19–36. [Accessed 6 May 2013]. DOI 10.1300/J516v04n01. Available from: http://www.tandfonline.com/doi/full/10.1300/J516v04n01_03.
DEIBERT, Ron J., 2003. Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. In: *Millennium - Journal of International Studies* [online]. 1 December 2003. Vol. 32, no. 3, pp. 501–530. [Accessed 3 April 2013]. DOI 10.1177/03058298030320030801. Available from: http://mil.sagepub.com/cgi/doi/10.1177/03058298030320030801.

DER DERIAN, James, 2003. The Question of Information Technology in International Relations. In: *Millennium - Journal of International Studies* [online]. 1 December 2003. Vol. 32, no. 3, pp. 441–456. [Accessed 3 May 2013]. DOI 10.1177/03058298030320030501. Available from: http://mil.sagepub.com/cgi/doi/10.1177/03058298030320030501.

ERIKSSON, Johan and GIACOMELLO, Giampiero, 2007. *International relations and security in the digital age* [online]. New York: Routledge.
ERIKSSON, Johan and NOREEN, Erik, 2002a. *Setting the agenda of threats: An explanatory model*. Uppsala: Department of Peace and Conflict Research, Uppsala University Uppsala. ISBN 9150616145.

ERIKSSON, Johan and NOREEN, Erik, 2002b. *Setting the agenda of threats: An explanatory model* [online]. Uppsala: Eriksson, Johan, and Erik Noreen. Setting the agenda of threats: An explanatory model. Uppsala: Department of Peace and Conflict Research, Uppsala University. [Accessed 9 May 2013]. Available from: http://www.musik.uu.se/digitalAssets/18/18591_uprp_no_6.pdf.
GEERS, Kenneth, 2010. Live Fire Exercise: Preparing for Cyber War. In: *Journal of Homeland Security and Emergency Management* [online]. 2010. Vol. 7, no. 1. [Accessed 27 May 2013]. Available from: http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1780/jhsem.2010.7.1.1780.xml.
GOODMAN, Will, 2010. Cyber Deterrence: Tougher in Theory than in Practice? In: *Strategic Studies Quarterly* [online]. 2010. no. Fall, pp. 102–135. [Accessed 31 May 2013]. Available from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA528033.
HANSEN, Lene and NISSENBAUM, Helen, 2009. Digital disaster, cyber security, and the Copenhagen School. In: *International Studies Quarterly* [online]. 2009. Vol. 53, pp. 1155–1175. [Accessed 28 October 2012]. Available from: http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/full.
KRAUSE, K., WILLIAMS, M.C. 1996, Broadening the Agenda of Security Studies: Politics and Methods, in Mershon International Studies Review (1996) 40, 229-231.
PRINCEN, Sebastiaan and RHINARD, Mark, 2006. Crashing and creeping: agenda-setting dynamics in the European Union. In: *Journal of European Public Policy* [online]. September 2006. Vol. 13, no. 7, pp. 1119–1132. [Accessed 30 May 2013]. DOI 10.1080/13501760600924233. Available from: http://dx.doi.org/10.1080/13501760600924233.
RID, Thomas, 2012. Cyber war will not take place. In: *Journal of strategic studies* [online]. 2012. Vol. 35, no. April. [Accessed 31 May 2013]. Available from: http://books.google.com/books?id=hSolAQAAIAAJ&pgis=1.
SCHMITT, Michael N, 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. ISBN 1107024439.
SUND,Christine.2007, Towards an international road-map for cybersecurity, Online Information Review, Volume 31 Issue 5, 2007 pp.566 – 582
WILLIAMS, M. 2003, Words, Images, Enemies: Securitization and International Politics, International Studies Quarterly (2003) 47, 511-531

Sources, studies:

ASHTON, Catherine, 2013. *Remarks by EU High Representative Catherine Ashton at press conference on the launch of the EU's Cyber Security Strategy* [online]. S.l. Available from: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135287.pdf.
COUNCIL OF EUROPE, 2004, Convention on Cybercrime CETS No.: 185, Brussels, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG
ENISA, 2012a, National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace,
ENISA, 2012b. *Threat Landscape Responding to the Evolving Threat Environment*. Heraklion.
EPC, 2010. *The Economic Impact of a European Digital Single Market*. Copenhagen.
EUROPEAN COMMISSION, 2008. *Report on the implementation of the European Security Strategy and ESDP* [online]. 2008. Brussels: s.n. [Accessed 2 June 2013]. Available from:

http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Report+on+the+Implementation+of+the+European+Security+Strategy#6.
EUROPEAN COMMISSION, 2013a. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels.
EUROPEAN COMMISSION, 2013b. *EU Cybersecurity plan to protect open internet and online freedom and opportunity*. 2013. Brussels: European Comission.

Contents

1. Introduction

"Cyberwar is coming!" argued John Arquilla and David F. Ronfeldt of RAND Corporation more than 20 years ago[1]. Moreover, they have expanded on their argument to suggest that new conflicts will be waged through low-intensity *netwar* as well as a more blatant confrontation that would conform to the term *cyberwar*[2]. Since then a profound discursive shift has taken place. Cybersecurity concerns are now commonplace in strategies of national security[3], military doctrines as well as everyday practices. Yet there were no major incidents causing harm on a mass scale and military hardware was not substituted for lines of weapon-grade code.

This thesis will analyse how did cyber sector come about and how did it become a front-burner security issue with special attention to the EU as relevant security actor and its framing of the cyberthreats. Correspondingly to the shift in salience of cyber issues the EU has sought to establish itself as a non-traditional yet relevant security actor, which creates a potent double dynamic. Disastrous scenarios of massive cyber-war or cyber-terrorism occurrences failed to materialize and the phenomenon of Y2K[4] served as a reality check and went to show how much can perception and reality differ. Yet there is broad consensus that security in the virtual space poses a strategic risk. Recently the EU has tied security of information and communication technologies (ICT) to such core values as freedom and prosperity in its Cybersecurity strategy (European Commission 2013a). There is a dubious mismatch between discourse of fear and reality that admittedly does not conform to projected threat images utilizing analogies such as electronic Pearl Harbor. Furthermore, a peculiar lack of scholarship that is able to connect the technical side of ICT and the more general theories in Security studies catches one's attention (Eriksson, Giacomello 2007). Another aspect of interest is

---

[1] (Arquilla, Ronfeldt 1993)
[2] (Arquilla, Ronfeldt 1995)
[3] For a comprehensive list of proliferation of national and international cyber security strategies see (ENISA 2014)
[4] Widely discussed problem of technical nature also known as the Millennium bug resulting from historical abbreviation of 4 digits of any year in dates to 2 digits – thus presenting software with potential logical error when ambiguous 00 was approaching. Whether through effective preparation or overemphasis of the problem it turned out to be a non-case (Meares, Fukumoto 2010). On the other hand it was a watershed in investment into ICT security.

whether traditional concepts used in strategic connotations in the context of international relations such as deterrence, sovereignty and definition of act of force apply in the novel realities of the cyber realm or whether a new approach is needed. The common position is that international law does extend into cyberspace (Schmitt 2012), also with the applicability of the Marten's clause that posits that means of warfare are not unlimited (Goldblat 2002, pp. 294-295).

Cyberspace provides a unique combination of the amalgamation of traditionally distinct categories of private and public, spanning wide area from human rights through economic prosperity to sovereignty issues and questions of internet governance. Its distinctly technical and expertise-contingent nature influences modalities of discourse by taking into seemingly expert non-political sphere of discussion. It is this complexity that will provide rich study material for the purpose of this thesis that seeks to untangle at least parts of this conundrum and elaborate on the most important concepts as well as critically analyse EU and its policy and analytical frame.

1.1. Structure of the thesis, methodology and research questions

In the first part (chapter 2) cyber domain will be briefly but sufficiently dealt with. It is particularly important to grasp some of the structural and technical features of the global network of networks to be able to understand how these constrain strategic and policy choices. The global network has its root in the military as well as scientific field; as such it was not intended to become omnipresent universal communication field as it stands now.

There is a certain ethos of freedom surrounding internet usage that is enabled and amplified by the predominantly private ownership of infrastructure (Ryan 2010)(Ziccardi 2012). Thus it is not self-evident that states should extend their sovereignty into the virtual space. Framing of ICT through steps of cognition,

interpretation and normative case by the EU will be dealt with in the third chapter. This analysis does not paint a full picture without insights from epistemic communities and strategic culture research that allows for grasping of ideational factors behind policy action. Through the analysis of official EU strategic documents and outputs the research will capture the dynamics of how did ICT related issues become one of the most salient topics of nascent EU security policy and other related policy areas as well. The novelty of cyber sector, where amalgamation of the private and public is commonplace fits rather well with the unique character of the European Union as quasi-sovereign actor that has served the function of blurring the boundaries between inside and outside successfully for several decades and wields significant symbolic power, thus providing a good position for value projection (Bigo 2000).

Furthermore, this thesis argues that security within cyber realm is better understood as risk management as opposed to the dichotomous traditional category of security/insecurity tied to survival c.f. (Cavelty 2008a). Critique of the hypersecuritization of the cyber sector will be drawn by pointing to the absence of expected large scale attack, thus utilizing non-cases to further the argument. The aim of this work is not to make a definitive statement on either cyber security approaches or pronouncing verdict on EU cyber security. It is rather to uncover most important trends and factors and fuse the predominantly technical world of ICT expertise to policy-making and IR strategic concepts.

1.2. Methodology

Methodologically, the thesis takes as its starting point theoretical apparatus of *threat framing* (Eriksson 2001a; Cavelty 2008b; Eriksson, Noreen 2002). This method belongs broadly to the constructivist camp of Copenhagen school of securitization as elaborated most succinctly by Buzan, Wæver, Wilde (1998).

However compared to the restrictive requirement of speech act in the sense of verbal communication it is more open to other factors such as visual communication

and everyday security practices. As such it paints a fuller picture and comes somewhat close to agenda-setting model[5] it suits well the chosen case of supranational institution due to less restricted input constraints. Threat framing should be understood as struggle over social meaning, which is constructed intersubjectively through various methods. Here it draws on influences from the French sociological tradition such as Bourdieu's concept of *symbolic violence* that points to how wielders of *social capital* e.g. policy makers deploy their power to define meanings (Bourdieu 1999). The creation of meaning among actors understood as intersubjective is fruitful in ontology of (not only) social relations. In other words, there is only reality understood and created as subjective interpretation by individuals and groups and phenomena are established by these disparate views. Shared backgrounds and historical processes shape these understandings in a very strong manner, almost to give the impression of inevitability or a causal relation with institutions that self-perpetuate these identities and orders in a hegemonic fashion(Cox 1981).

Yet it is the view taken within this analysis that elevating particular historical processes into objective and stand-alone black-box-like facts is not intellectually feasible .That is where the traditional theories of International Relations be it from the realist or liberal camp fall short. Even though attempts such as Stephen Walt's *balance of threat*[6] sought to improve the rather obvious inability of realism to deal with ideational factors, it still falls short in dissecting these ideas, tracing their roots and placing them in wider narratives. Concepts such as "sovereignty" that are often treated as given in a simplifying manner are only one of many possible configurations of how interactions between social units can look like (Walker 1990). The methodological approach of *threat framing* will allow for analysis of the relationship between substance of threat and its politicization and securitization, which is certainly not self-evident, uniform or following any given set of rules and must be scrutinized thoroughly (Eriksson, Noreen 2002, pp. 1-3).

[5]As elaborated for example in (Kingdon 2003; Princen, Rhinard 2006; Princen 2009)
[6] (Walt 1985, 1990)

It is particularly interesting to follow how a new type of human endeavour, such as interactions in virtual space in this case, gets framed and practices are solidified by norms or put within larger narrative. The framing tends to have a liberal/civil society basis in the West's narrative of upholding human rights in the online world as well as in the offline world which is seen as the key to prosperity[7]. States with rather less liberal democratic experience on the other hand seek to frame virtual sphere within their own sovereignty in order to gain tighter control. It is no coincidence that critical approach to sovereignty as a concept was mentioned beforehand, since that is one of the core tenets of the current setting that cyber dynamics put pressure on. The chosen framework that is informed by constructivist ontology will allow for critical assessment of how existing structures and predispositions grapple with new occurrences such as the elusive cyber threat. Moreover, treating security as intersubjective process will allow for inclusion of various subjects – referent objects – as well as inclusion of additional sectors (Williams 2003, pp 512-513). This feature is particularly useful for analysing the cyber realm since it cuts across both horizontal and vertical notions of what and who can be securitized.

Part of the research will also draw on the work done in cognitive social research - namely epistemic communities approach[8]. This strand of theory is fruitful in looking into how shared knowledge is created within expert communities, which the EU institutions dealing with cyber security related problems fit nicely e.g. Crisis Management and Planning Directorate (CMPD) and European Union Military Staff (EUMS). In this sense epistemic communities shape understanding of reality and define as well as constraint possible courses of action and thus influence the policy-making elite. Creation of norms and their subsequent codification is one of crucial forms of expression of epistemic, arguably in cyber security management in the early stages as well as poorly understood (Stevens 2012a). Contrary to traditional security studies scholarship it should be pointed out that this shared expert

[7] Analyzed in depth in chapter 3 especially 3.5
[8] Watershed in epistemic communities related research was the special issue of International Organization in 1992 acknowledging the need for reflective IR theory summarized by Adler, Haas (1992).

understanding as means of conceptualizing reality and often working on policy related issues becomes amalgamated with reality. Or in other words there is no clear delineation of subject and object of security as these both form part of socially intersubjectively produced reality (Mutimer 2007).

Additionally, cooperation in matters of security and defence has been lagging behind integration in other areas, partly because it borders on the cornerstone principle of state sovereignty that is invariably tied with territorial defence. It is a plausible explanation that recent advances, albeit cautious, are partly due to the ideational amalgamation, common experiences and growing like-mindedness (Cross 2013).

1.2.1. Framework

The core aspects of the theoretical approach used to capture *threat framing* that will be used in the main part of this thesis include[9]:

- The framing actor (the EU as represented by institutions, official documents and individuals)
- Type of referent object (network, human rights, critical infrastructure, use of military force, economic prosperity)
- Target audience (successful framing will take into account type of audience)
- Frame characteristics (elaborated/dynamic - subject to change and contested)

The goal of the analysis is to uncover how information technology related threats gain political and security salience as well as to shed some light onto the motives and tactics used to influence this process. It is rather problematic to seek to analyse hidden agenda – issues and documents that might be protected under national security means or kept out of sight to achieve bargaining advantage. It is not reasonable for this thesis to try to uncover these and the main focus will be on official documents, speeches, laws and secondary literature dealing with relevant

[9] The following section draws mostly on (Eriksson 2001b) and (Buzan, Wæver, Wilde 1998)

material. Some insight can be gained from analysing and contrasting official material and independent media sources as will be shown later. The type of object that is being secured and changes of reference dynamic in time will reveal transformation of threat image politics as well as changes in the overall narrative. In line with the Copenhagen School's approach the analysis will argue that deployment of *Schmittian* "us" vs. "them" discourse makes for a very potent securitizing mix and thus the construction of cyber "us" and cyber "them" are categories that should be intuitively present.

Frame is to be understood as the inter-related aspects of conceptualizing the issue, determining what is at stake and who is responsible and eventually suggesting means to deal with perceived threat (Snow, Benford 1992). Cavelty (2008b) uses threat-frame analysis on the case of US discourse on cyberterrorism and arrives at a conclusion that even though catastrophic cyber related scenarios have failed to materialize, the discourse has successfully stressed this type of threat as one of the most salient and significant resources have been spent to mitigate it. Eriksson (2001b) argues that it was the permissive post-Cold war policy window that has helped to bolster the military-cyber link that was there from the beginning.

Figure 1 illustrates logic of used threat framing model. Cognition and constitution of threat takes place within intersubjective frame, which is influenced by various exogenous pressures as well as utilization of particular historical experience and activation of common pool of identity. Typically, frames diagnose, evaluate and prescribe (Entman 1993, pp.51-52). This process then translates into strategies that are trying to present constructed frame or highlighted aspects of a phenomenon and have effects on (security) agenda. Importantly, strategies of securitization are functional only if target audience accepts the narrative as such (Buzan, Wæver, Wilde 1998, pp. 24-26). Because social relations are not linear in the sense of cause and effect, the intersubjective manner of how securitized agenda shapes cognition of threat needs to be taken into consideration as represented by the feedback arrow.

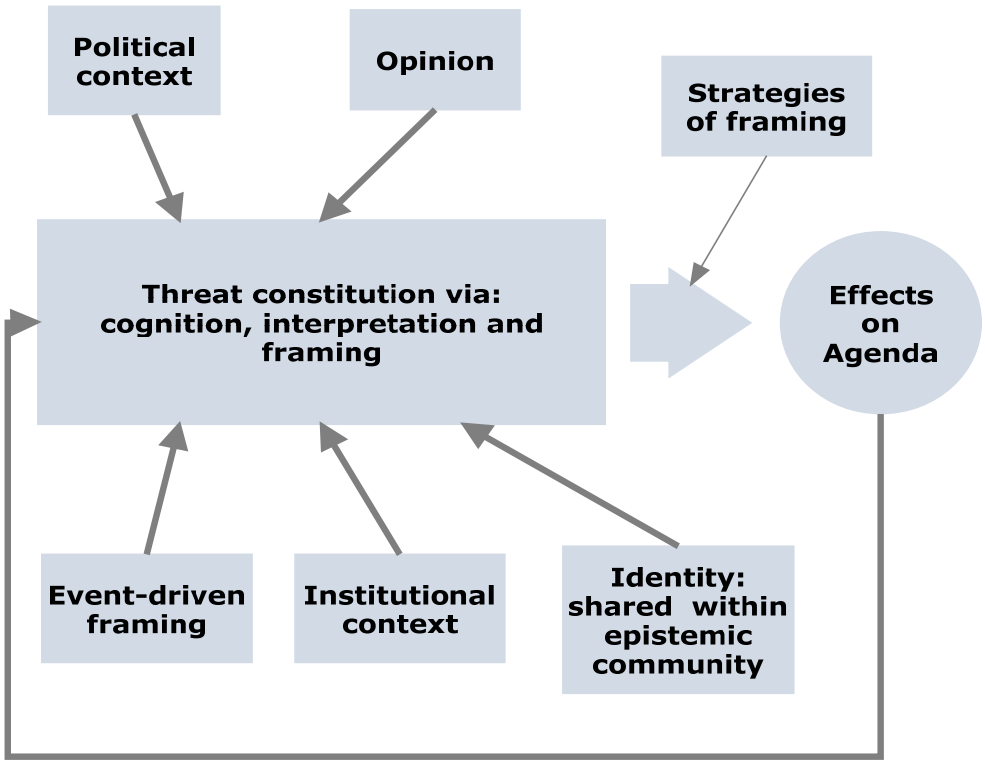

FIGURE 2 BASED ON (ERIKSSON, NOREEN 2002, P. 19)

In terms of frame functions (Snow, Benford 1988) discern three types:

- Diagnostic – defining a problem, specifying who is threatened (referent object) and who is to blame
- Prognostic – proposing how to deal with the threat, how can objectives be achieved
- Motivational – serving to mobilize realization of threat and rally for support.

Successful framing reaches all three categories, yet the diagnostic quality is the bare minimum where one can recognize the particular lens through which the framing actor perceives reality. Additionally, *frame resonance* is a quality that describes how likely a frame will succeed depending on the perceptiveness of audience, policy window and appeal to identities – similarly to the facilitating conditions of speech acts (Buzan, Wæver, Wilde 1998, p.17). There are two facets of frames that are of interest for analysis of the given topic[10]. First treats frames as products of a particular securitizing or norm-creating endeavour, thus one can perceive framing as dependent variable.

[10] Distinction well explained in (Cavelty 2008a, pp. 31-33)

Second one looks at the effects that frames have on behaviour of actors treating them as phenomena with their own substance influencing behaviour of actors. Logically, the first understanding precedes the second as frames first have to be established, yet the first constitutive period also departs from a particular historical and sociological experience, i.e. there is ever evolving struggle for frame dominance with successful frames achieving hegemony.

One of the goals of this thesis is to look at whether framing of cyber threat by the institutions of the EU has taken place and in which form as well as whether it reached all three categories of framing. As the threat framing approach borders on discursive analysis occurrences of cyber security related keyword complexes to allow for contextual content analysis of texts and utterances. Although this method has its limitations in terms of deliberately limiting scope of research to written text and thus possibly omitting e.g. visual securitizations (Hansen 2011) or actors who are for various reasons unable to "speak" (Hansen 2000) it still serves the purpose of comparability and scientific integrity. Furthermore, context plays a key role in the language of security, both the proximate "setting" and the "distal" context pointing toward sociocultural embeddedness (Balzacq 2010, pp. 36-38). Key cyber securitizing keywords that will be analysed and contextualized include:

- Cyber
- Cyber-security
- Cyber-attack
- Internet
- Network
- Information and Communication Technologies
- Critical (Information) Infrastructure Protection

To sum up the methodological approach used Figure 2 will help explain its main important points. The over-arching perspective departs from constructivist securitization logic. It is no coincidence that this type of research suits well to the inherently European theoretical approach, that builds on ideational and identity factors (Huysmans 1998).

Theoretical and Methodological overview

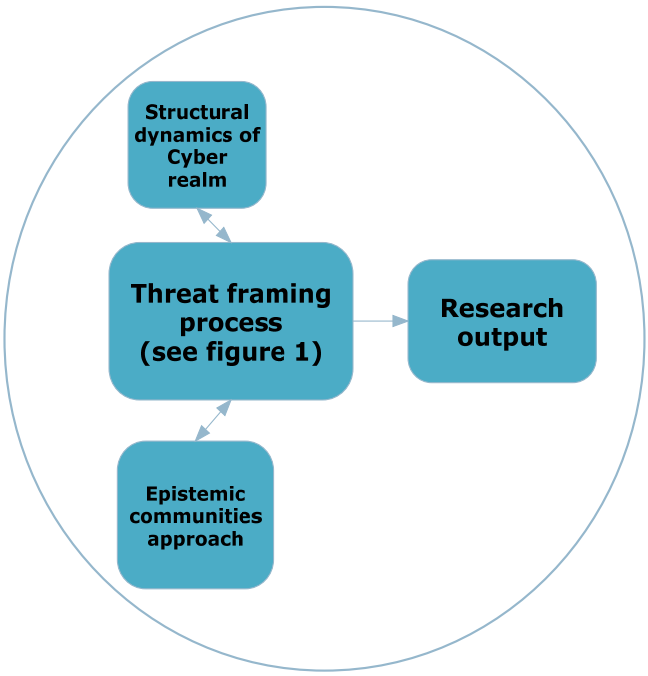

FIGURE 3

As a precursor to the framing analysis itself thorough yet useful chapters 2 and 3 will provide insights into the specific dynamics of the cyber sector. That is the strong epistemic expert community surrounding the world of IP-based communications from its inceptions and the complexity surrounding any large network. It will be argued that the embedded values within the epistemic communities surrounding esp. the global Internet are obstacle to strategic threat framing. Moreover, it will be shown that the nature of the cyber environment in itself explains what can be termed non-cases: lack of incidents fulfilling scenarios of cyber harm. These expansions on the threat framing model as specified earlier will allow for thicker analysis and more critical insight. Here an explanation of the epistemic community term is due. In Figure 1 it related to the

framing actor and its identity/culture in Figure 2 it relates to what is sometimes termed "ethos"[11] of the internet.

1.2.2. Research Questions

There is a set of interrelated research questions that this thesis aims to answer. The central puzzle can be spelled out as: ***How are cyber threats framed as security issues within the scope of the EU?*** Additionally, first part of this thesis will seek an answer to ***what are the specific dynamics of the cyber sector and how does this structurally constrain and shape what is possible.***

Turning back to figure 1 one can understand the inputs into the main threat framing process as variables seeking to explain the outcome of the process. These need not be exclusively competing, the chosen framework will allow for uncovering of co-constitution, avoiding the perilous causal relations paradigm which borders on the impossible in social sciences in general[12]. The strategies used to influence agenda should correspond to the type of referent object and audience and be part of the overall framing rationale. Effects on agenda can manifest in various ways. Apart from the more obvious agenda-setting they can also be agenda-removal or agenda-restructuring (Eriksson, Noreen 2002). Threats that already feature on the security agenda in some extent can be obstructed, re-prioritised as well as reinterpreted.

[11] As elaborated in section 2.2

[12] This is not to contradict the recognition that theory is always *for someone and for some purpose and grounded in time and space* (Cox 1981). Moreover, it seems plausible to the author of the thesis that preoccupation of International Relations theory with positivist methods giving the impression of scientific discourse is part of a larger discourse commonly termed enlightenment as to what can be considered scientific and what is not – a normalization of ideas(Foucault 1994).

2. Cyber security

Today we understand networked interfaces to be part of our everyday lives and the global network of networks arguably continues to be one of the great "flatteners"[13] that has propelled forward a whole range of developments usually termed collectively as globalization. As with other cases of innovative technology its journey was difficult, fraught with delays and blind alleyways. It should be of interest that the network which was conceived under the ARPA[14] project - more or less part of the direct response to the perceived technological gap in the Cold war confrontation – has turned into a private enterprise and zeitgeist technology with a distinct "neutrality" global common goods flavour. Yet again the hard-to-capture cyber realm is securitized and militarized within strategic discourse. This can be understood within the shift to widen security – manifested in amalgamation of the public and private since there can hardly be any distinction within the cyber sector. Additionally, it can be interpreted as a sign of *maturity* of the ICT realm in the sense that it has grown in importance and salience so as to make it a top-level security agenda (Der Derian 2003).

In the following section some fundamental concepts will be discussed which will lay the foundation for subsequent threat framing analysis. This is key since the technical foundations of the cyber realm are commonly understood as being out of reach because of their complexity. This *technification* can in fact be one of the tactics of securitization that serves to elevate cyber issues out of the sphere of non-politicized discussion (Hansen, Nissenbaum 2009). Moreover, it is paramount that current setup of the global network is a consequence of a particular historical process of establishment. Another important point elaborated in this section is that technology does not carry with it some internal inherent logic – this is always done through social interpretation and construction of meanings. In another words the common

[13] As argued by (Friedman 2006) as part of explanation of the changes that took place since the birth of the Internet proper. Useful analysis, even though it oozes technological determinism and does not give enough space to political factors and critique of the essentialist approach.
[14] Advanced Research Project Agency, later renamed to Defence Advanced Research Project Agency. Founded in 1958 it was one of the responses to the perception that the US is falling behind in the East West due to the "Sputnik effect"(Ryan 2010).

perception of the global network being liberal might be the case as of now, but certainly not taken for granted or susceptible to change in the future.

2.1. Nature and history of the cyber environment

The origins of networking as we know it now has its roots in the early 1960s. Several bright minds in the US army-funded ARPA have developed a network that came to be known as ARPAnet, military funded yet civilian expertise fuelled achievement. Young researcher Leonard Kleinrock presented his PhD thesis at MIT titled *Message delay in communication nets with storage*, that discussed the possibilities of packet switching network and the mathematical model needed to support it (Kleinrock 1962). It was also in the 1960s in the USA that a landmark Air Force defense and intercept system SAGE[15] became fully operational. It featured several completely novel technologies, among other the ability to interact with computer directly with use of a light-gun and providing operators with real-time information from several types of input sensors and in turn provided guidance to missiles and/or planes assigned to intercept a threat (IBM 1958). Networking took off as response to the need of decentralized command and control system in the grim outlook of Cold war confrontation, especially as discussed by Baran (1960). This visionary researcher working for RAND proposed that it is possible to build highly distributed non-hierarchical digital network that could withstand a high degree of link destruction (read thermonuclear warfare) provided that at least one link path remains intact (Baran 1960, p.15). Centralized command and control points, such as the hub-and-spoke nature of the ATT telephone network were rightfully seen as Achilles heels of the MAD deterrence logic. Thus the centrifugal nature of the computer network of networks is in part explained by its original use – to provide reliable command and control in Cold war escalation ladder to ensure second strike capability as discussed by strategists such as Herman Kahn (2007, first published 1960).

[15] Semi Automatic Ground Environment

Taken together one can see a picture of man – computer relationship (term popularized by visionary J.C.R. Licklider)[16] coming together within a military establishment and being enabled by some key advancements in the technological sphere. It was only later that the decentralization effects of networking were propelled forward by the introduction of universal communication protocol. The universality of the TCP/IP[17] suite which lies at the heart of the modern global network won over other formats, particularly AT&T-backed x.25 because it was so well-suited for whole spectrum of connections – computer to computer and network to network or computer to network (Ryan 2010, pp.43-44). Paradoxically, it was the US army that made TCP/IP it's preferred and only communication standard in the 1980s before internet proper took off in the early 1990s as a very open platform. This establishment of the open protocol that was made available to all in the 1990s with the goal of promoting global connectivity will be discussed more in depth in the following section since it is one of the most defining structures of the web.

2.1.1. *TCP/IP protocols – the language of the internet*[18]

Enabling pooling and sharing with non-discriminatory approach was the goal of evolving network. The distinction between monopolized telecommunications networks and *value-added* information data services conducted through the implementation of TCP/IP was diffused through the developed world and beyond within the spirit of neoliberal economic paradigm (Mueller 2010, pp. 55-57) The first were protected by patents and monopolies as well as constrained by the physical boundaries of nation-states through these contracts. The latter were appearing on the fringes of these monopolies, often on a voluntary, amateur or academic basis and by the key notion of global connectivity surpassed the control of national jurisdiction – although the USA agreed to truly set the regulating agency free starting in 2015 (Menn 2014). This language of the internet and coordination of how packets of data are switched has

[16] (Kita 2003)
[17] Transmission Control Protocol/Internet Protocol or the language of the global network initially pushed through as a standard for military computer communication it later spread to become the only truly universal protocol – civilian, industrial and military.
[18] This section utilizes some of the arguments and thoughts presented in paper for JPM611 Cybersecurity in International Relations lectured by Mgr. Nikola Schmidt in 2014 and published on POST - (Rozsypal 2014)

some serious security implications. Among the most prominent is the anonymous nature of the cyber environment. If an attacker is careful and covers his tracks the problem of attribution arises. The difficulties of attributing activities to users is possibly the most complicating factor in cyber defence[19] – if one cannot pinpoint the threat or from whom it emanates it is difficult to counter it meaningfully. Before delving deeper into what strategic implications of this and other cyber specificities are in subsequent chapters it is useful to look at how IPv4 addressing works and whether its envisioned alternative IPv6 presents a qualitative change or not.

While in its original conception it seemed hardly imaginable, the 32bit long address space of IPv4 that became the standard has roughly 4,3bn unique addresses – a limitation that currently poses significant problem. Final batch of IP addresses was allocated by the root domain administrator already 3 years ago (ICANN 2011). While the current state of connectivity is far from every person owning a device with network interface, recent developments such as the 3/4G mobile broadband network can consume more than a billion of IP addresses (IEEE-USA 2009). One notable factor of IPv4 is its underutilization. The actual utilization is measured with a lot of variation but it is quite obvious that especially early IPv4 requests were treated with light-minded approach and thus up to 70pct of allocated addresses in the US are unused (Early 2009). This is partly due to the initial system of allocation of IPv4s. The network IP allocation was classful from 1981 till 1993 and addresses were given out in portions know as classes A to D ranging in number of addresses available. For example a class B assignment would have the network portion of the IP 16bit long, thus allowing the other 16bits to be used for unique IP addresses – corresponding to 216 or 65 536 addresses. Companies or institutions would be allocated these batches even though in reality they might only need several thousand addresses (Russell 2004). This was partially addressed by the introduction of Classless Inter-Domain Routing (CIDR) in which IP allocation could be scaled more freely as a power of 2.

IP allocation however, remained essentially free even though the problem of lack of addressing space has been discussed for a substantial amount of time. The Internet

[19] As argued for example in (Geers 2011) or (Libicki 2009)

Engineering Task Force published call for white papers regarding “next generation” IP addressing in 1993 (Mankin, Bradner 1993), long before lack of IP addressing was real day-to-day problem. In the meantime several IPv4 conservation policies and technologies were adopted – which had adverse effects on attribution as well as security. Network Address Translation (NAT) is currently employed on a mass scale shielding subnetworks behind a router with single public IP. While it performs the task of prolonging the feasibility of v4 internet it does place constraints on what is possible, notably direct Peer2Peer connections and effective implementation of security features into layer 3 (IP) protocol. The inability of devices to connect directly to each other does require more work from servers to facilitate the routing. A feature that has been built into the new generation internet as embodied in IPv6 called Stateless Auto Configuration[20] enables devices to connect to a network even without the help of a server upholding the e2e principle. This plug-and-play feature can be cost-effective as well as socially enhancing by lowering the barriers to successful connection i.e. working toward narrowing the digital divide (European Commission 2013b, p.15).

Possibly more importantly, the IPSec protocol, a simple cryptographic method using hashes to determine whether data has been tampered with is not functional under NAT due to the middle step of subnetworking. Assigning IP addresses dynamically in time is also a method that is currently employed to make use with less unique IPv4s. However it puts additional strain on network routing hardware as well as complicating the desired end 2 end communication since addresses are not permanently fixed to a particular network interface. It is estimated that there can be currently up to 3 BN connected devices, even though unique IP utilization itself is around 40 % (2 BN) which shows that underutilization was mitigated by substantial amount (Huston 2013).

[20] Under this provision network devices can acquire new IP addresses on their own, without requiring work of DHCP server. A set of protocols ensures that devices ping the rest of the network they connected to making sure desired IP is not used by another user. While this in theory simplifies the connection process and puts all users on equal footing upholding the liberal character of the network a new type of threat such as rogue server redirecting traffic and taking user to a different subnet through the initial ping communication (Barker 2013). Full Specification of SLAC put forth in (Narten, Thomson, Jinmei 2007).

IPv6 was designed to address the shortcomings of v4 discussed above with the provision of almost infinite address space of 128bits[21]. Consequently future expansion of the global network would be unhindered by scarcity of addresses. However, exhibiting traces of tragedy of the commons the adoption of the new standard has been slow. The official launch of IPv6 was the IPv6 day in 2011, with public and private encouragement with the EU being a stark supporter (ENISA 2011). Figure 2 graphs data of accesses to Google servers through IPv6 – a clear trend of acceleration albeit on a small scale.

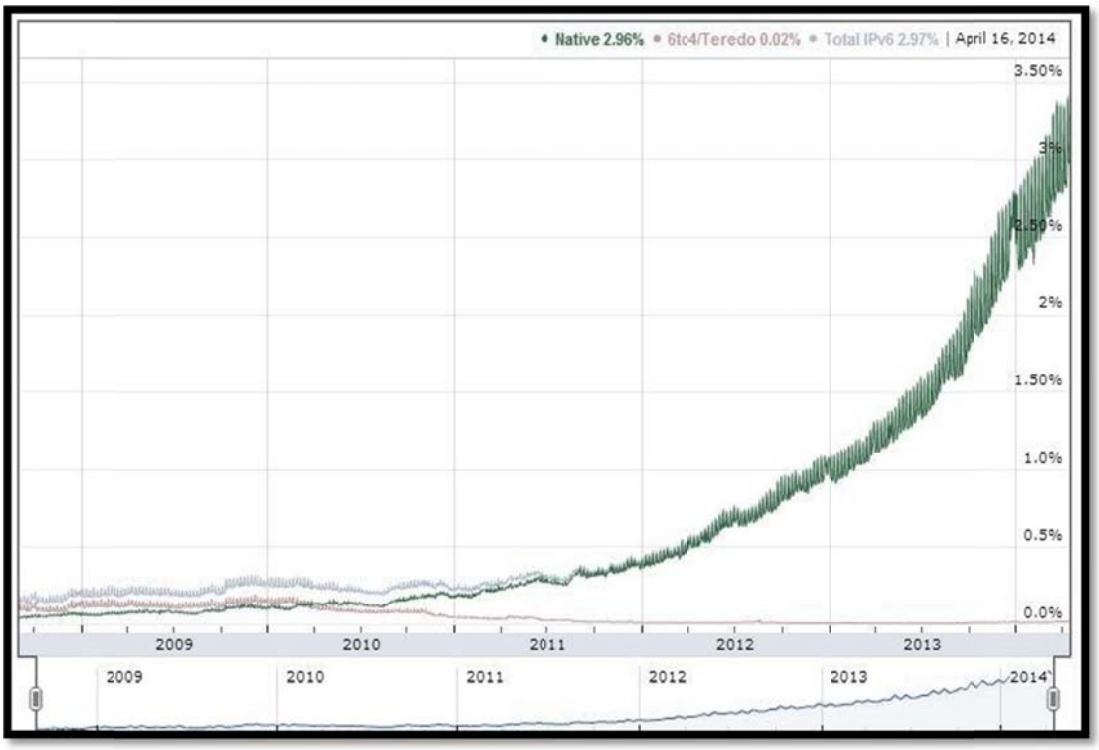

FIGURE 4 SOURCE (GOOGLE 2014A)

Upgrading through IPv6 means there will be no more need for NAT, DHCP making the network more efficient in terms of connectivity related costs yet at the same time at least theoretically enhance attribution. While it might hold for the common user should one imagine that future network devices would have their unique IP built into their interfaces by default it is dubious this would hold for the more advanced cyber hostilities. Anonymization methods such as onion routing or the usage of botnets will continue to be a problem under IPv6 infrastructure as well. Onion uses randomizing

[21] Within this space combinations giving unique IPs equal 3.4×10^{38}

methods to hide identity of users by displaying a different IP address – usually impossible to trace due to the technology of bouncing the route through a number of routers that work anonymously. The most well-known network that employs this method is Tor, former US Navy project to provide highly private communication (Syverson, Tsudik, Reed, Landwehr 2001). This is a fitting example showing that tools and weapons in cyberspace are coming close to being perfect double-edged swords. Botnets on the other hand are computers linked together by malicious software without the knowledge of owners and under command and control of attacker's software. Moreover, these infrastructures can have decentralized hierarchy of command and control as well as employing algorithms to shuffle their servers IP addresses making them resilient to takedown attempts(Graham, Olson, Howard 2011).

IPv6 should be understood as almost necessary upgrade that should enable further organic growth of the network. One should be cautious about frames that present IPv6 as a silver bullet solution to the attribution problem to justify a more robust control mechanism that might be lacking current emancipatory values. There is a distinct dynamic of technification as discussed in the introduction to this section which must be assessed critically. The next section will look more in depth into some of the structural effects of discussed technology and whether there are any inherent values embedded in the cyber realm and critique the black-box-like treatment of the technical aspect of ICT.

2.2. Ethos of the internet – structural or contingent factor?

Decentralization, universality, liberal values and emancipation are part of what is sometimes termed the ethos of the internet. In the words of one of the co-designers of the universal connectivity suite "the internet is for everyone" and we must keep "the network unrestricted, unfettered and unregulated" (Cerf 1999, p. 2). While this perceived ethos is certainly not uniform in the sense of a tangible definition, the nexus of the technology in use in modern day networking with origins of public internet in

the academic sphere that traditionally upholds liberal values forms a discursive (cyber) space (Mitra, Watts 2002). The principle of end to end communication (e2e) is one of the cornerstones of the open network architecture. While it is connected to TCP/IP suite for technical reasons it has also economic and social benefits. This non-discriminatory principle of allowing connectivity to virtually anyone who would conform to the network standard is a strong point for the advocates of internet neutrality. The principle of treating all traffic equally (neutrality) and protect the network from commercial pressures had notable positive impacts on facilitating and accelerating growth. ISPs were made to serve as gateways not gatekeepers to connect various sectors of the network(Ammori 2014). Decisions taken in the 1990s by the USA and others following suit to deliberately keep the state *out* of cyberspace controls have solidified this partly technical network design (Deibert, Crete-Nishihata 2012). The maintenance of WHOIS list[22] is one of the most notable powers of the network administrators, essentially a record indicating which IPs belong to which company. The North American RIR[23] ARIN has threatened to not update this list if transactions of IPs take place outside of its framework – basically upholding the "based on needs principle" (Mueller, Kuerbis, Asghari 2013). This can be interpreted as the upholding of the normative principle of neutrality of the network environment by the semi-independent regulators. Yet within the aforementioned problem of IPv4 space depletion it is rather obvious that it is obsolete in the sense of connectivity (number of possible connected devices) and suffers from regional bias – early IP allocations were done in a non-effective fashion mostly to US network users. Thus IP underutilization is highest in North America with up to 70% of assigned addresses being unused (Early 2009).

The quasi-ruler of the internet ICANN[24] was founded in 1998 on American soil yet it had the public benefit imperative imbued in its articles. This non-profit organization should be operating for "the profit of the Internet community as a whole"(ICANN 1998). Thus an organization that should take care of the network architecture is

[22] For example a top-level domain lookup as provided by (ICANN 2014)
[23] Regional Internet Registry – organization reallocating IP numbers from the top level administrator within 5 world regions: ARIN for North America, APNIC for Asia, Australia and New Zealand, LACNIC for South America, RIPE for Europe, Middle East and Central Asia, AfriNIC for Africa.
[24] Internet Corporation for Assigned Names and Numbers

operating within US jurisdiction -or more precisely the State of California – should take care of all users without discrimination. From today's point of view it is rather incredible that prior to ICANN founding IANA[25] was taking care of the DNS organization – effectively one bearded researcher by the name of Jon Postel working from his lab in Southern California who was the "tsar" deciding who was assigned which address within the network (Cerf 1998). This underscores the contingent and bottom-up character of the internet phenomenon. ICANN is responsible for the top level root domain of the DNS and global IP coordination on the level of generic and country code top-level domains (Weitzenboeck 2014).

The hierarchy of Internet governance is depicted in Figure 4. The last step to making ICANN perform its assigned numbers responsibility independently is that as of 2015 it will not be dependent upon the contract from US Department of Commerce and will thus become nominally independent non-profit organization (Rosenzweig 2014). The authority of ICANN and the subsequent RIRs is based on customary or organic relations – efforts to take Internet under the auspices of ITU within the UN framework have failed, notably after the Dubai 2012 World Conference on International Telecommunications[26] or the World Summit of Information Society[27] in 2003 and 2005 respectively. The logic of the predominantly Western stakeholders being that the web should not be tainted by the intergovernmental authority of the UN department and that centralization of oversight is in fact not desirable (European Parliament 2012). However, it is one of the crucial points of the EU cyber governance policy to *establish a clear timeline for the globalisation of ICANN, including its Affirmation of Commitments* and advance internet governance through *sound multistakeholder process* (European Commission 2014). Yet the voice coming from the UN-backed ITU states that *Internet-related public policy issues is the sovereign right of States*[28]*,* a narrative that has spurred global movement[29] to keep internet to a large

[25] Internet Assigned Numbers Authority
[26] (ITU 2014a)
[27] (ITU 2014b)
[28] (ITU 2003)
[29] One the most important being Google's *Take action* to protest against perceived push to bring internet governance under control of governments in the course of the Dubai WCIT with several million supporters backing internet as the ultimate tool of free expression (Google 2014b).

degree out of reach of governmental UN framework. Efforts to regulate cyber offensive weapons in the 1990s modelled after the Chemical weapons convention were blocked by the US, partly due to the perception that it would be strategically unwise to put a limit on cyber capabilities that at the time appeared as superior (Arquilla 2011). With waning US hegemony this process is under incentive to be renewed – and indeed current efforts to link cyber to Laws of Armed conflict and Humanitarian Law support this argument[30].

It is a fair assumption that if IPv6 is successfully introduced giving ISPs and other network facilitators rather detailed knowledge of the identity of users and states manage to grasp tighter control through framing via sovereignty it is a potent mix for censorship. This is of particular importance since the use of information outlets has been the *anchoring tool of state power* (Castells 2007, p. 316). Moreover the current push for *multistakeholder participation*[31] with emphasis on consensus typical for non-hierarchical forms of organization may take its toll on day-to-day effectiveness of network facilitation.

[30] Especially Tallinn manual, but also numerous national cyber security strategies. See also discussion under section 2.3.1
[31] (NET Mundial 2014)

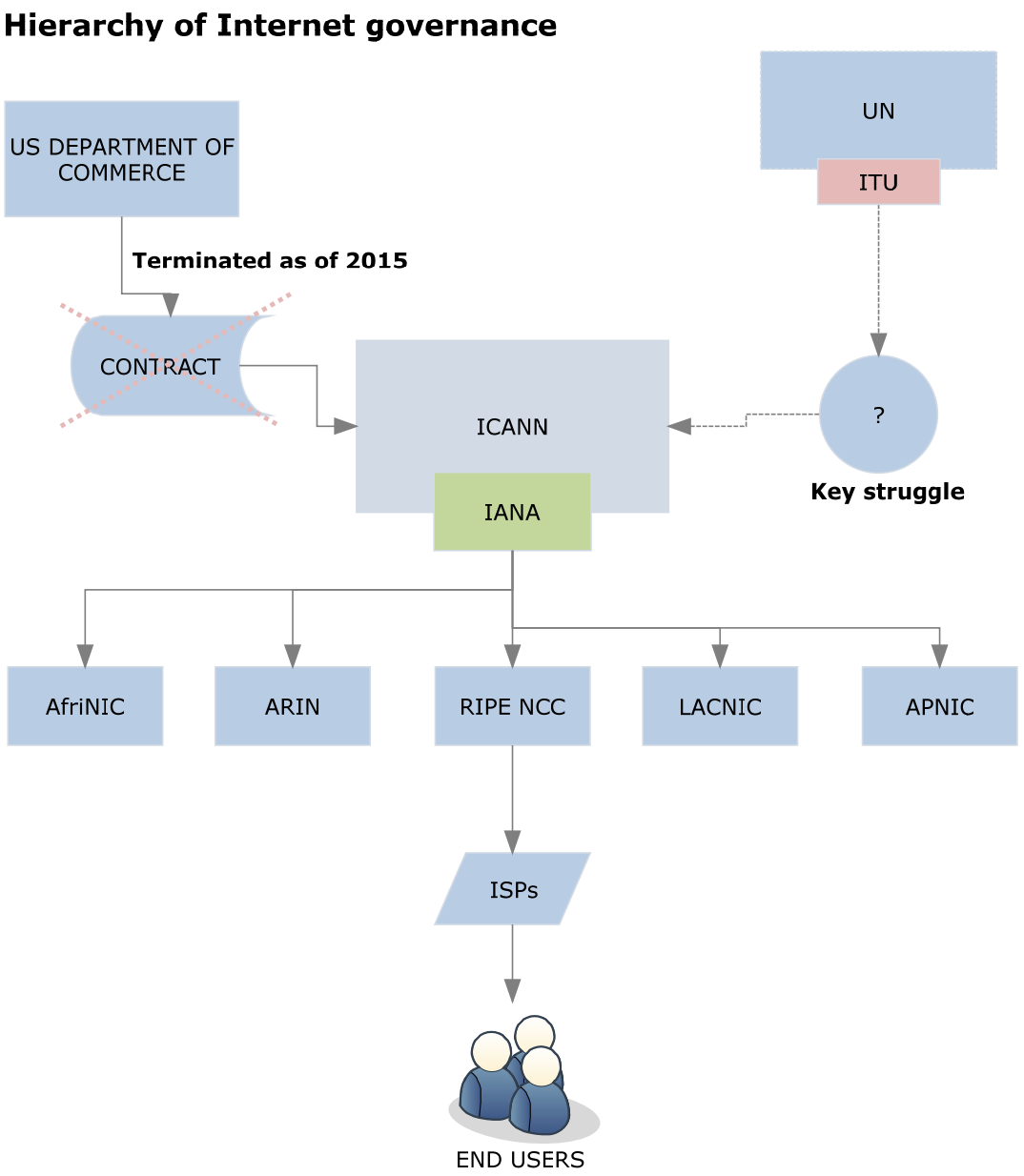

FIGURE 5 SOURCES: (HUSTON 2005)(ARIN 2014)

The degree to which the original "internet society" type internet has changed or is currently changing as a result of contending narratives will be touched upon in latter part of this thesis, however it is not its primary focus. To stay within the *threat framing* mind-set it is reasonable to note that contending narratives are struggling and fusing within the cyber realm. As part of this process technical needs of the platform are increasingly determined by politicians instead of experts and thus politicized and framed within larger narrative (Der Derian 2003). The nature of the internet as global

commons, however, clashes with this need for political control pressure that implies fitting the interconnected network into rationalities of colourful polities – many of which are not entirely compatible to say the least.

Figure 4 shows some of the conceptions of cyberspace and their nature. Securitization and degree of internet governance were chosen to show that militarization/securitization and introduction of formalized or centralized governance need not to appear hand in hand. One of the directions pushing for more control and represented to a large extent by the ITU views the network as infrastructure that the state should take care of as well as define traffic laws. This is sometimes amalgamated with "connectivity as human right" discourse that argues additionally states need to provide connectivity as a common good and facilitator of human rights (Lucchi 2011).

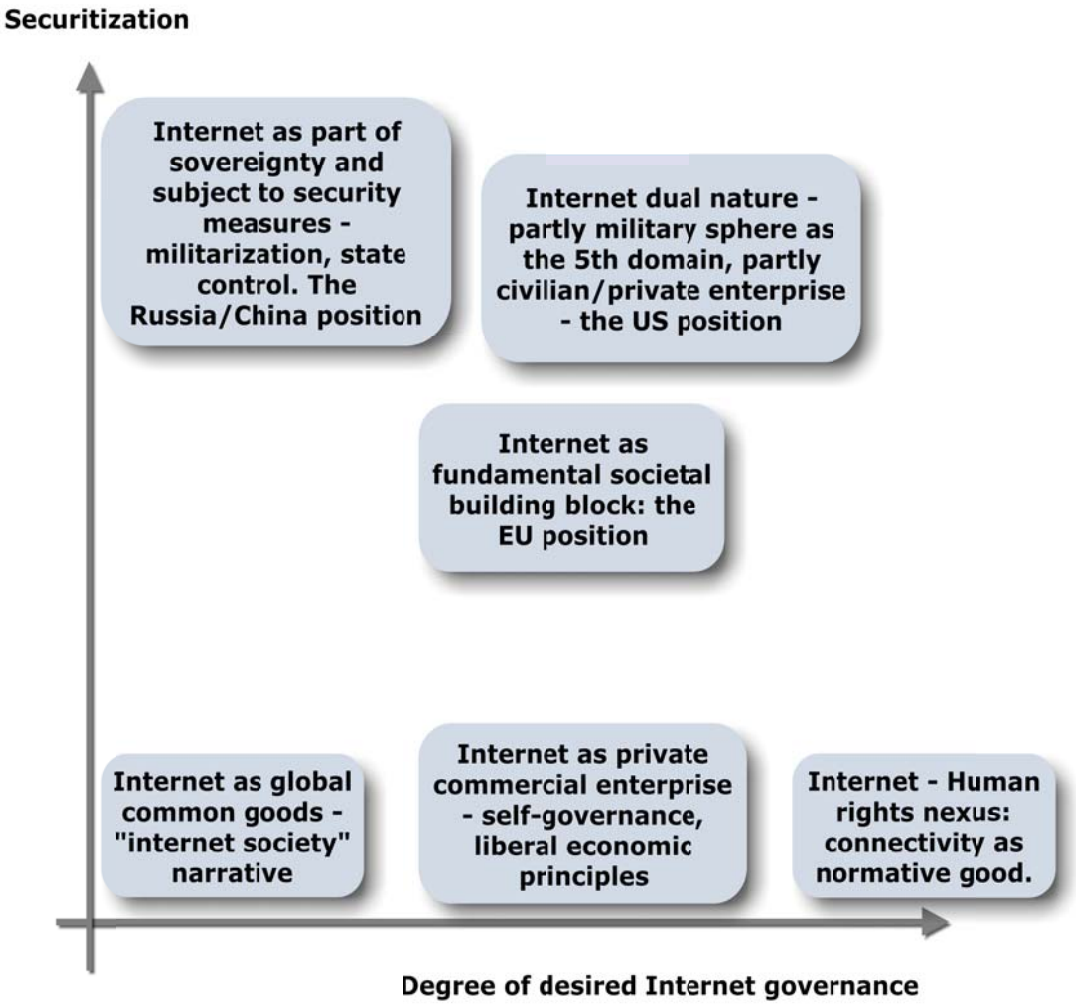

FIGURE 6

The ambiguity and specific semi-organic form of governance of the internet is one of its defining features, it can be used as a vehicle for various ends ranging from democratic participation and propagation of human-rights related values to tools of powerful oppression and control (Potzsch 2013). Deibert & Crete-Nishihata (2012) have conceptualized the process of emergence of pressures to introduce more state control into cyberspace as a form of norm regression – in the sense of reinstituting early 1990s notion of cyberspace as global commons into state-based cyber governance. The narratives/aggregate positions in Figure 4 are presented here for simplification purposes and to further the framing argument. While it is the position of this research that there is a status quo best represented by the "internet society" cluster that is under pressure from both governance (esp. ITU/UN) and militarization/securitization clusters (Cyber powers: esp. China, Russia, Israel, USA). With European Union being in between these pressures i.e. balancing security considerations with network impacts of the society as a whole it will be dissected in a more precise manner.

To continue within the tenets of ideal-types the debate oscillates between cyber-libertarians and cyber-conservatives[32]. The first camp argues that the Internet has its emancipatory and liberalizing logic imbued within the technological architecture and suffers from technological determinism that is commonly to the weakening of nation state. Castells (2010) argues in his prominent work *The Rise of the Network Society* that technology indeed drives social change and that the global network is transforming the now obsolete system of sovereign nation-states that will return to tribal configuration held together by cyber relations irrespective of territorial dimension. While this insight is valuable in showing that there are changes in narratives and that structures of the social order are subject to change it tends to discount the durability of ideas and overemphasizes the role of the technology as having its own logic that drives change in certain direction. This approach tends to proclaim that information technology has brought a qualitative paradigmatic shift as for example Bard and Söderqvist (2002) argue in their neo-Marxist analysis of Netocracy – the new power elite. Within this

[32] Terms as used by (Mueller 2010, pp. 2-11)

view ownership of information is more important than ownership of capital and information hubs are the real wielders of power.

Yet again these assumptions are technologically driven and fail to capture the richness of what social reality is. It is true that ICT are putting pressure on the nation state in various ways. Borderless communication through universal protocols is the norm, participation and control is distributed through the decentralization running counter to the traditional nation-state logic of centralization. Additionally, it facilitated the growth of new institutions: most notably ICANN as mentioned above or IETF[33] representing native institutions that do not have a clear cut relationship with the traditional playground of sovereign nation-states(Mueller 2010). Arguing from the perspective of intersubjectivity, it is dubious that any technology possesses inherently ethos or logic that will invariably reveal itself. Similarly to the construction of the nuclear taboo and the less obvious chemical weapons taboo[34] the technological basis and its conceptual use is far from given or self-evident in the case of the emergence of the global network. Neither it is true as cyber-conservatives argue that the traditional categories such as nation-state inextricably linked to sovereignty trump whatever pressures global connectivity has brought and that cyber will be incorporated into regulation and armies as a new domain or weapon. This approach focuses traditionally on problem-solving and does pay much attention to underlying assumptions that can render the whole analysis outcome void. Hence it is necessary to look into how are threats within cyberspace constituted and how do these fit into more general framework of the concerned actors.

[33] Internet Engineering Task Force – run by the Internet Society and implementing technical protocols based on consensus on voluntary basis (IETF 2014).
[34] As argued forcefully by e.g. (Price, Tannenwald 1996) and more in depth dissection of the nuclear weapons taboo (Tannenwald 2008).

2.3. Threats in cyberspace

Debate on what are the threats in the virtual space and who is threatened (the referent object) is rather lively. Does war imply lethality? Can we apply traditional use of force criteria on the cyber sector? Thomas Rid (2012) argues that all hostile cyber activities to date do not classify as war and that supposing anything coming close to cyber war proper is not in the making – in fact that these acts are merely intelligence and espionage through novel technology part of state behaviour for a substantial amount of time. Yet John Stone (2013) replies to this article published in the influential Journal of Strategic studies that what is falling behind is our understanding of kinetic warfare and that cyber hostilities could in fact classify as acts of war – if one accepts that violence and force need not imply lethality.

Moreover, with increasing intertwining of military domain and cyber means the risk of escalation and miscommunication runs high without clarification. John Arquilla has since the 1990s toned down his rhetoric and in a more recent work argues that cyber warfare and traditional modes of conflict should be separated (Arquilla 2011). In the cyber realm adjectives such as alleged or possible are inconveniently frequent. Especially if one combines this with the conceptual problems that social scientific analysis presents by itself it makes for a potent mix of interpretations and manipulations. Thus the struggle for the definition of threat and its features which is part of any securitization is perhaps more pervasive in the cyber sector. For example putting together cyber threat together with terrorism is a potent mix in the post 911 security environment and thus commonly used in the political debate about possible future threats and how to best prepare for it (Cavelty 2008b, pp. 21-22).

Figure 5 illustrates the landscape of threats in cyberspace, which will be dealt with in turn. The mantra of non-attribution, asymmetry, and amalgamation of the private and state activities holds here as well and thus these should only be understood as analytical categories that in the real world are overlapping in various ways.

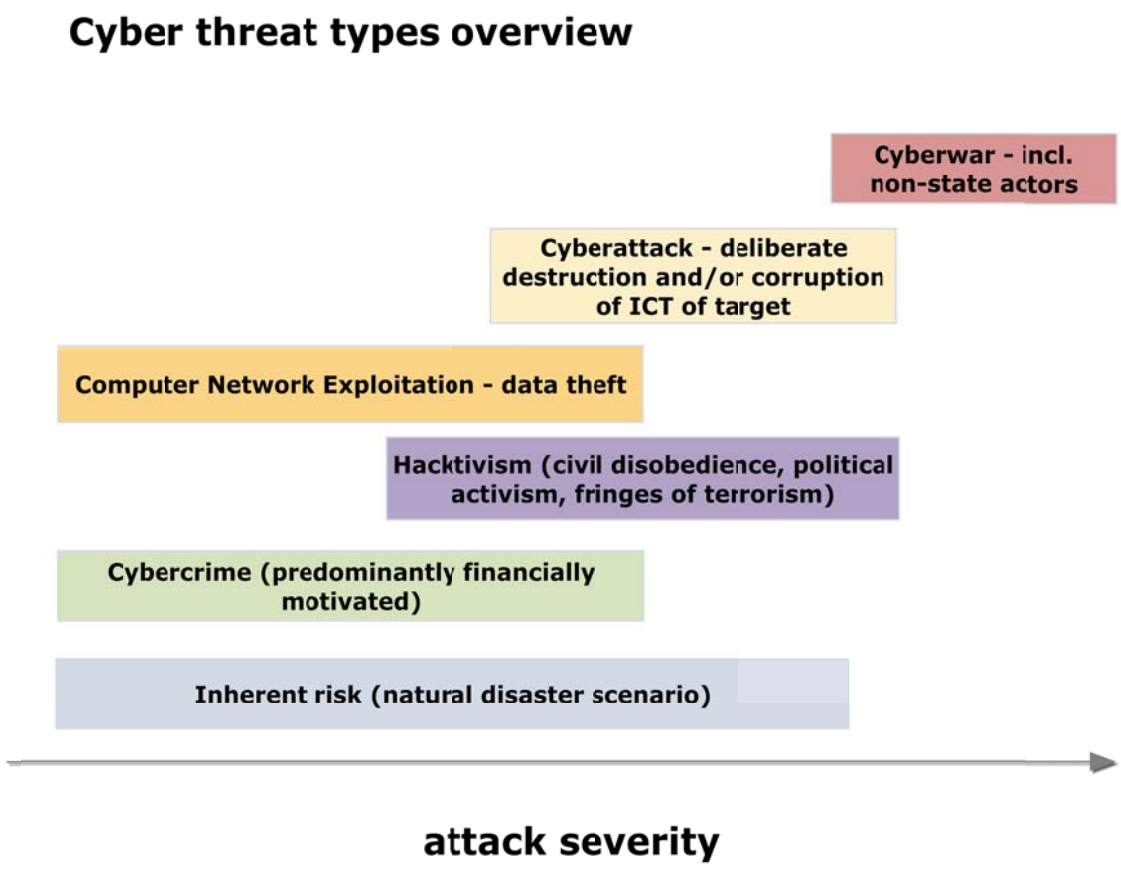

FIGURE 7 UTILIZES TERMS AND ARGUMENTS FROM (HANSEN, NISSENBAUM 2009; LIBICKI 2009; GEERS 2011)

Inherent risk stands for risks that are not deliberate attacks. As with any other infrastructure, networks need infrastructure such as servers and optical fibres connecting them to work. Apart from physical destruction due to natural causes, which is a topic on the fringes of cyber security related literature it can also be disruption due to faulty programming. This type of inherent risk is present especially because of the complexity of ICT – the famous Y2K bug that mostly failed to materialize comes to mind. Protecting infrastructure from both random and hostile threats is usually dealt with under the header *critical information infrastructure protection*[35]. This strand of cyber securitization is one of the major links between cyber and threats to individuals, societies and states together with the *cyberwar* and *cyberterrorism* clusters. This narrative has a prominent place in the cyber threat landscape since the early internet[36], taking fundamental qualities of the computerized space as catalysts of the

[35] Good review of more than 20 CIIP policies and definitions of what should be protected can be found in (Wenger, Abele-Wigert, Dunn 2006)
[36] (Hansen, Nissenbaum 2009, p.1157)

threat – namely chain reactions that can have massive cascading effects as well as contagious nature of cyber worms. CIIP is a broader term that encompasses inherent risks, hacktivists, cyber-attacks as well as mass-scale scenarios that would be part of cyberwar interpretation.

Cybercrime is by far the most prominent form of cyber exploitation (ENISA 2013). It denotes acts against the confidentiality, integrity and availability of computer data as well as identity-related computer crime related crime with predominantly financial motivation. It also the most regulated area of cyber behaviour with 82 countries having signed at least one cybercrime convention[37], with the Budapest convention under the auspices of The Council of Europe being arguably the most successful cyber treaty to date (Geers 2011, pp. 29-30). Delineating what is criminal has long been one of the crucial powers of nation-states and it seems that this authority over determining what constitutes a crime and what are the methods and punishment for such behaviour. Compared to the regulation of internet governance and hostile behaviour of states within cyberspace this has been marked by less struggle and rather clear link to criminal prosecution.

Hacktivism forms a cluster of cyber activists and hackers that use the internet as a platform to pursue their *political* ends. These range from genuine activism that falls within the scope of human rights, civil disobedience and civil society offshoots to bordering terrorism in coordinated attacks that aim to subvert hegemonic institutions that are perceived as oppressive. Additionally, a group that can be termed cyber warriors[38] that claim to work on behalf of their governments on a voluntary basis is now a well-established phenomenon. The attribution conundrum however makes it rather difficult to discern between one off lone wolf hacktivists, organized groups

[37] These are: The Council of Europe Convention on Cybercrime, the League of Arab States Convention on Combating Information Technology Offences, the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information, or the Shanghai Cooperation Organization Agreement in the Field of International Information Security. (United Nations Office on Crime and Drugs 2013)
[38] (Paget 2012)

acting on their own and clandestine state backed operations. To put it in wise words of Sun Tzu: “all warfare is based on deception”[39].

Hostile cyber-activity that appears increasingly more on the level of states and has strategic connotations termed Computer Network Exploitation (CNE) would fit into the category of espionage. Espionage has a tradition of being in the grey zone of bordering diplomacy as codified by international law and being outright illegal (Kish, Turns 1995). Cyber in this case serves the age-old endeavour of espionage albeit with different means. If CNE operations are understood as an act of force or act of war than a dangerous *casus belli* would be present virtually always (Libicki 2009, pp. 64-66). In another words, the CNE threats are similar to common cybercrime activities – with the distinction of being securitized by nation-stated on the basis of perceived relevance to sovereignty and integrity.

Cyber-attacks are distinguished from CNE and lower intensity activities by aiming to or actually causing physical harm. There is a clear link to CIIP mentioned earlier with e.g. SCADA[40] control systems being likely targets. While there have been cases of such behaviour (see section 2.3.1) these have been rather isolated and limited in scope. Cyberwar – that can be understood as coordinated systematic sequence of cyber-attacks remains only a strategic concepts. In this sense there are similarities to nuclear war which because of its non-existence required imaginative suppositions and framing based on perceptions rather than empirical facts. As stated by one of the few advocates of cyber desecuritization: *(p)erhaps more than any other form of combat, cyberwar is storytelling — appropriately for a form of conflict that means to alter information*(Libicki 2013). Advanced persistent threats (APT) currently represent the most aggressive cyber behaviour as will be discussed via the case of Stuxnet in the next section.

[39] (Tzu 2010, article 18)
[40] Supervisory Control and Data Acquisition

While the apparent gap between securitization language of cyber warfare and hard "virtual space" facts is striking and points toward over-securitization one should not underestimate the enhancing/enabling power of cyber efforts in propaganda and "hearts and minds" within a conflict. The bulk of the discussion tends to stress the acuteness of cyber threats and the ill-preparedness of governments, organizations, armies and society as a whole to deal with these (Crosston 2011). As will be discussed in the next section, the psychological effects of cyber offensive activities so far trump the little damage that has been done to physical infrastructure.

The universality of the network design causes concern with regard to cyber sector as we know it now. The infrastructure suite was not designed with security in mind, but simplicity. Within the common discourse of cyber sector being somewhat hostile environment *connectivity is well ahead of security* (Geers 2011, p. 10). Correspondingly, this (im)balance favours the offensive for several reasons. The desired goal of resilience to physical destruction through decentralization has its adverse effect in lowering cyber resilience through connectivity. Within the world of interconnected networks it is sufficient to gain access to one network or one computer to be able to access virtually the whole system, perimeter defense is challenging.

The customary law of war supposes that belligerents identify themselves and distinguish between combatants[41]. In the cyber realm this might be difficult to do so, let alone if attackers deliberately use deception as part of their tactical plan. The use of botnets also classifies as concealment and a very effective one. These networks of hacked computers are infected with malicious piece of code and under command and control of rogue server. Affected computers can be in various countries and thus subject to various jurisdictions. Additionally, "active cyber defence" or tracing and retaliation on attackers might be simply impossible because one will only hit on innocent intermediaries. Cyber retaliation which is discussed currently as one of the directions of securing data might then cause more harm by targeting wrong actors (Websense 2014). Misattribution would also run the risk of having to deal with two

[41] As understood within the framework of customary international law and the Geneva conventions (ICRC 1949).

enemies – the original attacker and the wrongfully accused / counter-attacked. Thirdly, with lack of "flags" in cyber-space retaliation could be framed by third parties as aggression (Libicki 2009).

Moreover the decentralized web-like structure of the global network makes it likely impossible to *dominate* within this space – the preferred strategic conduct of militaries with the goal of effective control (Joubert 2010). In vein of the Law of the instrument: *if all you have is a hammer, everything looks like a nail*[42] institutions and communities tend to respond to perceived new threats through their adaption to old realities. The extensive use of hyphenated words in cyberspace creates such an impression, e.g. cyber-war, cyber-warfare putting it tacitly into the same box as the original terms. The perception of insecurity and vulnerability is often presented as the driver of policy and social change, effectively restricting and presupposing on what should be the course of action based on perception of (ever-present) threat (Furedi 2008). In another words the threat perception is what drives change no the threat itself. That is independent of what type of threat is engaged but due to the novel and technical nature of cyber environment the difference or what can be termed separation of threat and perception is arguably larger.

2.3.1. Theory vs. practice: empirical evidence of materialization of cyber threats

The effects of cyber-attacks to date have been rather modest in comparison with some of the forecasts of cyber Pearl Harbors, cyber apocalypse or cyber terror plots. This complex of securitization dynamic appropriately termed FUD (fear, uncertainty and doubt)[43] applies to both state securitization and private sector securitization. It is certainly one of the specifics of the cyber sector that the bulk of protection and security related investment is done by the private sector and taken care of by firms from the private sector who understandably securitize the issues in order to

[42] (Maslow 2004)
[43] (Westin 2012)

make their business profitable. This is in contrast to the theoretical monopoly of nation-state with regard to projecting of physical (military) power i.e. the idea of monopoly of legitimate physical violence (Weber 2004).

Well-known experiment from the Day After series sponsored by the RAND Corporation[44] simulates world-wide disruption of communication and many other aspects of society including loss of lives – yet even though these thought experiments are almost 20 years old fortunately no such events of comparable scale have taken place. Due to the nature of this research and its interest in cyber sector dynamics in general and implications on security behaviour of states and organizations majority of cases that fall into the category of cybercrime or organized crime as such will be omitted. Moreover, one should note that no lives were lost so far during any cyber-attack in spite of notable securitization and even destruction of physical devices or infrastructures is rare to non-existent.

2.3.1.1. Estonia 2007 – Cyber riots

In late spring of 2007 coordinated cyber-attack targeting Estonian private and public infrastructure as well as government websites took place. This followed Estonian governments plan to relocate WW II Soviet memorial, which was labelled blasphemous by the Russian Foreign Minister Sergei Lavrov and sparked civil unrest by the sizeable Russian minority in Estonia (Socor 2007) . The attacks which utilized mainly denial-of-service (DoS) and more advanced distributed-denial-of-service (DDoS) methods were aiming on a large attack surface. Estonia has since the 1990s systematically developed ICT as preferred means of banking and interaction with government services[45]. With such deep intertwining between online and offline worlds network was coupled with state and society within the discourse (Hansen, Nissenbaum 2009, p.1169).Although some links to Russian based server machines were established, due to the fluid nature of cyberspace and the extensive usage of botnets used to flood targets with requests no clear link to the Russian administration was made. The attacks

[44] (Anderson, Hearn 1996)
[45] In 2007 more than 95% of banking operations were conducted online and more than 98% of Estonian territory was covered with internet access (Kikk, Kaska, Vihul 2010 pp. 16-17).

came from more than 50 countries[46] as shown by country IPs. This demonstrated the lack of relevant "flags" in cyberspace and highlighted the attribution problem. Though the attack was rather prolonged for a DDoS attack lasting for weeks[47], it did not target critical infrastructure with the aim of causing wanton destruction and consequences remained largely on the level of inconvenience. Estonian administration however was quick to suggest a link between violation of cyberspace and violation of sovereignty[48], further prompting discussion on whether such attack can invoke NATO Article V provisions. Furthermore, the securitizing logic was taken over or even actively pushed forward by major media outlets by common usage of the term "cyberwar" for the first time in a (alleged) state-to-state attack (Farivar 2009).

While not providing grounds for a specific action the incident has sparked debate within NATO that has moved cyber security up the ladder of threats and led to the establishment of CCD COE[49] in Tallinn a year later (Grenda 2013). The most important work that is the result of the Centre's work is the Tallinn manual that seeks to clarify how does cyber realm fit into the existing body of International law and how should cyber warfare be regulated (Schmitt 2013). Group of experts that has worked on the document agreed that international law principles apply in cyberspace and that jus in bello rules apply to computer network attacks as well (Schmitt 2012). Furthermore, computer network attack can trigger right of national self-defence under the provisions of UN Charter. However, even if one concludes that cyber-attack can be a trigger for such legal claims[50] what can be claimed as defensive actions by the securitizing actors opens up a large space, including pre-emptive and preventive attacks and controversial "active" cyber defence.

These cyber-incidents had notable influence on the dynamics of threat cognition in Brussels as Estonia was of course at the time already EU member state making it very illustrative case for following research. The EU had in coordination with

---

[46] (Michaels 2007)
[47] At least 128 unique attacks were distinguished (Arbor Networks 2007)
[48] (Anderson 2007)
[49] Cooperative Cyber Defence Centre of Excellence
[50] As specified by article 51 of the UN Charter (United Nations 1945)

NATO announced a series of long-term cyber-defence goals and began efforts to establish European CERT (Herzog 2011). Moreover, the framing has shifted from matters of internal security (cybercrime) toward mass-scale attacks that might have the effects of military action. In the first CIIP directive the European commission goes on to state that cyber-attacks can have serious effects on societal vital functions and that the case of Estonia is part of a general trend of attack sophistication and increasing frequency as well as severity (European Commission 2009, p. 1, 4).

2.3.1.2. Stuxnet – weapon of specific destruction

Protection and targeting of control systems in (critical) infrastructure is one of the key facets of cyber security. Doomsday scenarios often invoke narratives that put the networked character of these systems at the core of the large-scale damage potential. Cyber defence exercises (CDX) seek to model realistic scenarios that usually involve targeting SCADA systems: e.g. Baltic Cyber Shield[51], Eligible Receiver[52] or Cyber Europe 2012[53]. Although surrounded by a veil of mystery as well as history, alleged sabotage of the Soviet gas pipeline SCADA caused massive explosion in 1982 (Reed 2007). As part of the Cold war strategy of undermining Soviet economy the CIA has allegedly planted a backdoor access bug into the Canadian built control infrastructure that was later utilized to cause the pipeline to malfunction. This cyber operation from distant past remains the most destructive in terms of physical power/magnitude of explosion. Yet the translation mechanism from physical-world effects to perception takes a complicated and contingent way. The vandalism-like attack on Estonia analysed in the previous section was relatively trivial[54] compared to sophisticated worms that

[51] Exercise in defending critical infrastructure under the auspices of CCD COE it simulated attack on SCADA-enabled power generation factories. The attackers succeeded in gaining access to the model factories yet did not manage to cause physical destruction as such (Geers 2010).
[52] First large scale CDX in the US in 1997, attackers have succeeded in compromising power generation and emergency services (Adams 2001).
[53] Europe-wide exercise with 25 participating countries sponsored by the EU and including players from the private sphere it simulated a large scale DDoS attack on public institutions (ENISA 2012) – presumably modelled after the Estonian cyber incidents.
[54] e.g. (Joubert 2012) -

are able to take control over target system – yet it produced serious repercussions for cyber policy especially within NATO and more generally the West.

The Stuxnet worm was from a technical point of view some of the most sophisticated malicious code ever deployed[55] with specific target being Iranian uranium enrichment facilities. It featured several zero-day exploits[56], genuine stolen digital signatures; first-ever PLC[57] rootkit and other advanced methods as well as limited yet significant physical damage to the Natanz nuclear enrichment plant. Some of these methods were completely novel, most important to the worm's apparent success though was the combination of these features. Its goal was to take control and tamper with centrifuges enriching uranium. Imprinted within the worm's design was a set of conditions that gives away the perpetrator's goal of a surgical strike. Even after the worm has propagated beyond its original scope the majority of infected computers were in Iran as graphed in Figure 7.

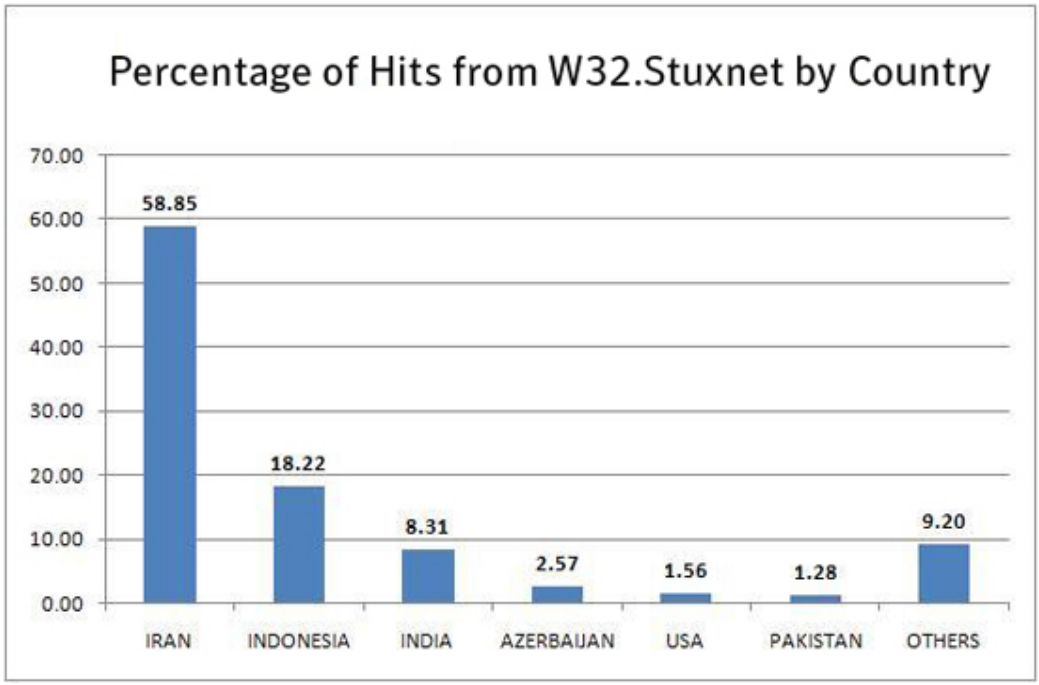

FIGURE 8(FALLIERE, MURCHU, CHIEN 2011)

[55] Generally accepted perception see c.f. (Falliere, Murchu, Chien 2011)(Collins, McCombie 2012)(Farwell, Rohozinski 2011)(Peterson 2013)

[56] Previously unknown vulnerabilities in software and firmware. Once used to facilitate an attack they become less valuable, because patches will be developed rapidly. These can be purchased on the cyber black market as well as for example hiring a server farm to conduct a DDoS attack or various exploit kits (Ablon, Libicki, Golay 2014).

[57] Programmable Logic Controller – a piece of hardware that controls industrial processes, in this case Siemens manufacture machine that was controlling the centrifuge process.

It was not designed to cause widespread havoc, quite the contrary it was supposed to operate in a very specific environment as secretly as possible. Within the unusually complex code were instruction to be become active only if more than 155 centrifuges are found and these had to be spinning at 800-1200Hz – i.e. targeting centrifuges in Natanz plant where there were 164 connected as one block that were in the process of enrichment of uranium (Nachenberg 2012). Moreover, it had the ability to prerecord normal operation of centrifuges and then send this data to the operator in order to convince them that their equipment is not malfunctioning. By taking a self-restraint attitude it managed to stay operational on Iranian machines for substantial amount of time and caused physical damage to several of the centrifuges as well as destabilizing the Iranian programme as a whole. Additionally, the virus needed to be completely self-sufficient since target systems are air-gapped – that is physically separated from the Internet. This also required that a version of the virus be brought onto the PLCs probably on a flash drive to jump this defensive barrier (Langner 2011). The massive self-propagation and viral behaviour of Stuxnet was most likely unwanted mistake that flawed later version of the worm and effectively revealed it to the outside world. The double-edge sword nature of cyber weapons raises legitimate concern that Stuxnet could be modified and updated to target other PLC utilizing systems.

Attribution or lack of thereof remains the leitmotif of all cyber-attacks and Stuxnet is no exception. Circumstantial evidence points towards a covert CIA programme by the name Olympic games that was conducted with close cooperation with the Israeli cyber experts (Sanger 2012). Iran's perceived attempt at obtaining weapon grade uranium is highly securitized in both the US and Israel and the sheer scope of the project the circumstantial evidence is rather compelling[58]. The lack of attribution reveals one of the facets of cyberspace: it can be preferred strategic choice for states to act compared to conventional kinetic strike. The Stuxnet worm has achieved substantial delay to the Iranian programme, conservatively estimated at two years (Collins, McCombie 2012). Under the proposed Tallinn manual guidelines it

[58] Especially the necessity to have a lab where such code could be tested with equipment similar to the Iranian plant, (Sanger 2012) presents within his book that equipment seized from Muamar Gadaffi by the US was in fact used for this purpose.

would most certainly fall under the cyber sovereignty principle and right to self-defence (Schmitt 2013, Rules 1, 9, 15). Additionally, it serves as illustrative case in point of the notable militarization of cyberspace (Cavelty 2012) with e.g. US Air Force updating its mission statement to include cyber operations recently (Cook 2010).

The case of Stuxnet also shows the discrepancy between theory and practice – while there are serious efforts to define cyber-attacks of this scope as acts of force and further analysis that presents itself as balanced the normative jolt can hardly be omitted. Though extrapolations are always misleading to some extent it is reasonable to argue that should the US, a NATO country or other major power be target of such attack the articulation and response to threat would be much more eloquent. Of course, it also needs to be taken into account that Iran's nuclear programme of enriching uranium past electric power generation level[59] is in the grey zone of illegality under the Non Proliferation Treaty.

The academia-policy making nexus is heritage of the study of security that tends to be politicized with especially one cluster of the security studies having the status of instrumental tactical deliberation on how to beat the enemy – strategic studies (Betts 1997). Moreover, it is a part of the practical reality of researchers and policy makers migrating back and forth which makes the distinction between (theoretically) impartial academia and normatively oriented state administration rather blurry (Bailes, Dinesen, Haukkala, Joenniemi, Spiegeleire 2011). In the case of Stuxnet we are therefore presented with interesting paradox: a worm that can cause massive harm and probably constitutes an act of force and is thus illegal under current International law interpretation – yet targeting a state that defies the hegemony of the UN/NPT regimes and is therefore the "enemy" implicitly present within the discourse.

The underlying logic of amity/enmity that pre-structures results of analysis and normative skewing is common-place (Campbell 1990). As was argued by Booth (1991)

[59] While only 5% enriched Uranium is needed for nuclear reactor electricity production, Iran has enriched some Uranium to at least 20% with possibly other undeclared activities hinting at military dimension of the whole programme (IAEA 2013)

rather well: the concepts that are connected with the nation-state such as power and order shape reality and imbue it with strategic objectives effectively barring emancipation as a form of sustainable security.

2.3.1.3. Russia – Georgia conflict 2008: ICT targeting as part of military campaign

During the conflict between Russia and Georgia over disputed territories of South Ossetia cyber means served supporting role to kinetic combat. Both sides themselves or through their sympathizers employed computer network operations, consisting of attacks designed to disable or degrade key infrastructure, and exploitation or hijacking of government computer systems (Deibert, Rohozinski, Crete-Nishihata 2012). DDoS attacks formed a large part of this supporting campaign and while it was timed to coincide with the start of the official Russian military campaign no official involvement was admitted (Bumgarner 2009). Its targets (government institutions, financial institutions and communication infrastructure in general) bear similarity to the Estonia incident a year earlier yet might be framed within the larger picture of the conventional campaign. Russian forces have previously employed similar information tools in the second Chechen war (Thomas 2000). Importantly, the role of physical ICT infrastructure played a role here as some of the main communication links on the western side of Georgia were physically destroyed[60] – making this instance forceful argument to study the usually omitted aspect of where servers and connecting links are physically based.

The use of cyberspace as a tool for political-military goals demonstrates the business-as-usual asset that has its root in realist/geopolitical paradigm where *realpolitik* is extended into the new domain (Manjikian 2010). Yet the cases of Estonia, Stuxnet and Georgia show that attackers were applying self-restraint. Critical infrastructure was not attacked, the cases of Estonia and Georgia with allegedly organized Russian involvement were aimed to cause inconvenience and influence the

[60] (Deibert, Rohozinski, Crete-Nishihata 2012)

information sphere as well as to spread propagandist messages and in the case of Georgia legitimize the real-world kinetic campaign (Hollis 2011). In the case of Stuxnet it was a very specific code that was designed not to cause wanton destruction. Even though cyber realm is not regulated by rigid arms control treaty such as the CWC or even softer regimes that pertain to Nuclear weapons limitations one can argue that there are norms created by custom. Communities of practice are the carriers of norms and lead to their dissemination (Adler 2008). Self-restraint as a political rationality can thus extend into cyberspace and limit projected impact of hostile cyber activities. Alternatively, it can be an expression of the mutual interconnectedness and vulnerability in cyber space where it would be a strategic miscalculation since retaliation in kind might be possible.

2.3.1.4. Other notable cyber incidents

To demonstrate the varied use several other notable incidents will be briefly analysed. To keep in line with the predominantly strategic (state-level) concern in cyber realm, threats that were large scale in terms of number of machines infected or world wide scope but financially motivated i.e. criminal will be omitted. Needless to say, due to the inherent centrifugal nature of the global network based on TCP/IP solid data are difficult to obtain, especially in open-source manner. Unlike armed conflicts proper[61], which are more easily distinguishable with cyber incidents it is often unclear who are the belligerents and what is the scope of the attack. It is however one of the key points of this research to show the dynamics that appear when novel cyber means are confronted with the more traditional definition of threats and conflict.

Hailing from the family of Advanced Persistent Threats the **Flame** virus hit computers and servers in Iran and the Middle East. While abnormally complex, it differs from the Stuxnet worm in that it was not designed to cause damage but rather serve as espionage tool capturing data from hard-drives as well as other computer

[61] A number of conventional conflict databases exist e.g. (International Institue for Strategic Studies 2014; Uppsala Conflict Data Program 2014; DACS 2014)

interfaces and sending them to command and control computers (Demidov, Simonenko 2013). Once again it is unclear where did it originate or where do the data sent to command and control centres lead. Additionally, it appears that the virus was active for 2 years before being discovered(Kaspersky Lab 2012).

To stay within the region, notable attack took place in 2012 when malware dubbed **Shamoon** infected Saudi Aramco[62] computers with the apparent goal of disrupting production (Hall, Blas 2012). The virus managed to destroy over 50 000 hard drives as well as data on a server yet failed to halt production of oil by the company due to mistake in the code syntax (Riley, Engleman 2012). Previously unknown group called "The Cutting Sword of Justice" stating anti-oppression motives. Yet speculation fuelled by US Secretary of Defence Leon Panetta voicing concern points toward Iranian involvement, possibly with some form of re-usage of the covert Olympic Games cyber programme (Bronk, Tikk-Ringas 2013). Judged on effects of lost data, it seems to be one of the most serious incidents ever. Similarly to other attacks to date attribution is dubious apart from the most likely dissemination method of choice – a USB stick introduced by one of the employees (Perlroth 2012).

Another mass espionage APT codenamed **Red October** was discovered in 2012. It has been operational for at least several years (Kaspersky Lab 2013). Moreover, it managed to gain access to machines in governmental, diplomatic and scientific research organizations with distinct geographic focus on former USSR, Central Asia and Eastern Europe. The details are again murky with forensic evidence pointing at a collaborative effort of Chinese and Russian-speaking operatives (Infosecurity 2013). Cyber espionage that is sometimes mislabelled as warfare forms the bulk of large scale threats – compared to the heightened securitization of CIIP and the potential for its destruction.

[62] State-owned oil company, largest oil producer and reserve holder in the world (Saudi Aramco 2014)

In 2009 network codenamed **GhostNet** was uncovered. This large scale network that consisted of over 1295 hosts in 103 countries was found through tracking spying on Tibetan institutions with circumstantial evidence pointing at China(Deibert, Rohozinski 2009). This exploit utilized a Trojan named gh0st RAT that could gain real time control of the host computer. The cited report however stops short of linking this activity to Chinese government, leaving open the possibility that it was a group of "patriotic" hackers or other states' secret services using Chinese underground hackers as proxies.

In an effort to bring the spotlight on these issues the Head of USCYBERCOM stated that cyber espionage is the greatest transfer of wealth in human history (Alexander 2012). In a thorough analysis of **APT1** a cluster of cyber espionage activities the security firm Mandiant has been able to trace some of these activities into a particular building in Shanghai that belongs to special unit of the People's Liberation Army (Mandiant 2013a). China has a long history of breaching the Western introduced and thereby alien standards of intellectual property. ICT capabilities are a plausible strategic choice for power projection of the underdog (Inkster 2013). It is customary that analyses of threats are done by private cyber security firms and these usually include rather general information and would refrain from linking cyber incidents to interfaces and institutions, possibly also to stay within the open source information scope. In this sense Mandiant's report is landmark in that it includes detailed forensic information in multiple appendices that amount to "smoking-gun" evidence linking intellectual property theft and espionage to Chinese army if not disproved. The sensation of authenticity is enhanced by including a video of a hacker session, that accompanied with a commentary shows step by step attack(Mandiant 2013b). This public name and shame approach can open the door for further securitizations on the subject and can be possibly understood as normative deterrent. Since these are relatively fresh developments it will be interesting to see if it will become the norm private security firms will provide the bulk of forensics and expertise. Comparison to the outsourcing of humanitarian and other aspects of state conduct comes to mind (Hynek 2008).

To sum it up, there were notable cyber-attacks where states were (most likely) involved or supported them through proxies. Given the enormous attack surface – virtually all aspects of society being to some extent computerized – the effects of attacks though notable remain fairly limited. Judging by the limited scope of cyber-attacks to date it is plausible that expressing self-restraint is an expression of the mutual dependency in the cyber world, where a massive and thus traceable attack would be followed by retaliation. The often mentioned idea of double-edged sword fits this situation well. Hence there is a form of deterrence logic working its way in the cyber realm[63], assuring that states do not undertake large scale cyber campaigns, although cyber espionage is commonplace on all continents. The "threat inflation"[64] and relatively scarce major cyber incidents – that is excluding financially motivated hacking, fraud, phishing etc. – points toward over-securitization of the domain as such. Possible explanations for divergence between expectations of "cyber-doom" scenarios and real-world cases include: the policy window that was opened after the end of the Cold war, misunderstanding of the technical constraints of the cyber domain, struggle for funding and raison d'être by various institutions as well as marketing moves by private cyber security companies(Lawson 2011; Cavelty 2008b, 2012; Deibert 2003; Eriksson 2001b; Westin 2012). Having discussed the specifics of cyber space through its history as well as empirical cases the analysis will now turn to the European Union as security actor in cyberspace and its framing of perceived threats as well as response to these.

[63] See (Crosston 2011) who argues that cyber posture along deliberate Cyber Mutual Assured Debilitation may yield the same effects of stability as the original hair-trigger logic of nuclear MAD.
[64] (Brito, Watkins 2011)

3. European Union and its (cyber) security narrative

Having laid the groundwork of the cyber sector in section 2, its particular historical background, threat dynamics and illustrative cases the analysis can now move on to dissect the case of EU and its involvement in cyber securitization. The framework that was laid out in section 1 will be used on the following pages with substantial amount of data analysed. Additionally, theoretical insights relating to European strategic culture and its implication on cyber threat framing will be analysed as well as extension of the arguments presented earlier on structural constraints in cyberspace and the "ethos" of the global network.

3.1. European Union: constitution of a security actor and strategic culture

The complexity of cyber related issues fits well with the complex supranational position of the EU. Acting across borders and part as aggregator of ideas part as driver of policy dynamics it underscores the importance of diffusion of ideas within epistemic communities (Eriksson 2001b). Importantly, there is interesting interplay between the EU establishing itself as a security actor as such and the trend of IT securitization as such. Insights from strategic culture oriented research that focuses on the identity and normative constraints surrounding the use of force and strategic choices enrich understanding of this particular narrative. The process is based on the formation of unique philosophical, political, normative, cultural and cognitive characteristics into a particular identity (Johnston 1995). It is through this historically contingent viewpoint that one can understand some of the defining features of fledgling European strategic culture. While it is not inherently in opposition to features of *realpolitik* it does help to understand the strong normative base of European strategic thinking. Strategic culture can be understood as ideational base that informs actor's strategy in wider sense (i.e. grand strategy) while also serving as base of the threat framing mechanism. As Smith (2011) argues the EU does possess three features that form the base of a grand strategy: physical security, economic security and value projection – which is of added value to the grand strategies to sum of member states.

The idea of foreign policy coordination and integration has been present, albeit in a weak form, in the integration discourse since the 1950s and later led to the establishment of European Political Cooperation (Smith 2004). The intergovernmental weakness of EPC and its non-military character are noticeable in Single European Act of 1986 as well as using the word "security" and refraining from using "defense" as this would point toward territorial defense (Fiala, Pitrová 2009, pp. 599-602). This cautious yet noticeable spill-over effect into security matters took increased urgency after the whirlwind of events in the early 1990s. The absence of a global struggle that rendered many nuances not noticeable as well as the bitter experience with Balkans and the inability of Europe to act accelerated the whole process. To put it in the words of Jacques Delors, in the early phase of Yugoslavia conflict the EC had only three weapons at its disposal: „public opinion, the threat to recognize Slovenia and Croatia and economic sanctions"[65] and spurred debate on the role of WEU and the EC taking care of its own near neighbourhood. With various national cultures under one roof of EC and later EU it is understandable that the mantra of coherence and comprehensive approach resonates strongly and is in fact one of the unifying factors of European strategic documents. The discussion on the relationship between EU, WEU and NATO is temporarily resolved with the Petersberg tasks[66], which state that the WEU will engage in crisis management operations and frames the WEU engagement within the emerging EU Security framework. The uneasy NATO – EU relationship is enigmatic on its own, adding a further layer of complexity to the already fragmented nature of supranationality(Cornish, Edwards 2005). The Kosovo campaign served as yet another event driving the emancipation of European security community which touches upon some of the central aspects of sovereignty. As Mérand (2010) argues from a distinctly Bourdieu-inspired framework both the sociological and structural aspects of experience of security integration through NATO and perception of crises in Europe or its near neighbourhood was formative for the launch of ESDP in 1998.

[65] (quoted in Salmon 1992, p. 248)
[66] (Western European Union Council of Ministers 1992)

Furthermore, the difficulty that traditional approaches such as (neo)-realism, intergovernmentalism or neofunctionalism have in explaining the degree of integration in sensitive security field point to large role of ideas, perception of reality and identity as stressed by constructivist approaches (Meyer, Strickmann 2011). The distinct "civilian" or "comprehensive" approach stressing the need for combination of military and non-military means that give CSDP its distinct flavour has its roots in the core of EU states pushing for multilateralism, QMV[67] within the EU and federalism in general (Risse 2012).

Brussels-based and European related epistemic communities provide valuable insights into how such identity is formed within relatively short space (Cross 2013). As introduced in section 1 of this thesis there are two aspects of epistemic communities that are used in this analysis. Firstly it is the creation of a community or strategic culture that is connected to the emergence of CFSP and its major part CSDP[68]. This process has allowed for cautious yet notable strengthening of EU-institutional framework and field experience in the 34 missions to date[69] with experiences solidifying communal identity. Complex interdependence that both creates and is a product of shared identity in a circular fashion is major dynamic behind „actorness" of the EU (Howorth 2010). The second level through which epistemic communities come into play are the communities of technical experts in the cyber field. As was argued earlier, the distinct way in which the information revolution took place has its effects on the shared identities of experts working within the field. This is further accelerated by the border-dissolving nature of ICT.

Attempts to classify the EU as a type of actor have often included novel categories such as normative power, civilian power or postmodern power(Smith 2008). Generally, they hint toward accent on soft power issues, value projection, human-rights discourse and the fusing of socioeconomic and military fusing of security approach. The balance however has shifted and under the oft repeated label of comprehensive approach a

[67] Qualified Majority Voting – voting mechanism ensuring that at least 50% of the EU population as well as member states are part of the majority, currently at 74,8% of the EP members.
[68] To make matters clearer only CSDP will be used as the successor to ESDP
[69] (ISIS Europe 2014)

"global power" discourse has formed. As Rogers (2009) argues this change should be understood as a top-down project, which grants the EU considerable room to act and form its identity at least partly independently of the Member states. In the hallmark document *A Secure Europe in a Better World – European Security Strategy*[70] from 2003 basic principles of ESS are drawn up. EU is declaring to be prepared *to share the responsibility* of maintaining global security and the need to *develop a strategic culture that fosters early, rapid and when necessary robust intervention*. Thus one can sense that the epistemic communities on the European level reached tangible level of self-consciousness. This should be understood as realization of the goal set forth in the original Maastricht Treaty to:

implement a common foreign and security policy including the eventual framing of a common defence policy, which might in time lead to a common defence, thereby reinforcing the European Identity and its independence in order to promote peace, security and progress in Europe and the world[71].

This was later picked up and extended through the folding of WEU into EU structures as part of the Lisbon, where the solidarity clause is built into EU institutional architecture through article 222[72]. Identity based explanations provide powerful insight into how the *europeanization* of elites has fostered emergence of common culture. Furthermore, data from public opinion research suggest there is a strong support for integration of European Foreign policy as shown by figure 8 at least in theory[73]. In a qualitative study for the European Commission it was shown that foreign policy coordination suffers from "cacophony" and the ability of the EU to act is distinctly worse than in issues related to internal security cooperation e.g. police cooperation (Optem 2006).

[70] (European Commission 2003)
[71] (European Communities - Council 1992, p.4)
[72] (Conference of the Representatives of the Governments of the Member States 2007)
[73] Data from Eurobarometer only available from 2003 to 2005.

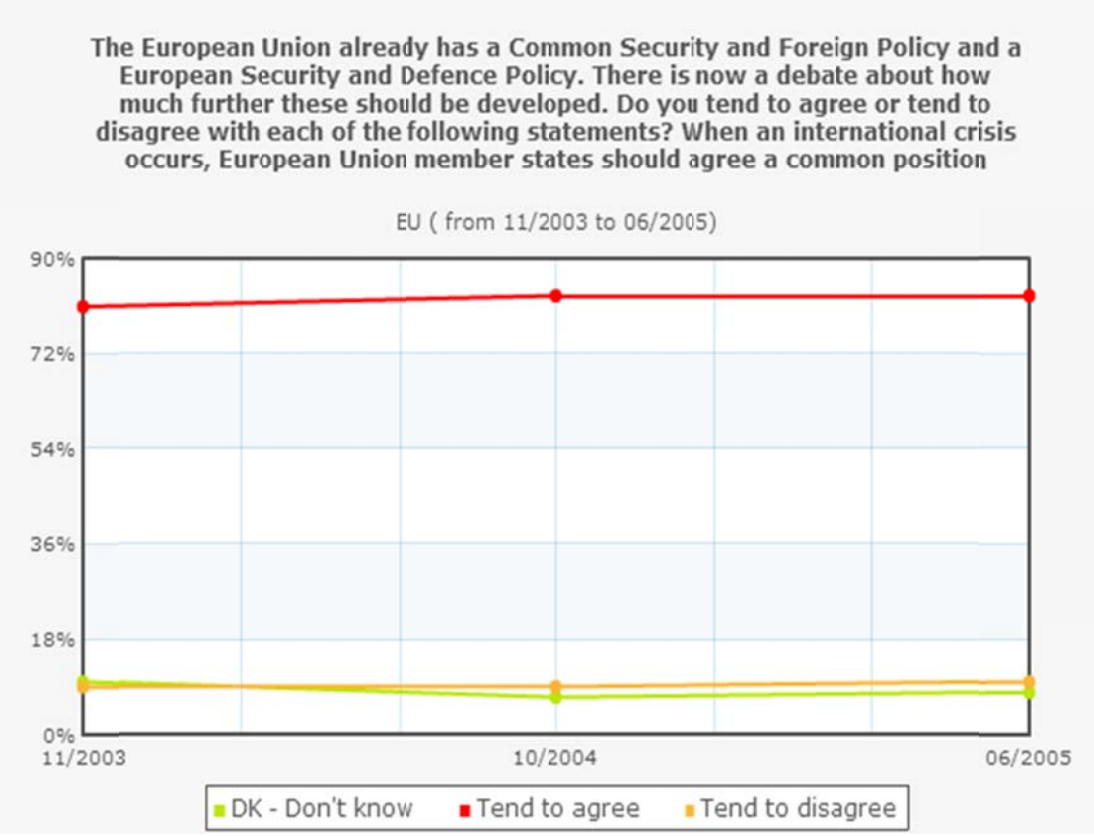

FIGURE 9 SOURCE: (EUROPEAN UNION 2010)

The sheer scale of effort that has produced over 1000 common strategies, common positions and joint actions in common foreign and security policy (CFSP) since 1993 and more than 2000 foreign policy statements by the EU Council and Presidency between 1995 and 2008 points to the tangibility of the whole process (Risse 2012). Having reviewed at least some broader aspects of the EC/EU security cooperation, integration, development of a particular strategic culture the thesis will study in more detail how cyber-related actions appeared and were framed.

3.2. Framing of Cyber-security within the EU: broader context

Swift comparison to the US debate on ICT security issues reveals that it was present in top policy making discourse in some form since the early 1990s. Of particular interest is the expert report *Computers at Risk*[74] from 1991 that foresaw

[74] (Computer Science and Telecommunications Board 1991)

many of the emerging problems of interconnectivity and networking of critical infrastructure. As early as 1997 the Commission on Critical infrastructure Protection submitted its report[75] to President Clinton linking crucial societal infrastructure with possible cyber disruption and urged for comprehensive protection. EU documents related to cyber security only began to surface in the early 2000s[76] which is understandable given the maturing of common policies and related discourses in late 1990s.

Unlike across the Atlantic in the EU existed a noticeable trend of distinguishing between civilian cyber-security concerning crime that fall under the aegis of the EU and strategic cyber-security concerned with military affairs that stays within the responsibility of the member states (Andreasson 2011). In a broader sense this can be understood as norm setting that is based on bottom-up processes with its blocks being criminal offences, critical infrastructure protection, pursuit of extension of human rights into cyberspace and progressing toward more sensitive strategic issues relating to "hard" security. This is underscored by the only international treaty regarding cyber security in effect being the Budapest Convention on Cybercrime from 2001[77] to which all EU member states are parties. Although the treaty was successfully pushed through under the auspices of Council of Europe and not the EU itself, the tight relationship these two institutions enjoy makes them epistemically connected and like-minded[78] and it is used here to paint a fuller picture of threat framing. The convention was also supported by common position document (Council of the European Union 1999). The convention focuses on a broad spectrum of computer related offences such as:

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer forgery and fraud
- Child pornography issues

[75] (President's Commission on Critical Infrastructure 1997)
[76] (Cencetti, Marrone 2013)
[77] (Council of Europe 2001)
[78] As shown for example through Memorandum of Understanding from 2007 (European Union, Council of Europe 2007)

What is perhaps of more interest than these fairly non-problematic issues that should be prosecuted by national jurisdictions are the latter parts of the convention that should give more power to law enforcement and fight cross border cybercrime with cross border cooperation. These powers are not in fact specific to cybercrimes but relate to any ICT use such as:

- Corporate liability
- Search and seizure of stored computer data
- Real-time monitoring of network traffic data
- Interception of content data

Thus the liberal world of cyber was linked to real-world criminal investigations and allowed authorities to legally control data flows and implement rule of law. This is not without criticism vis-a-vis censorship, free speech and the possibility of abuse for repression (Samson 2006). Furthermore, the strategy of *hypersecuritization*[79] where it is the everyday security occurrences taken to illustrate the ominous side of ICT provides a link as to how this can be extended from everyday practices to cybercrime and gradually to strategic cybersecurity to normalize it as a domain. It is notable that there are strikingly low prosecution numbers compared to other areas of crime, suggesting a mixture of insufficient ability of the law enforcement, attribution problems and the decentralized nature of the cyber realm as such (Wall 2008). Moreover, the Budapest convention provides base for a normative framework among like-minded nations that can be later diffused to create a type of normative deterrence frame in cyberspace (Stevens 2012b). These norms of conduct need not be formalized but might nevertheless exist – and lack of regulation of the cyber domain need not lead to "digital war against all" as Hughes (2010) argues.

[79] (Hansen, Nissenbaum 2009)

3.3. Frame constitution: Complex role of ICT through the prism of the EU

Building on the framing methodology that was introduced in chapter 1.2 and more specifically figures 1 and 2 the analysis will now focus on the various aspects and prisms through which ICT appears in EU discourse. The variety of issues that are inter-related shows that the structural complexity and intertwining of various spheres is a pervasive phenomenon as argued in prior chapters. It will be argued that partly because of the EU tradition as "civilian" community there is rather little militarily framed cyber security. Yet that does not make ICT issues second-order, precisely because the overall epistemological understanding emphasizes civil and economic areas. Arguments that ICT infrastructure requires centralized measures to maintain confidentiality, integrity and reliability – the so-called CIA triad of cyber security – transforms itself through connection to crucial societal functions as well as values. The referent object of what is at stake expands gradually to include Critical Infrastructure Protection, Human rights issues, economic development and even security proper to form large cluster of threats and fears. Thus in the official documents the frame is constituted in general terms since the early 2000s, preceding larger scale strategies that represent this epistemological realization. What follows are excerpts from early official documents of the EU to illustrate this foundation of the threat framing dynamic.

From now on, network and communication security is a strategic issue of the highest importance (Economic and Social Comittee 2002).

The success of the information society is important for Europe's growth, competitiveness and employment opportunities, and has far reaching economic, social and legal implications…there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society (Comission of the European Communities 2001a).

Acts deemed to be terrorist offence – causing extensive destruction to a facility…including information system (Council of the European Union 2002).

Protecting communication networks is increasingly considered as a priority for policy makers mainly because of data protection, ensuring a functioning economy, national security, and the wish to promote e-commerce. These challenges are compounded by the fact that the market will tend to under invest in security for reasons….of market imperfections (Comission of the European Communities 2001b).

(I)t is not just a question of learning how to use new technologies, it is also a question of adapting old habits and practices… This no longer primarily a question for technicians. What is needed for an effective transition is leadership from politicians. (Comission of the European Communities 2001c).

Overall, these documents uncover some basic tenets of the framing process. Clear link is established between the functioning of ICT systems, connectivity, the Internet and computer-based systems to the functioning of society and economy as such thus opening a door for the involvement of governments and EU institutions. Military securitization is not a clear trend at that time, the civilian character of EU discourse prevails with some explicit arguments pointing to market failure regulation – traditionally very strong area of EU involvement.

Moreover, it is more often the benefits and potential which is seen as partly unfulfilled that are stressed by the official documents. The vulnerability and perceived threat come up in vague notions, it is mostly related to cybercrime or terrorism. Only slowly can one see the linkage of cyber and critical infrastructure and (supra)national security that becomes more evident in latter documents and strategies. Coordination of CERT teams also makes its way into high level policy documents, but it stays within the line of coordination prior to the establishment of ENISA, the European CERT and strengthening of EUROPOL with EC3[80] to fight cybercrime which gives the EU more agency as such. It is also useful to realize that the reported use of the internet was only

[80] EUROPOL Cybercrime Centre that commenced activity in 2013 (EUROPOL 2014)

some 26% in the year 2000[81] compared to recent data showing some usage for up to 75% of the EU population in Autumn 2013 Eurobarometer[82]. This means that the lived everyday experiences have since then changed qualitatively, creating a different epistemic space.

3.4. Signs of maturity: Cyber security framing gaining prominent features

Although the first European Security Strategy from 2003 is not a watershed event in the sense of changing the purpose or fundamentally altering the capabilities of the EU it summarizes the foundation of what is most often termed "comprehensive" approach[83]. Yet it provides a useful point to examine the security narrative of the EU in the most general sense. Thus the wide concept of security deliberately makes use of various tools and seeks to target security problems at its root by promoting good governance and internal security. EU anti-piracy operation Atalanta[84] in the Horn of Africa, which was the first EU naval operation and was complemented by police training missions[85] and efforts to stabilize society at the root of the conflict sheds some light into what comprehensiveness EU aims for. The degree to which reality meets the strategic narrative can be contested, yet the fact that the EU seeks to create and express identity of tangible security actor is a sign of change. Following the post-911 zeitgeist one can find a link between terrorism which employs ICT means as global communication while at the same time making interconnected systems of infrastructure vulnerable to attack (European Commission 2003).

Delving into the Report on implementation of the ESS one finds that cyber threats have gained salience and are now presented as a distinct part of the document

---

[81] (European Union 2000)
[82] (European Union 2013)
[83] As argued and explained e.g. by (Cross 2013; Biscop, Howorth, Giegerich 2009; Smith 2011, 2008)
[84] Mission commenced in 2008 in support of UNSC resolutions (Council of the European Union 2008)
[85] EUTM Somalia commenced in 2010 and was since twice extended (Council of the European Union 2010)

(European Commission 2008). The focus on CIP is intensified, the cybercrime facets emphasised and the link between terrorism and cyber as either mean or target weakened. The report also recommends further work in this sector to be done, which could be understood as invitation for the creation of the first Cybersecurity strategy that was adopted in 2013 and will be analysed more in depth later. The next section will look into efforts that were made between 2003 and 2008 to argue that cybersecurity issues in their various shades are gaining salience as well as taking more distinct forms. Yet the narrative stops short of taking cybersecurity to the strategic level i.e. into the military sphere and focuses mostly on risk management efforts and crime mitigation.

Critical Infrastructure Protection in the fight against terrorism[86] creates a frame that argues for increased attention to potentially catastrophic terrorist attacks against critical infrastructures of the community warning of *cascading effects* and *potential loss of lives.* In the document establishing ENISA[87] it is stated that:

(t)he security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society not least because of the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks, that may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens[88]*.*

Thus taking a distinctly effects-based risk management approach that is to a certain extent incompatible or parallel to traditional security approach concerned with sovereignty, international law and is inherently and ostensibly political and normative. Efforts related to critical infrastructure protection include the establishment of early warning system CIWIN[89], complemented by piloting Green Paper on CIP[90]. This was followed by establishment of EPCIP[91] in 2006[92], where it is stated that the EU should

[86] (European Commission 2004)
[87] European Network and Information Security Agency
[88] (European Parliament, Council of the European Union 2004)
[89] Critical Infrastructure Early Warning Network
[90] (Commission of the European Communities 2005)
[91] European Programme for Critical Infrastructure Protection

focus on transboundary critical infrastructure threats and leave national critical infrastructure to be dealt with by member states through principle of subsidiarity. The chosen strategy follows all-hazards approach i.e. effects-based framework with no particular emphasis on ICT threats or ICT-terrorism connection. In a larger framework dating in the same year the *Strategy for a Secure Information Society* however goes on to state that:

The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society.[93]

Yet the frame tries to portray the problem and its solution mostly inward – in a similar way to regulation of other network-based infrastructure. Fundamental rights also come up as values that need to be upheld in cyberspace and without intervention or cooperation under EU guidance are at risk in regard to EU citizens. Yet one finds within the Counter-terrorism strategy attempt at regulation of internet traffic in order to *stop the misuse of internet*[94], which presupposes a robust traffic screening infrastructure as well as enforcing a particular normative frame deciding what is correct use and what is not. It is however true that expert opinions both from the EU institutions and Academia suggest that internet is a space that is functions as a facilitator of violent radicalization(Bures 2011).The link between terrorism and critical infrastructure attacks by electronic means are put forth in general terms within this strategy, yet lack urgency compared to conventional bomb attacks experienced in that time in Europe – as this document was published after both the Madrid and London bombings. However, in later Action Plan on Combating Terrorism the EU CT Coordinator points to possible terrorist attack on SCADA control systems as key concern with direct link to the Stuxnet attack[95]. The experience and interpretation of prominent cases thus shows clearly event-driven framing.

---

92 (Commission of the European Communities 2006a)
93 (Commission of the European Communities 2006b)
94 (European Commission 2005)
95 (EU Counter-Terrorism Coordinator 2011)

Tracing contingency of policy to events one inevitably has to take into account the Estonian cyber-incidents, which provoked some attention-grabbing framing such as "the first war in cyberspace" (see section 2.3.1.1 for more detail). Document titled with self-explanatory title "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"*[96]*.* Departing somewhat from the effects-based approach of prior documents the Estonian, Lithuanian and Georgian incidents are interpreted as evidence of a general trend documenting that *(c)yber-attacks have risen to an unprecedented level of sophistication*[97]*.* Analysis of weaknesses tends to translate into threats via political process with inadequate scrutiny, fusing potentials and real threats as Cavelty (2012) argues. In this sense the link between the interconnectedness and perceived vulnerability of CI and the network as such is unclear, especially given the lack of empirical evidence with the most oft cited argument being mere DDOS-attacks on "strategic" scale. The first pan-European cyber exercise Cyber Europe under the auspices of ENISA was held in 2010 set up by a directive of EU ministerial conference in Tallinn with the 2007 incidents still having effect on policy making[98]. The exercise was since followed by another two runs in 2012[99] and 2014[100]. Furthermore, ENISA coordinates national CERTs that are now present in all member states, calling them "digital fire brigades"[101]. This discursive turn implies that cyber threats are common parts of everyday live and should be or are becoming integrated into the complex of services provided by MS/EU along the lines of common Emergency services. However, given the predominantly private character of the ICT world it is not quite possible for state/suprastate to be the sole provider of these services, which leads to adoption of official PPP[102] approach launched by the aforementioned 2009 document on CIIP.

---

96 (European Commission 2009)
97 ibid p.5
98 (ENISA 2011a)
99 CERTs, Financial institutions, eGovernment institutions and ISPs from all member states took part in the exercise (ENISA 2012)
100 Evaluation report not yet available
101 (ENISA 2011b)
102 Public Private Partnership programme EP3R

Taking the whole complex of cyber related issues up the ladder of priorities and into mainstream policy efforts is signified by the far-reaching Digital Agenda for Europe announced in 2010. This effort posits ICT sector as key for the future development of EU as a whole. The celebration of innovation acquired through ICT means is offset with the need to step up *global risk management*, argues for the integration of European *digital single market* under the direction of the EU extending its mandate into yet another sector and push for the creation of normative legal environment that would combat *harmful online content* while at the same time *protect individuals' privacy and rights online*[103]. The efforts taken to conceptualize cyberspace signal that there is a trend to incorporate cyberspace into the existing norm of the European Convention on Human Rights, notably with regard to Article 8 on privacy protection and Article 10 on the right to free expression[104]. To put it in words of the EU Commissioner for the Digital Agenda: there should be a "multistakeholder model based on human rights"[105].

3.5. Cybersecurity strategy of the European Union – recent framing moves

Published in 2013, the Cyber Security Strategy of the European Union entitled *An Open, Safe and Secure Cyberspace*[106] caps off the various strands of conceptualizing cyber security issues by the EU into one overarching document. With the proliferation of such documents by various states[107] it is perhaps a sign of how cybersecurity as such became ripe and moved to front-burner type issue. As such it fulfils all three framing categories[108] - diagnostic, prognostic and motivational.

In the phase of interpreting and defining the problem a case is made that *(o)ur freedom and prosperity increasingly depend on a robust and innovative Internet*, suggesting that ICT and overall societal wellbeing is a structural condition that needs to

[103] (European Commission 2010)
[104] (Council of Europe 1950)
[105] (Kroes 2014)
[106] (European Commission 2013b)
[107] For a comprehensive list of such documents see e.g. (ENISA 2014)
[108] Following (Snow, Benford 1988; Eriksson, Noreen 2002) see section 1.2.1 for more detail

be taken into account. In a similar vein to earlier discourse it stresses the complex nature of how cyber world takes on societal functions such as providing forum for free expression and political rights – with explicit mention of the Arab spring as yet another policy-driving event. More over the connection to societal functioning through critical infrastructure is upheld once more and specific naming of potential state-sponsored cyber-attacks appears alongside terrorist and natural disaster possibilities reflecting the growing realization that cyber operations form part of overt or covert foreign policy instruments. In fact it does explicitly state that serious cyber-attack can be trigger of the solidarity clause, which goes to show that strategic cybersecurity has penetrated policy making on the highest level. The immaturity of cyberdefense related issues is confirmed by the perceived lack of facilities and doctrine[109], the militarization of ICT is perhaps the most contested area of institutional involvement. The Strategy also tacitly recognizes that the powerful role the global network has achieved as *instrument of global progress* happened without significant governmental oversight – thus acknowledging its specificity and the liberal emancipatory ethos.

The prognostic part of the frame puts forth general themes of how should cyber space be regulated and perceived potential threats countered. Here the document states that *cyber resilience*, *reducing cybercrime, developing defence capabilities under CSDP* and *establishing international policy* that will allow for *promotion of EU values* are the goals. The normative element of EU efforts was also underscored in a speech launching ECSS by Catherine Ashton: *The European Union is determined to promote and defend its values online*[110]*.* Thus the issue of internet governance or lack of thereof to be more precise is also part of the frame. Recent communication[111] on Internet governance goes on to state that the EU will pursue *upholding fundamental rights online*, aim for un-fragmented global network and pursue *multi-stakeholder governance*. This notion that appears in relevant documents for a substantial time and can be said to reflect the official EU position on the future of the internet is however rather vague. It is unclear who the stakeholders that could

[109] As documented by the recent RAND study for EDA (Robinson, Walczak, Brune 2013)
[110] (Ashton 2013)
[111] (European Commission 2014)

influence decisions taken are and whether there will be a hierarchy reflecting importance. Additionally, the plausibility of successful communication between sovereign states, international institutions, NGOs and others is far from self-evident and future development will shed more light into how exactly this might work or whether it is more of wishful thinking. Related to the question of internet governance is the upgrading onto a new protocol IPv6 (see chapter 2.1.1). ENISA supports[112] the new standard, which could potentially provide crucial link to more centralized control over the network, provide more secure and less shady cyberspace – possibly at the expense of privacy and organic freedom of the global network.

By aiming to increase resilience of ICT systems the EU pushes for deterring potential attacks by minimizing possible gains as well as increasing resistance to failure. Or in other words it is the pursuit of dissuasion by denial, making the adversary perceive that gains are highly improbable if attacked(Davis 2014). The resilience and redundancy are linked to the CIP and CIIP strategies that operate in a risk management space that is somewhat different in nature that (state) security. Deterrence by denial can be achieved even against non-state actors e.g. by. delegitimization of purpose for target audiences (Wilner 2011). Importantly it is the combination of defence and gain-denial with conscious building of normative framework (cyber as space enhancing freedom and prosperity) that is potentially bolstering the effects on threat mitigation.

Moreover, motivational framing seeks to provide groundwork for legitimizing involvement in cyber issues. The efforts of the EU that fit within larger regulation trend as discussed in chapter 2 seek to make the case that the importance of ICT has reached imaginary threshold after which it is too important to be left to organic growth. Furthermore the logic is that ICT world is a value in itself that might be lost if we do not take sufficient action to protect it. In line with the Digital Agenda it promotes *safe access to all*[113] - yet delineates what is acceptable and not along the lines of cyber-crime, cyber-terrorism and human rights creating cyber “us” vs. cyber “them”. Thus the frame opens the door toward security-openness trade-off that is used to legitimize

[112] (ENISA 2011c)
[113](European Commission 2013b, p.4)

intrusions of regulators and law enforcement in order to protect cyber "us". The narrative has increasingly posited ICT related issues as crucial parts of society as it stands now (more or less stating the importance that built up organically) as well as connecting these to normatively desired vision of the future and making it integral part of "progress". The conception positing that some of the most salient socio-economic risks to overall societal wellbeing lie within cybersecurity space is one that is shared globally – as documented e.g. by World Economic Forum research[114]. Looking back to the very beginnings of European post-war integration which was founded on two commodities that were perceived as crucial to the (socio)-economic functioning of Europe and their control as vital in precluding war one can find similarities to the current narrative. Cooperation and integration in the fast evolving cyber sphere should allow for both socio-economic wellbeing as well as minimizing of unwanted harmful behaviour – including warfare as stated in the EU CSS of 2013.

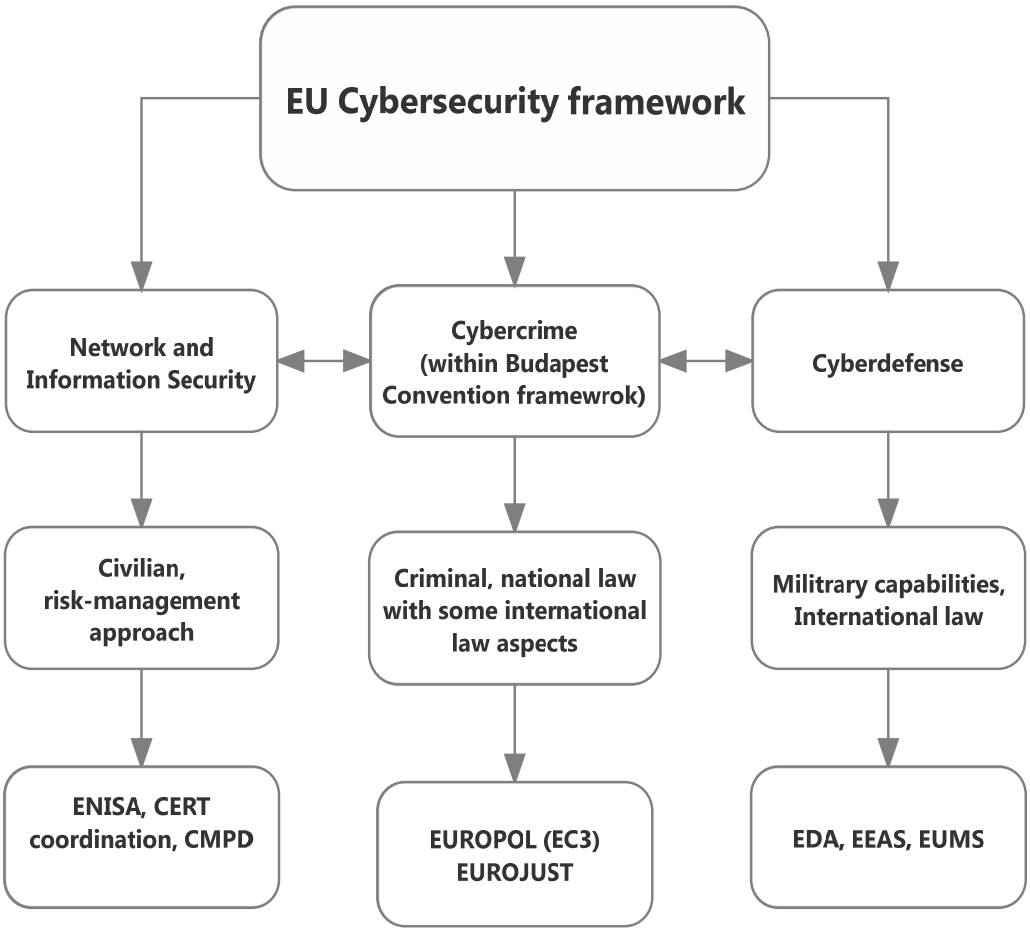

FIGURE 10 BASED ON (PAWLAK 2013; EUROPEAN COMMISSION 2013B)

[114] Quoted in (Robinson, Walczak, Brune 2013, p.4)

Figure 9 sketches out simplified EU cybersecurity framework. With the proclaimed differentiation into three strands of ICT security related issues it seems to solve the problems connected to the fluid nature of cyberspace, namely cross-sovereignty, lack of attribution and public-private delineation. Yet, this framework is EU's own view necessarily containing some simplification – as was argued throughout section 2 the incompatibility of cyber and values inherent to the specific processes that constituted it resist moulding into easily conceptualized categories.

Figure 10 on the other hand summarizes the complex set of views that come together to inform the cognition and creation of cybersecurity framing within the EU space and implicitly as well as explicitly push for the creation of norms regulation cyber space. For the sake of feasibility, the goal was not to track cyber discourses within the myriad EU institutions but to paint overall yet refined picture of this under-researched phenomenon.

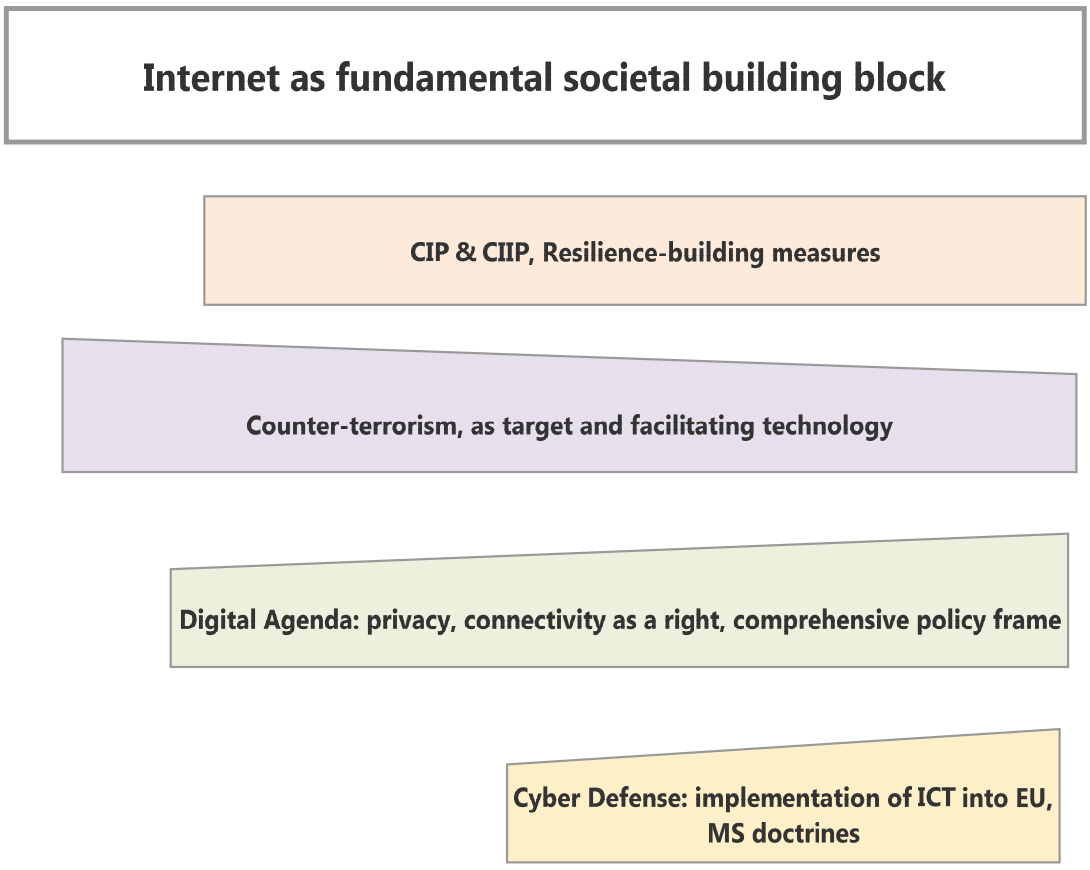

FIGURE 11

The overall narrative is termed *Internet as fundamental societal building block*, simplification that in the view of this thesis puts a fitting label on the EU position. Recalling Figure 5, the argument goes that due to the nature, historical background and natural tendency to incorporate multiple stakeholders, the narrative tends to occupy a "middle ground". This is especially visible in the accommodation of various approaches that are not automatically compatible, but are presented as complementary: Resilience building in CIP, Digital Agenda issues and linking the debate into national as well as international law and human rights and security proper with increasing involvement of CSDP and MS strategic cultures in the cyber realm. The "ethos" of cyberspace also co-constitutes the responses and plays structurally significant role in transferring its inherent values into policy responses.

Yet for matters discussed above in section 3.1 the "comprehensive" approach naturally downplays military force both for reasons of historical reasons (integration as anti-war insurance) and simply the lack of available capabilities. Additionally, one can detect that the policy narrative took in significant input from events which spurred new initiatives and shifts of efforts. Thus counter-terrorism prominence after 2001 fades somewhat only to be sparked in 2005 and later overshadowed by the Estonian "cyberwar" in 2007. Furthermore, there is a gradually rising emphasis on reformation of the Internet governance model by transforming into murkily defined multi-stakeholder process loosely connected to incentives to adopt IPv6. With ICT being not only taken as state of affairs, but actively promoting its use, regulation and development which is bolstered by "fundamental societal building block" narrative one can detect what Der Derian fittingly termed technological *maturity*[115].

[115] (Der Derian 2003)

4. Conclusion

The goal of this thesis was to untangle some of the complex issues in cyber security and ICT in general, provide understanding of a number of key concepts that relate to cyber issues and prepare theoretical and technical ground for analysis of the EU threat framing narrative. It is the position of the author that such thorough preparation was needed since the general problem of the literature that deals with ICT suffers from either being too generally theoretical/strategic or overly technical with the much needed middle ground being rather empty[116]. Thus effort was made to include technical, strategic and sociological perspectives in novel way and provide added value. Moreover, departing from distinctly critical perspective it was the aim to show changes of narratives and provide understanding of how identities inform cognition and the framing of the various shades of cybersecurity issues. It was argued that there is a profound discrepancy between the cluster of "cyber-doom" narratives that have developed since the early 1990s and empirical evidence up till current day. The cases that were analysed and used as real life material to show how threats materialize (section 2.3) are deemed limited in scope. Moreover, the envisioned cascading failure of critical infrastructures due to terrorist or state sponsored attack fortunately remains in the non-case category.

Arguments providing possible explanation for these phenomena revolve around two fundamental lines: over-securitization or hyper-securitization and misunderstanding of the functioning of ICT as such. Without delving into too much detail the first argument sees the penetration of ICT into virtually all aspects of life and thus securitization of everyday life as key dynamic within the rise of cyber security to prominence as well as the failure to be in sync with reality. Furthermore, practical issues of reaching for funds, especially within the financially strenuous sector of security proper/military ICT hardware can provide part of the explanation how has this come about. There are several notions for the misunderstanding strand. It is argued that the particular way in which the Internet has come about and the connectivity at

[116] There are notable exceptions such as the work of Cavelty (2012, 2008a, 2008b), (Hansen, Nissenbaum 2009) or (Eriksson 2001b) cited throughout the thesis.

the expense of security design of the TCP/IP suite have profound effects on the "nature" of the digital sphere. These are predominantly liberal values that promote connectivity as citizens' right, resist centralized governance and have emancipatory effects. Moreover, the mutual vulnerability that is present in the asymmetric world of the Global network does suggest some stabilizing effects in a form of inherent deterrence that precludes disruptive attacks. This is furthered by the efforts of predominantly Western governments to create a normative frame that would solidify these roots into a stronger framework, notably through the Budapest convention on Cybercrime. The research here also draws on the epistemic communities approach to show how shared identities influence cognition of reality and framing of problems – used both in connotation with expert ICT communities and later EU-related communities.

Separate critique goes toward the oft repeated argument of offence-defense advantage where cyber-attacks are perceived as having advantage over cyber-defense. These hinge mostly on the structural effects of interconnectivity and the attribution problem, but omit important aspects that also have profound impacts on this logic. These are especially the uniqueness of vulnerabilities that need to be explored and underestimation of the redundancy that is already in place – which has effects similar to deterrence by denial.

Having completed thorough yet useful analysis of the concepts and modalities within cyber realm the thesis moves on to dissect the framing of cyber threats by the European Union. The methodological framework is compatible with previous analysis in the sense that it departs from the broad securitization camp, but it is mostly section 3 that allows for the deployment of the apparatus developed in section 1.2 on methodology. Particular effort is devoted to pinpoint the interplay between the maturing of European integration including security, ideational and identity factors that inform what is termed EU "comprehensive" approach and the rise in salience of ICT related issues. The analysis shows how cyber related issues penetrate policy making and wider discursive space from multiple directions. The picture we get is a rich landscape where distinct and not necessarily compatible conceptions of cyber

security coexist. These come from the field of Counter-terrorism, Cyber-crime, Cyber-defense Critical Infrastructure Protection and the normative Digital Agenda frame. Cyber security is correspondingly understood through the prism of internal security (crime/terrorism), risk-management (CIP/CIIP) and sovereign security (cyber-defense/CSDP). As in other areas of security the dichotomy between freedom and security reveals itself with tangible discursive struggle that seeks to reconcile indiscriminate connectivity and privacy concerns with the perceived need for robust and safe network.

While it is a necessarily limping analogy one can see similar arguments that were employed in the beginnings of European integration regarding coal and steel production and market regulation being applied within the cyber discourse of current day. If coal and steel were the life blood of then industrial societies it is currently the exchange of digital information that is the life blood of post-industrial Europe and this is reflected in the overall “fundamental societal building block” narrative that one can piece together from current EU discourse.

5. Bibliography

ABLON, Lillian, LIBICKI, Martin C. and GOLAY, Andrea A., 2014, *Markets for Cybercrime Tools and Stolen Data*. Santa Monica.

ADAMS, James, 2001, Virtual Defense. *Foreign Affairs* [online]. 2001. [Accessed 26 April 2014]. Available from: http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense

ADLER, E and HAAS, PM, 1992, Conclusion: epistemic communities, world order, and the creation of a reflective research program. *International organization* [online]. 1992. Vol. 46, no. 1, p. 367–390. [Accessed 4 April 2014]. Available from: http://journals.cambridge.org/production/action/cjoGetFulltext?fulltextid=3216984

ADLER, E., 2008, The Spread of Security Communities: Communities of Practice, Self-Restraint, and NATO's Post--Cold War Transformation. *European Journal of International Relations* [online]. 1 June 2008. Vol. 14, no. 2, p. 195–230. [Accessed 4 April 2014]. DOI 10.1177/1354066108089241. Available from: http://ejt.sagepub.com/cgi/doi/10.1177/1354066108089241

ALEXANDER, Keith B., 2012, An Introduction by General Alexander. *The Next Wave* [online]. 2012. [Accessed 28 April 2014]. Available from: http://www.nsa.gov/research/tnw/tnw194/article2.shtml

AMMORI, Marvin, 2014, The Problem With Obama's Internet Policy. *Foreign Affairs* [online]. 2014. [Accessed 18 June 2014]. Available from: http://www.foreignaffairs.com/articles/141536/marvin-ammori/the-case-for-net-neutrality

ANDERSON, Nate, 2007, Massive DDoS attacks target Estonia; Russia accused. *Ars Technica* [online]. 2007. [Accessed 26 April 2014]. Available from: http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/

ANDERSON, Robert H. and HEARN, Anthony C., 1996, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA "The Day After ... in Cyberspace II."*Santa Monica.

ANDREASSON, Kim J., 2011, *Cybersecurity: Public Sector Threats and Responses* [online]. Boca Raton : CRC Press. [Accessed 25 June 2014]. ISBN 978-1439846636. Available from: http://books.google.com/books?id=isU3ewATX3QC&pgis=1

ARBOR NETWORKS, 2007, DDoS & Security Reports » Estonian DDoS Attacks – A summary to date. [online]. 2007. [Accessed 26 April 2014]. Available from: http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/

ARIN, 2014, ARIN NUMBER RESOURCE POLICY MANUAL. [online]. 2014. [Accessed 12 January 2014]. Available from: https://www.arin.net/policy/nrpm.html#eight3

ARQUILLA, John and RONFELDT, David F., 1995, *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict* [online]. Santa Monica. [Accessed 2 April 2014]. Available from: http://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/cyberwar.html

ARQUILLA, John and RONFELDT, David, 1993, Cyberwar is coming! *Comparative Strategy* [online]. 1993. Vol. 12, no. 2, p. 141–165. [Accessed 2 April 2014]. Available from: http://www.tandfonline.com/doi/abs/10.1080/01495939308402915

ARQUILLA, John, 2011, The Computer Mouse that Roared : Cyberwar in the Twenty-First Century. 2011. Vol. xviii, no. 1, p. 39–49.

ASHTON, Catherine, 2013, *Remarks by EU High Representative Catherine Ashton at press conference on the launch of the EU's Cyber Security Strategy* [online]. Brussels. Available from: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/135287.pdf

BAILES, Alyson J K, DINESEN, René, HAUKKALA, Hiski, JOENNIEMI, Pertti and SPIEGELEIRE, Stephan De, 2011, 05: *The Academia and Foreign Policy Making: Bridging the Gap*. Copenhagen. 2011.

BALZACQ, Thierry, 2010, *Securitization Theory: How Security Problems Emerge and Dissolve* [online]. New York : Routledge. [Accessed 18 June 2014]. ISBN 1135246149. Available from: http://www.google.cz/books?hl=en&lr=&id=ZGmNAgAAQBAJ&pgis=1

BARAN, P, 1960, *On a Distributed Command and Control System Configuration* [online]. Santa Monica. [Accessed 2 April 2014]. Available from: http://www.rand.org/pubs/research_memoranda/RM2632.html

BARD, Alexander and SÖDERQVIST, Jan, 2002, *Netocracy: the new power elite and life after capitalism*. London : Pearson Education. ISBN 1903684293.

BARKER, Keith, 2013, The security implications of IPv6. *Network Security* [online]. June 2013. No. 6, p. 5–9. [Accessed 17 January 2014]. DOI 10.1016/S1353-4858(13)70068-0. Available from: http://linkinghub.elsevier.com/retrieve/pii/S1353485813700680

BETTS, RK, 1997, Should strategic studies survive? *World Politics* [online]. 1997. Vol. 50, no. 1, p. 7–33. [Accessed 28 April 2014]. Available from: http://journals.cambridge.org/abstract_S0043887100014702

BIGO, Didier, 2000, When Two Become One : internal and external securitisations in Europe. In : *International relations theory and the politics of European integration: power, security and community*. London : Routledge. p. 171–205. ISBN 1134611919.

BISCOP, S, HOWORTH, J and GIEGERICH, B, 2009, 27: *Europe: A Time For Strategy*. Brussels.

BOOTH, Ken, 1991, Security and emancipation. *Review of International studies* [online]. 1991. Vol. 17, no. 4, p. 313–326. [Accessed 29 October 2012]. Available from: http://www.jstor.org/stable/10.2307/20097269

BOURDIEU, Pierre, 1999, *Language and symbolic power*. Harvard University Press. ISBN 0674510410.

BRITO, Jerry and WATKINS, Tate, 2011, 11: *Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy* [online]. Fairfax. [Accessed 26 June 2014]. Available from: http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/harvardnsj3&section=4

BRONK, Christopher and TIKK-RINGAS, Eneken, 2013, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict* [online]. [Accessed 28 April 2014]. Available from: http://bakerinstitute.tendenciapp.com/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf

BUMGARNER, John, 2009, *Overview by the UC-CCU of the Cyber Campaign Against Georgia in August of 2008*.

BURES, Oldrich, 2011, *EU Counterterrorism Policy A Paper Tiger?* Burlington : Ashgate. ISBN 9781409411246.

BUZAN, Barry, WÆVER, Ole and WILDE, Jaap De, 1998, *Security: A New Framework For Analysis* [online]. London : Lynne Rienner Publishers. [Accessed 25 October 2012]. ISBN 1555877842. Available from: http://books.google.com/books?hl=en&lr=&id=j4BGr-Elsp8C&pgis=1

CAMPBELL, David, 1990, Global inscription: How foreign policy constitutes the United States. *Alternatives* [online]. 1990. Vol. 15, no. 3, p. 263–286. [Accessed 26 October 2012]. Available from: http://www.jstor.org/stable/10.2307/40644685

CASTELLS, Manuel, 2007, *The Power of Identity* [online]. Second. Oxford, UK : Wiley-Blackwell. ISBN 978-1-4051-9687-1. Available from: http://doi.wiley.com/10.1002/9781444318234

CASTELLS, Manuel, 2010, *The Rise of the Network Society*. 2nd Editio. Chichester : Blackwell Publishing Ltd. ISBN 978-1-4051-9686-4.

CAVELTY, Myriam Dunn, 2008a, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon: Routledge.

CAVELTY, Myriam Dunn, 2008b, Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics* [online]. 2008. Vol. 4, no. 1, p. 19–36. [Accessed 6 May 2013]. DOI 10.1300/J516v04n01. Available from: http://www.tandfonline.com/doi/full/10.1300/J516v04n01_03

CAVELTY, Myriam Dunn, 2012, The militarisation of cyber security as a source of global tension. In : *Strategic Trends 2012* [online]. Zurich : Center for Security Studies, ETH Zurich. ISBN 978-3-905696-36-3. Available from: http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012-Cyber.pdf

CENCETTI, Claudia and MARRONE, Alessandro, 2013, EU and Cyber Security: What's Next? *European Global Strategy* [online]. 2013. [Accessed 25 June 2014]. Available from: http://www.europeanglobalstrategy.eu/nyheter/opinions/eu-and-cyber-security-whats-next

CERF, Vint, 1999, The Internet is for Everyone. *Speech at Computers, Freedom, and Privacy* [online]. 1999. [Accessed 14 April 2014]. Available from: http://www.internetsociety.org/internet-everyone

CERF, Vint, 1998, *I REMEMBER IANA RFC2468* [online]. [Accessed 16 April 2014]. Available from: http://tools.ietf.org/html/rfc2468

COLLINS, Sean and MCCOMBIE, Stephen, 2012, Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism* [online]. April 2012. Vol. 7, no. 1, p. 80–91. [Accessed 27 April 2014]. DOI 10.1080/18335330.2012.653198. Available from: http://www.tandfonline.com/doi/abs/10.1080/18335330.2012.653198

COMISSION OF THE EUROPEAN COMMUNITIES, 2001a, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* [online]. Brussels. Available from: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:52001AE1474&qid=1403898984787

COMISSION OF THE EUROPEAN COMMUNITIES, 2001b, *Network and Information Security: Proposal for A European Policy Approach*. Brussels.

COMISSION OF THE EUROPEAN COMMUNITIES, 2001c, *eEurope 2002, Impact and Priorities, A communication to the Spring European Council in Stockholm*. Brussels.

COMMISSION OF THE EUROPEAN COMMUNITIES, 2005, *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels.

COMMISSION OF THE EUROPEAN COMMUNITIES, 2006a, *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. Brussels.

COMMISSION OF THE EUROPEAN COMMUNITIES, 2006b, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment."*Brussels.

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, 1991, *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C. : National Academy Press.

CONFERENCE OF THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES, 2007, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*. Brussels.

COOK, Colonel James, 2010, "Cyberation" and Just War Doctrine: A Response to Randall Dipert. *Journal of Military Ethics* [online]. December 2010. Vol. 9, no. 4, p. 411–423. [Accessed 27 April 2014]. DOI 10.1080/15027570.2010.536406. Available from: http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536406

CORNISH, P and EDWARDS, Geoffrey, 2005, The strategic culture of the European Union: a progress report. *International Affairs*. 2005. Vol. 81, no. 4, p. 801–820.

COUNCIL OF EUROPE, 1950, *European Convention on Human Rights (as amended)*. Rome.

COUNCIL OF EUROPE, 2001, *Convention on Cybercrime* [online]. Budapest. [Accessed 26 June 2014]. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

COUNCIL OF THE EUROPEAN UNION, 1999, *Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe* [online]. Brussels. [Accessed 27 June 2014]. Available from: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:31999F0364&qid=1403898984787

COUNCIL OF THE EUROPEAN UNION, 2002, *Council framework decision of 13 June 2002 on combating terrorism 2002/475/JHA*. Brussels.

COUNCIL OF THE EUROPEAN UNION, 2008, *Council adopts joint action on a European Union military operation against acts of piracy and armed robbery off the Somali coast*. Brussels.

COUNCIL OF THE EUROPEAN UNION, 2010, *COUNCIL DECISION 2010/96/CFSP of 15 February 2010 on a European Union military mission to contribute to the training of Somali security forces*. Brussels.

COX, R. W., 1981, Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium - Journal of International Studies* [online]. 1 June 1981. Vol. 10, no. 2, p. 126–155. [Accessed 6 October 2012].

DOI 10.1177/03058298810100020501. Available from:
http://mil.sagepub.com/content/10/2/126.extract

CROSS, M. K. D., 2013, The Military Dimension of European Security: An Epistemic Community Approach. *Millennium - Journal of International Studies* [online]. 24 September 2013. Vol. 42, no. 1, p. 45–64. [Accessed 25 March 2014].
DOI 10.1177/0305829813497821. Available from:
http://mil.sagepub.com/cgi/doi/10.1177/0305829813497821

CROSSTON, Matthew D, 2011, World Gone Cyber MAD How " Mutually Assured Debilitation " Is the Best Hope for Cyber Deterrence. *Strategic Studies Quarterly*. 2011. No. Spring, p. 100–116.

DACS, 2014, Data on Armed Conflict and Security. [online]. 2014.
[Accessed 28 April 2014]. Available from: http://www.conflict-data.org/

DAVIS, Paul K, 2014, 1027: *Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy*. Santa Monica. WR.

DEIBERT, R and ROHOZINSKI, R, 2009, Tracking GhostNet: Investigating a cyber espionage network. *Information Warfare Monitor*. 2009. No. JR02, p. 53.

DEIBERT, R. J., ROHOZINSKI, R. and CRETE-NISHIHATA, M., 2012, Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue* [online]. 15 February 2012. Vol. 43, no. 1, p. 3–24. [Accessed 23 March 2014].
DOI 10.1177/0967010611431079. Available from:
http://sdi.sagepub.com/cgi/doi/10.1177/0967010611431079

DEIBERT, RJ and CRETE-NISHIHATA, M, 2012, Global governance and the spread of cyberspace controls. *Global Governance* [online]. 2012. Vol. 18, no. 3, p. 339–361. [Accessed 7 March 2014]. Available from:
http://journals.rienner.com/doi/abs/10.5555/1075-2846-18.3.339

DEIBERT, Ron J., 2003, Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies* [online]. 1 December 2003. Vol. 32, no. 3, p. 501–530. [Accessed 3 April 2013].
DOI 10.1177/03058298030320030801. Available from:
http://mil.sagepub.com/cgi/doi/10.1177/03058298030320030801

DEMIDOV, Oleg and SIMONENKO, Maxim, 2013, Flame in Cyberspace. *Security Index: A Russian Journal on International Security* [online]. March 2013. Vol. 19, no. 1, p. 69–72. [Accessed 28 April 2014]. DOI 10.1080/19934270.2013.757131. Available from:
http://www.tandfonline.com/doi/abs/10.1080/19934270.2013.757131
DER DERIAN, James, 2003, The Question of Information Technology in International Relations. *Millennium - Journal of International Studies* [online]. 1 December 2003. Vol. 32, no. 3, p. 441–456. [Accessed 7 March 2014].

DOI 10.1177/0305829803032003050l. Available from: http://mil.sagepub.com/cgi/doi/10.1177/0305829803032003050l

EARLY, James P., 2009, *An Introduction to IPv6 by James P. Early, Ph.D.* [online]. 2009. Project Advance. Available from: http://www.youtube.com/watch?v=uNb7wd0-jpI

ECONOMIC AND SOCIAL COMITTEE, 2002, *Opinion of the Economic and Social Committee on the "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on network and information security: proposal for a European* [online]. Brussels. [Accessed 27 June 2014]. Available from: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:52001AE1474&qid=1403898984787

ENISA, 2011a, *Cyber Europe 2010 – Evaluation Report*. Heraklion.

ENISA, 2011b, Updated Map (v2.5) of "Digital Fire-brigades"- CERTs — ENISA. [online]. 2011. [Accessed 8 July 2014]. Available from: http://www.enisa.europa.eu/media/news-items/updated-map-of-digital-firebrigade-certs

ENISA, 2011c, World IPv6 Day -8th June; time to take action & switch to the future — ENISA. [online]. 2011. [Accessed 14 January 2014]. Available from: http://www.enisa.europa.eu/media/news-items/world-ipv6-day-8th-june-time-to-take-action-switch-to-the-future
ENISA supports the World IPv6 Day, 8th June, and encourages more companies, authorities and organisations to take action and start using IPv6.

ENISA, 2012, *Cyber Europe 2012 Key Findings and Recommendations*. Athens.

ENISA, 2013, *ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats*. Athens.

ENISA, 2014, National Cyber Security Strategies in the World. [online]. 2014. [Accessed 11 April 2014]. Available from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

ENTMAN, Robert M., 1993, Framing: Toward clarification of a fractured paradigm. *Journal of communication* [online]. 1993. Vol. 43, no. 4, p. 51–58. [Accessed 24 April 2014]. Available from: http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.1993.tb01304.x/full

ERIKSSON, Johan and GIACOMELLO, Giampiero, 2007, *International relations and security in the digital age*. Routledge. ISBN 020396473X.

ERIKSSON, Johan and NOREEN, Erik, 2002, *Setting the agenda of threats: An explanatory model*. Uppsala : Department of Peace and Conflict Research, Uppsala University Uppsala. ISBN 9150616145.

ERIKSSON, Johan, 2001a, Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management* [online]. December 2001. Vol. 9, no. 4, p. 200–210. [Accessed 11 May 2013]. DOI 10.1111/1468-5973.00171. Available from: http://www.blackwell-synergy.com/links/doi/10.1111/1468-5973.00171

ERIKSSON, Johan, 2001b, Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management* [online]. December 2001. Vol. 9, no. 4, p. 200–210. DOI 10.1111/1468-5973.00171. Available from: http://www.blackwell-synergy.com/links/doi/10.1111%2F1468-5973.00171

EU COUNTER-TERRORISM COORDINATOR, 2011, *EU Action Plan on combating terrorism*. Brussels.

EUROPEAN COMMISSION, 2003, *A Secure Europe in a Better World*. Brussels.

EUROPEAN COMMISSION, 2004, *Critical infrastructure protection in the fight against terrorism COM(2004) 702* [online]. Brussels. [Accessed 27 June 2014]. Available from: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm

EUROPEAN COMMISSION, 2005, *The European Union Counter-Terrorism Strategy*. Brussels.

EUROPEAN COMMISSION, 2008, *Report on the implementation of the European Security Strategy and ESDP* [online]. 2008. Brussels. [Accessed 2 June 2013]. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Report+on+the+Implementation+of+the+European+Security+Strategy#6

EUROPEAN COMMISSION, 2009, *Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks an* [online]. Brussels. [Accessed 18 June 2014]. Available from: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST 8375 2009 INIT

EUROPEAN COMMISSION, 2010, *A Digital Agenda for Europe*. Brussels.

EUROPEAN COMMISSION, 2013a, *EU Cybersecurity plan to protect open internet and online freedom and opportunity*. 2013. Brussels : European Comission.
EUROPEAN COMMISSION, 2013b, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels.

EUROPEAN COMMISSION, 2014, *Internet Policy and Governance Europe's role in shaping the future of Internet Governance*. 2014. Brussels : European Comission.

EUROPEAN COMMUNITIES - COUNCIL, 1992, *Treaty On European Union*. Brussels.

EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION, 2004, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*. Brussels.

EUROPEAN PARLIAMENT, 2012, *Motion for a resolution on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP))*. Brussels.

EUROPEAN UNION and COUNCIL OF EUROPE, 2007, *Memorandum of Understanding between the Council of Europe and the European Union* [online].
[Accessed 26 June 2014]. Available from: http://www.coe.int/t/der/docs/MoU_EN.pdf

EUROPEAN UNION, 2000, *Standard Eurobarometer 54*. Brussels.

EUROPEAN UNION, 2010, When an international crisis occurs, European Union member states should agree a common position. *Eurobarometer surveys* [online]. 2010. [Accessed 1 July 2014]. Available from: http://ec.europa.eu/public_opinion/cf/showchart_line.cfm?keyID=2258&nationID=11,1,27,28,17,2,16,18,13,6,3,4,22,7,8,20,21,9,23,31,24,12,19,29,26,25,5,14,10,30,15,&startdate=2003.11&enddate=2005.06#fcExportDiv

EUROPEAN UNION, 2013, *Standard Eurobarometer 80 - Media Use in the European Union*. Brussels.

EUROPOL, 2014, A collective EU response to cybercrime. [online]. 2014.
[Accessed 1 July 2014]. Available from: https://www.europol.europa.eu/ec3

FALLIERE, Nicolas, MURCHU, Liam O and CHIEN, Eric, 2011, *W32 . Stuxnet Dossier*. Cupertino.

FARIVAR, Cyrus, 2009, A Brief Examination of Media Coverage of Cyberattacks (2007-Present). In : *The Virtual Battlefield: Perspectives on Cyber warfare*. Ios Press. p. 182–188. ISBN 978-1-60750-060-5.

FARWELL, James P. and ROHOZINSKI, Rafal, 2011, Stuxnet and the Future of Cyber War. *Survival* [online]. February 2011. Vol. 53, no. 1, p. 23–40.
[Accessed 27 March 2014]. DOI 10.1080/00396338.2011.555586. Available from: http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586
FIALA, Petr and PITROVÁ, Markéta, 2009, *Evropská unie* [online]. Brno : Centrum pro studium demokracie a kultury. [Accessed 23 June 2014]. ISBN 8073251809. Available from: http://books.google.com/books?id=5T87uAAACAAJ&pgis=1

FOUCAULT, Michel, 1994, *The Order of Things: An Archaeology of the Human Sciences* [online]. Random House. [Accessed 9 April 2014]. ISBN 0-679-75335-4. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Order+of+Things:+An+Archaeology+of+the+Human+Sciences#0

FRIEDMAN, Thomas L, 2006, *The world is flat: A brief history of the twenty-first century*. 1st update. New York : Farrar, Straus and Giroux. ISBN 0-374-29279-5.

FUREDI, Frank, 2008, Fear and Security: A Vulnerability-led Policy Response. *Social Policy & Administration* [online]. December 2008. Vol. 42, no. 6, p. 645–661. [Accessed 4 April 2014]. DOI 10.1111/j.1467-9515.2008.00629.x. Available from: http://doi.wiley.com/10.1111/j.1467-9515.2008.00629.x

GEERS, Kenneth, 2010, Live Fire Exercise: Preparing for Cyber War. *Journal of Homeland Security and Emergency Management* [online]. 2010. Vol. 7, no. 1. [Accessed 27 May 2013]. Available from: http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1780/jhsem.2010.7.1.1780.xml

GEERS, Kenneth, 2011, *Strategic cyber security* [online]. Tallinn : CCD COE Publication. [Accessed 25 April 2013]. ISBN 9789949904051. Available from: http://books.google.com/books?hl=en&lr=&id=4h6KIDAfGhAC&oi=fnd&pg=PA9&dq=Strategic+Cyber+Security&ots=sUl23FeiED&sig=sztDn3KPQMgrzSeo3iCQ1xqQKqs

GOLDBLAT, Josef, 2002, *Arms control* [online]. London : SAGE Publications. [Accessed 29 November 2013]. ISBN 0 7619 4015 4. Available from: http://media.matthewsbooks.com.s3.amazonaws.com/documents/tocwork/076/9780761940166.pdf

GOOGLE, 2014a, IPv6 – Google Statistics. [online]. 2014. [Accessed 16 April 2014]. Available from: http://www.google.com/ipv6/statistics.html#tab=ipv6-adoption

GOOGLE, 2014b, Take Action - Google. [online]. 2014. [Accessed 19 April 2014]. Available from: https://www.google.com/takeaction/

GRAHAM, James, OLSON, Ryan and HOWARD, Rick, 2011, *Cyber security essentials* [online]. Boca Raton : CRC Press. [Accessed 25 April 2014]. ISBN 9781439851265. Available from: http://books.google.com/books?hl=en&lr=&id=hu4bJo5v3dsC&oi=fnd&pg=PP1&dq=Cyber+Security+Essentials&ots=VmXjD4VOgC&sig=Bwgw9ZLqqRt0zsE8if2mbEk4r4A

GRENDA, Bogdan, 2013, Cyber Security of NATO Air Operations. In : *NATO Towards the Challenges of a Contemporary World 2013* [online]. Warsaw : Instytut Badań nad Stosunkami Międzynarodowymi w Warszawie (International Relations Research

Institute in Warsaw). p. 316. [Accessed 26 April 2014]. ISBN 8362784032. Available from: http://books.google.com/books?id=rgCPAgAAQBAJ&pgis=1

HALL, Camilla and BLAS, Javier, 2012, Aramco cyber attack targeted production - FT.com. *Financial Times* [online]. 2012. [Accessed 28 April 2014]. Available from: http://www.ft.com/intl/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html#axzz30Bm8uTBD

HANSEN, L., 2000, The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. *Millennium - Journal of International Studies* [online]. 1 June 2000. Vol. 29, no. 2, p. 285–306. [Accessed 26 October 2012]. DOI 10.1177/03058298000290020501. Available from: http://mil.sagepub.com/cgi/doi/10.1177/03058298000290020501

HANSEN, L., 2011, Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis. *European Journal of International Relations* [online]. 19 January 2011. Vol. 17, no. 1, p. 51–74. [Accessed 28 October 2012]. DOI 10.1177/1354066110388593. Available from: http://ejt.sagepub.com/cgi/doi/10.1177/1354066110388593

HANSEN, Lene and NISSENBAUM, Helen, 2009, Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly* [online]. 2009. Vol. 53, p. 1155–1175. [Accessed 28 October 2012]. Available from: http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/full

HERZOG, Stephen, 2011, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*. 2011. Vol. 4, no. 2, p. 49–60.

HOLLIS, DM, 2011, Cyberwar case study: Georgia 2008. *Small Wars Journal* [online]. 2011. No. January. [Accessed 28 April 2014]. Available from: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

HOWORTH, Jolyon, 2010, The EU as a Global Actor : Grand Strategy for a Global Grand Bargain ? *Journal of Common Market Studies* [online]. 4 May 2010. Vol. 48, no. 3, p. 455–474. DOI 10.1111/j.1468-5965.2010.02060.x. Available from: http://doi.wiley.com/10.1111/j.1468-5965.2010.02060.x

HUGHES, Rex, 2010, A treaty for cyberspace. *International Affairs* [online]. March 2010. Vol. 86, no. 2, p. 523–541. DOI 10.1111/j.1468-2346.2010.00894.x. Available from: http://doi.wiley.com/10.1111/j.1468-2346.2010.00894.x

HUSTON, Geoff, 2005, Opinion: ICANN, the ITU, WSIS, and Internet Governance. *The Internet Protocol Journal* [online]. 2005. Vol. 8, no. 1. [Accessed 17 April 2014]. Available from:

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-1/internet_governance.html

HUSTON, Geoff, 2013, Valuing IP Addresses. *RIPE Labs* [online]. 2013. [Accessed 12 January 2014]. Available from: https://labs.ripe.net/Members/gih/valuing-ip-addresses

HUYSMANS, J., 1998, Revisiting Copenhagen:: Or, On the Creative Development of a Security Studies Agenda in Europe. *European Journal of International Relations* [online]. 1 December 1998. Vol. 4, no. 4, p. 479–505. [Accessed 4 April 2014]. DOI 10.1177/1354066198004004004. Available from: http://ejt.sagepub.com/cgi/doi/10.1177/1354066198004004004

HYNEK, Nikola, 2008, Conditions of emergence and their (bio)political effects: political rationalities, governmental programmes and technologies of power in the landmine case. *Journal of International Relations and Development* [online]. June 2008. Vol. 11, no. 2, p. 93–120. [Accessed 5 December 2013]. DOI 10.1057/jird.2008.5. Available from: http://www.palgrave-journals.com/doifinder/10.1057/jird.2008.5

IAEA, 2013, *Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran GOV/2013/27*. Vienna.

IBM, 1958, *The SAGE/BOMARC Air Defense Weapons System*. New York.

ICANN, 1998, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers. [online]. 1998. [Accessed 16 April 2014]. Available from: http://www.icann.org/en/about/governance/articles

ICANN, 2011, Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied. *Press Release* [online]. 2011. [Accessed 10 January 2014]. Available from: http://www.icann.org/en/news/press/releases/release-03feb11-en.pdf

ICANN, 2014, Welcome to WHOIS | WHOIS. [online]. 2014. [Accessed 17 April 2014]. Available from: http://whois.icann.org/

ICRC, 1949, The Geneva Conventions of 12 August 1949. [online]. 1949. [Accessed 11 April 2014]. Available from: http://www.icrc.org/eng/assets/files/publications/icrc-002-0173.pdf

IEEE-USA, 2009, *Next Generation Internet : IPv4 Address Exhaustion , Mitigation Strategies and Implications for the U . S .* [online]. Available from: http://www.ieeeusa.org/policy/whitepapers/IEEEUSAWP-IPv62009.pdf

IETF, 2014, Mission Statement. [online]. 2014. [Accessed 17 April 2014]. Available from: http://www.ietf.org/about/mission.html

INFOSECURITY, 2013, Red October cyber-espionage campaign used highly sophisticated infiltration techniques. [online]. 2013. [Accessed 28 April 2014]. Available from: http://www.infosecurity-magazine.com/view/30551/red-october-cyberespionage-campaign-used-highly-sophisticated-infiltration-techniques/

INKSTER, Nigel, 2013, Chinese Intelligence in the Cyber Age. *Survival* [online]. March 2013. Vol. 55, no. 1, p. 45–66. [Accessed 28 April 2014]. DOI 10.1080/00396338.2013.767405. Available from: http://www.tandfonline.com/doi/abs/10.1080/00396338.2013.767405

INTERNATIONAL INSTITUE FOR STRATEGIC STUDIES, 2014, Armed Conflict Database. [online]. 2014. [Accessed 25 April 2014]. Available from: https://acd.iiss.org/
ISIS EUROPE, 2014, Mission Chart | CSDP MAP. *Mission Chart* [online]. 2014. [Accessed 23 June 2014]. Available from: http://www.csdpmap.eu/mission-chart

ITU, 2003, *WSIS: Declaration of Principles* [online]. Geneva. [Accessed 21 April 2014]. Available from: http://www.itu.int/wsis/docs/geneva/official/dop.html

ITU, 2014a, World Conference on International Telecommunications (WCIT-12). [online]. 2014. [Accessed 19 April 2014]. Available from: http://www.itu.int/en/wcit-12/Pages/default.aspx

ITU, 2014b, World Summit on the Information Society. [online]. 2014. [Accessed 19 April 2014]. Available from: https://www.itu.int/wsis/index.html

JOHNSTON, Alastair Iain, 1995, Thinking about strategic culture. *International security* [online]. 1995. Vol. 19, no. 4, p. 32–64. [Accessed 22 June 2014]. Available from: http://www.jstor.org/stable/2539119

JOUBERT, Vincent, 2010, Getting the essence of cyberspace: a theoretical framework to face cyber issues. In : *Conference on Cyber Conflict Proceeding*. Tallinn : CCD COE Publication. 2010. p. 111–125.

JOUBERT, Vincent, 2012, *Five years after Estonia's cyber attacks: lessons learned for NATO?* Rome.

KAHN, Herman, 2007, *On thermonuclear war*. Princeton : Cambridge University Press. ISBN 978-1-4128-0664-0.

KASPERSKY LAB, 2012, Flame Cyber Weapon Facts. [online]. 2012. [Accessed 28 April 2014]. Available from: http://usa.kaspersky.com/flame

KASPERSKY LAB, 2013, "Red October" Diplomatic Cyber Attacks Investigation. *Secure List* [online]. 2013. [Accessed 25 April 2014]. Available from: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation

KIKK, Eneken, KASKA, Kadri and VIHUL, Liis, 2010, *International cyber incidents: Legal considerations* [online]. Tallinn : Cooperative Cyber Defence Centre of Excellence. [Accessed 25 April 2014]. ISBN 9789949904006. Available from: http://www.ccdcoe.org/231.html

KINGDON, John W., 2003, *Agendas, alternatives, and public policies* [online]. 2nd. New York : Longman. [Accessed 31 May 2013]. ISBN 0321121856. Available from: http://books.google.com/books?id=hSolAQAAIAAJ&pgis=1

KISH, John and TURNS, David, 1995, *International law and espionage*. The Hague : Kluwer Law International. ISBN 904110030X.

KITA, C.I., 2003, J.C.R. Licklider's vision for the IPTO. *IEEE Annals of the History of Computing* [online]. 2003. Vol. 25, no. 3, p. 62–77. DOI 10.1109/MAHC.2003.1226656. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1226656

KLEINROCK, Leonard, 1962, *Message delay in communication nets with storage* [online]. Massachusets Institute of Technology. [Accessed 8 April 2014]. Available from: http://dspace.mit.edu/handle/1721.1/11562

KROES, Neelie, 2014, *The Internet needs better governance, starting now - Speech at NetMundial*. 2014. Brussels : European Comission.

LANGNER, Ralph, 2011, Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE* [online]. 2011. No. June, p. 49–51. [Accessed 27 April 2014]. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5772960

LAWSON, Sean, 2011, 10: *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History* [online]. Fairfax. [Accessed 26 June 2014]. Available from: http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history.pdf

LIBICKI, Martin C., 2009, *Cyberdeterrence and cyberwar* [online]. Santa Monica : Rand Corporation. ISBN 9780833047342.

LIBICKI, Martin C., 2013, Tangled Web: Cyberwar Fears Pose Dangers of Unnecessary Escalation. *RAND Review* [online]. 2013. [Accessed 9 April 2014]. Available from: http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html

LUCCHI, N, 2011, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *Cardozo J. Int'l & Comp. L.* Vol. 19, p. 645–678.

MANDIANT, 2013a, *APT1 Exposing One Of China's Espionage Units*. Alexandria.

MANDIANT, 2013b, Mandiant Intelligence Center Report. [online]. 2013. [Accessed 28 April 2014]. Available from: http://intelreport.mandiant.com/

MANJIKIAN, Mary McEvoy, 2010, From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* [online]. 7 June 2010. Vol. 54, no. 2, p. 381–401. DOI 10.1111/j.1468-2478.2010.00592.x. Available from: http://doi.wiley.com/10.1111/j.1468-2478.2010.00592.x

MASLOW, Abraham H, 2004, *The psychology of science: A reconnaissance*. Richmond : Maurice Bassett. ISBN 0976040239.

MEARES, Mary M and FUKUMOTO, Akiko, 2010, When Disaster Doesn't Strike : Reframing Y2K Coverage in Japan and the United States. *The Northwest Journal of Communication*. 2010. Vol. 39, no. 1, p. 17.

MENN, Joseph, 2014, U.S. government aims to shed control of Internet addresses. *Reuters* [online]. 2014. [Accessed 18 April 2014]. Available from: http://www.reuters.com/article/2014/03/15/us-usa-internet-domainnames-idUSBREA2D1YH20140315

MÉRAND, Frédéric, 2010, Pierre Bourdieu and the Birth of European Defense. *Security Studies*. 21 May 2010. Vol. 19, no. 2, p. 342–374. DOI 10.1080/09636411003795780.

MEYER, Christoph and STRICKMANN, Eva, 2011, Solidifying constructivism: how material and ideational factors interact in European defence. *Journal of Common Market Studies*. 2011. Vol. 49, no. 1, p. 61–81.

MICHAELS, Jim, 2007, NATO to study defense against cyberattacks. *USA Today* [online]. 2007. [Accessed 26 April 2014]. Available from: http://usatoday30.usatoday.com/printedition/news/20070615/a_nato15.art.htm

MITRA, A. and WATTS, E., 2002, Theorizing Cyberspace: the Idea of Voice Applied to the Internet Discourse. *New Media & Society* [online]. 1 December 2002. Vol. 4, no. 4, p. 479–498. [Accessed 14 April 2014]. DOI 10.1177/146144402321466778. Available from: http://nms.sagepub.com/cgi/doi/10.1177/146144402321466778

MUELLER, ML, 2010, *Networks and states: The global politics of Internet governance* [online]. Cambridge : MIT Press. ISBN 9780262014595.

MUTIMER, David, 2007, Beyond strategy: Critical thinking and the new security studies. In : *Conference Papers -- International Studies Association*. EBSCOhost. 2007. p. 118–151.

NACHENBERG, Carey, 2012, Dissecting Stuxnet. *Center for International Security and Cooperation seminar - Stanford University* [online]. 2012. [Accessed 27 April 2014]. Available from: http://www.youtube.com/watch?v=DDH4m6M-ZIU

NARTEN, Thomas, THOMSON, Susan and JINMEI, Tatuya, 2007, *IPv6 Stateless Address Autoconfiguration RFC4862* [online]. 2007. Network Working Group. [Accessed 20 April 2014]. Available from: http://tools.ietf.org/html/rfc4862

NET MUNDIAL, 2014, Roadmap for the future evolution of the Internet governance. [online]. 2014. [Accessed 23 April 2014]. Available from: http://document.netmundial.br/2-roadmap-for-the-future-evolution-of-the-internet-governance/

OPTEM, 2006, *The European Citizens and the Future of Europe - Qualitative Study in the 25 Member States*. Gambais.

PAGET, Francois, 2012, *Hacktivism* [online]. Available from: http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf

PAWLAK, Patryk, 2013, *Cyber world : site under construction* [online]. Paris. Available from: http://www.iss.europa.eu/uploads/media/Brief_32.pdf

PERLROTH, Nicole, 2012, Cyberattack on Saudi Oil Firm Disquiets U.S. - NYTimes.com. *The New York Times* [online]. 2012. [Accessed 28 April 2014]. Available from: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

PETERSON, Dale, 2013, Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies* [online]. 2013. Vol. 36, no. 1, p. 120–124. [Accessed 27 April 2014]. Available from: http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.742014

POTZSCH, H., 2013, The emergence of iWar: Changing practices and perceptions of military engagement in a digital era. *New Media & Society* [online]. 16 December 2013. No. December, p. 1461444813516834–. [Accessed 14 April 2014]. DOI 10.1177/1461444813516834. Available from: http://nms.sagepub.com/content/early/2013/12/15/1461444813516834.abstract The present article investigates the influences

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE, 1997, *Critical Foundations: Protecting America's Infrastructures*. Washington, D.C.

PRICE, Richard and TANNENWALD, Nina, 1996, The Nuclear and Chemical Weapons Taboos. In : *The Culture of National Security: Norms and Identity in World Politics*. New York : Columbia University Press. p. 114–152. ISBN 0231104693.

PRINCEN, Sebastiaan and RHINARD, Mark, 2006, Crashing and creeping: agenda-setting dynamics in the European Union. *Journal of European Public Policy* [online]. September

2006. Vol. 13, no. 7, p. 1119–1132. [Accessed 30 May 2013]. DOI 10.1080/13501760600924233. Available from: http://dx.doi.org/10.1080/13501760600924233

PRINCEN, Sebastiaan, 2009, *Agenda-setting in the European Union* [online]. Basingstoke : Palgrave Macmillan. [Accessed 29 May 2013]. ISBN 0230220533. Available from: http://books.google.com/books?id=QK4bAQAAMAAJ&pgis=1

REED, Thomas, 2007, *At the Abyss: An Insider's History of the Cold War* [online]. Random House. [Accessed 2 April 2014]. ISBN 0307414620. Available from: http://www.amazon.com/At-Abyss-Insiders-History-Cold/dp/0891418377

RID, Thomas, 2012, Cyber war will not take place. *Journal of strategic studies* [online]. 2012. Vol. 35, no. April. [Accessed 31 May 2013]. Available from: http://books.google.com/books?id=hSolAQAAIAAJ&pgis=1

RILEY, Michael and ENGLEMAN, Eric, 2012, Code in Aramco Cyber Attack Indicates Lone Perpetrator. *Bloomberg* [online]. 2012. [Accessed 28 April 2014]. Available from: http://www.bloomberg.com/news/2012-10-25/code-in-aramco-cyber-attack-indicates-lone-perpetrator.html

RISSE, Thomas, 2012, Identity Matters: Exploring the Ambivalence of EU Foreign Policy. *Global Policy* [online]. 8 December 2012. Vol. 3, no. December, p. 87–95. [Accessed 1 July 2014]. DOI 10.1111/1758-5899.12019. Available from: http://doi.wiley.com/10.1111/1758-5899.12019

ROBINSON, N, WALCZAK, A and BRUNE, SC, 2013, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)* [online]. Santa Monica. [Accessed 7 March 2014]. Available from: http://www.rand.org/pubs/research_reports/RR286.html

ROGERS, James, 2009, From "Civilian Power" to "Global Power": Explicating the European Union's "Grand Strategy" Through the Articulation of Discourse Theory. *Journal of Common Market Studies*. September 2009. Vol. 47, no. 4, p. 831–862. DOI 10.1111/j.1468-5965.2009.02007.x.

ROSENZWEIG, Paul, 2014, U.S. Gives Up IANA and DNS Control via ICANN. *New Republic* [online]. 2014. [Accessed 17 April 2014]. Available from: http://www.newrepublic.com/article/117037/us-gives-iana-and-dns-control-icann

ROZSYPAL, Jakub, 2014, Updating the global network through IPv6. *POST* [online]. 2014. [Accessed 10 April 2014]. Available from: http://postnito.cz/?p=4972

RYAN, Johnny, 2010, *A History of the Internet and the Digital Future*. London : Reaktion books. ISBN 978 1 86189 777 0.

SALMON, Trevor C, 1992, Testing times for European political cooperation: the Gulf and Yugoslavia, 1990-1992. *International Affairs*. 1992. Vol. 68, no. 2, p. 233–253.

SAMSON, Ted, 2006, Critics clash over Cybercrime Convention. *Infoworld.com* [online]. 2006. [Accessed 27 June 2014]. Available from: http://www.infoworld.com/t/security/critics-clash-over-cybercrime-convention-084

SANGER, David E, 2012, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York : Crown. ISBN 978-0-307-71804-4.

SAUDI ARAMCO, 2014, At a glance. [online]. 2014. [Accessed 28 April 2014]. Available from: http://www.saudiaramco.com/en/home.html#our-company%7C%2Fen%2Fhome%2Four-company%2Fat-a-glance.baseajax.html

SCHMITT, Michael N, 2012, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*. 2012. Vol. 54, no. December.

SCHMITT, Michael N, 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge : Cambridge University Press. ISBN 1107024439.
SMITH, Karen E., 2008, *European Union Foreign Policy in a Changing World*. New York : Wiley. ISBN 0745640184.

SMITH, Michael E., 2004, Institutionalization, Policy Adaptation and European Foreign Policy Cooperation. *European Journal of International Relations* [online]. 1 March 2004. Vol. 10, no. 1, p. 95–136. [Accessed 4 April 2014]. DOI 10.1177/1354066104040570. Available from: http://ejt.sagepub.com/cgi/doi/10.1177/1354066104040570

SMITH, Michael E., 2011, A liberal grand strategy in a realist world? Power, purpose and the EU's changing global role. *Journal of European Public Policy* [online]. March 2011. Vol. 18, no. 2, p. 144–163. [Accessed 31 May 2014]. DOI 10.1080/13501763.2011.544487. Available from: http://www.tandfonline.com/doi/abs/10.1080/13501763.2011.544487

SNOW, David A and BENFORD, Robert D, 1988, Ideology, frame resonance, and participant mobilization. *International social movement research*. 1988. Vol. 1, no. 1, p. 197–217.

SNOW, David A and BENFORD, Robert D, 1992, Master frames and cycles of protest. In : *Frontiers in social movement theory*. New Have : Yale University Press. p. 133–155.

SOCOR, Vladimir, 2007, Moscow Stung by Estonian Ban on Totalitarianism's Symbols. *Eurasia Daily Monitor* [online]. 2007. [Accessed 25 April 2014]. Available from: http://www.jamestown.org/programs/edm/single/?tx_ttnews[tt_news]=32427&tx_ttnews[backPid]=171&no_cache=1

STEVENS, Tim, 2012a, Norms, Epistemic Communities and the Global Cyber Security Assemblage. *E-IR* [online]. 2012. [Accessed 4 April 2014]. Available from: http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage/

STEVENS, Tim, 2012b, A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. 2012. Vol. 33, no. 1, p. 148–170. DOI http://dx.doi.org/10.1080/13523260.2012.659597.

STONE, John, 2013, Cyber War Will Take Place! *Journal of Strategic Studies* [online]. 2013. Vol. 36, no. April, p. 101–108. [Accessed 17 April 2014]. Available from: http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.730485

SYVERSON, Paul, TSUDIK, Gene, REED, Michael and LANDWEHR, Carl, 2001, Towards an analysis of onion routing security. In : *Designing Privacy Enhancing Technologies*. Springer. 2001. p. 96–114. ISBN 3540417249.

TANNENWALD, Nina, 2008, *The Nuclear Taboo:The United States And the Non Use Nuclear Weapons Since 1945*. New York : Cambridge University Press. ISBN 9780521524285.

THOMAS, Timothy L., 2000, Manipulating The Mass Consciousness: Russian And Chechen "Information War" Tactics In The 2nd Chechen-Russian Conflict. In : *The second Chechen War* [online]. Shrivenham : Strategic and Combat Studies Institute. p. 168. [Accessed 28 April 2014]. ISBN 9781874346326. Available from: http://fmso.leavenworth.army.mil/documents/chechiw.htm

TZU, Sun, 2010, *On The Art of War*. Aziloth Books. ISBN 978-1907523175.
UNITED NATIONS OFFICE ON CRIME AND DRUGS, 2013, *Comprehensive Study on Cybercrime*. New York.

UNITED NATIONS, 1945, *Charter of the United Nations and Statute of the International Court of Justice*. 1945. San Francisco.

UPPSALA CONFLICT DATA PROGRAM, 2014, Database - Uppsala Conflict Data Program (UCDP). *Conflict Encyclopedia* [online]. 2014. [Accessed 28 April 2014]. Available from: http://www.ucdp.uu.se/gpdatabase/search.php

WALKER, R. B. J., 1990, Security, Sovereignty, and the Challenge of World Politics. *Alternatives: Global, Local, Political* [online]. 1 January 1990. Vol. 15, no. 1, p. 3–27. [Accessed 25 October 2012]. DOI 10.1177/030437549001500102. Available from: http://alt.sagepub.com/content/15/1/3.extract
WALL, David, 2008, Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology*. 2008. Vol. 22, no. July, p. 45–63.

WALT, SM, 1985, Alliance formation and the balance of world power. *International Security* [online]. 1985. Vol. 9, no. 4, p. 3–43. [Accessed 29 October 2012]. Available from: http://www.jstor.org/stable/10.2307/2538540

WALT, SM, 1990, *The Origins of Alliance*. Ithaca : Cornell University Press. ISBN 978-0801494185.

WEBER, Max, 2004, *The Vocation Lectures*. Indianapolis : Hackett Publishing Company. ISBN 0872206661.

WEBSENSE, 2014, *2014 Security Predictions*.

WEITZENBOECK, E. M., 2014, Hybrid net: the regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology* [online]. 8 January 2014. Vol. 22, no. 1, p. 49–73. [Accessed 12 April 2014]. DOI 10.1093/ijlit/eat016. Available from: http://ijlit.oxfordjournals.org/cgi/doi/10.1093/ijlit/eat016

WENGER, Andreas, ABELE-WIGERT, I and DUNN, Myriam, 2006, *International CIIP Handbook 2006* [online]. Zurich : Center for Security Studies. [Accessed 23 April 2014]. Available from: http://kms1.isn.ethz.ch/serviceengine/Files/ISN/16156/ipublicationdocument_singledocument/64e1b764-023d-47ea-bc4d-449215d016b7/en/CIIP_HB_06_Vol.1.pdf

WESTERN EUROPEAN UNION COUNCIL OF MINISTERS, 1992, *Petersberg Declaration* [online]. Bonn. [Accessed 26 June 2014]. Available from: http://www.weu.int/documents/920619peten.pdf

WESTIN, Ken, 2012, The Four Horsemen of the Cyber-Apocalypse: Security Software FUD. *Tripwire* [online]. 2012. [Accessed 25 April 2014]. Available from: http://www.tripwire.com/state-of-security/off-topic/the-four-horsemen-of-the-cyber-apocalypse-fud-in-security-software-marketing/

WILLIAMS, MC, 2003, Words, images, enemies: securitization and international politics. *International Studies Quarterly* [online]. 2003. Vol. 47, no. 4, p. 511–531. [Accessed 4 April 2014]. DOI 10.1046/j.0020-8833.2003.00277.x. Available from: http://onlinelibrary.wiley.com/doi/10.1046/j.0020-8833.2003.00277.x/full

WILNER, Alex S., 2011, Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. *Journal of Strategic Studies* [online]. February 2011. Vol. 34, no. 1, p. 3–37. [Accessed 7 July 2014]. DOI 10.1080/01402390.2011.541760. Available from: http://dx.doi.org/10.1080/01402390.2011.541760

ZICCARDI, Giovanni, 2012, *Resistance , Liberation Technology and Human Rights in the Digital Age*. Dordrecht : Springer. ISBN 978-94-007-5276-4.