National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

INTERNATIONAL TEAMWORK ON CYBER THREATS

Maj O. Lotze

JCSP 41

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 41

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

INTERNATIONAL TEAMWORK ON CYBER THREATS

Maj O. Lotze

Word Count: 5041

Compte de mots : 5041

INTRODUCTION

Recent dynamics and events in the cyber domain always spark new discussions about the effectiveness of anti-cyber-attack procedures and capabilities in order to face these raising threats towards industrial cooperation, nations and populations. The attack on the French news channel TV5 and its blocking of their broadcasting capabilities on April 8th, 2015 claimed by ISIS affiliates, the attacks against the media concern Sony on November 24th 2014 and the stealing of data by perhaps a North Korean Group as well as older events like the Stuxnet attacks in September 2010 conducted by an suspected Israeli group show the relevance towards today's security concerns by the people and their governments. The increased use of the internet with its global networking of daily life, industrial connectivity of supply chains and ideas as well as the international communication on the private and public sector increase the need for rules and procedures in the case of misuse, thread and manipulation. All digital connected countries with each of its state and non-state actors are looking for appropriate circumstances of rules and regulations in order to defend their interest and achieve their respective goals on the private, economic and political level. Different countries have different geostrategic approaches and interests as well as different understandings of topics like cyber security, Internet governance or data protection. In today's world and its interconnectivity on the digital level, these fundamental differences can lead to misunderstandings, mistrust and contra productive efforts towards originally common goals. This paper will lay out the different approaches by the United States of America (US) and the European Union

(EU), with selected views on German and Canadian involvements, towards the topics of cyber security, Internet governance and data protection. The issues on international synchronization of efforts under the influence of national policies and goals as well as different understandings and approaches towards these topics are in the focus of this paper.

The first part will lay out the current situation, frameworks and international normative foundations in which cyber operations take place and which limits occur. The description of the current international multi-stakeholder model, specific national program debates in the US and the EU on the topic, the Budapest convention and its regulations on cybercrime as well as the military approach in the frame of the Tallinn manual will be matter of discussion. The second part will focus on current approaches by the US and the EU on countering cyber threads and it will discuss the implications of an offensive (US) versus a defensive approach (EU). Capacity building and specific topics like critical infrastructure protection and data protection will be matter of discussion. The final part will be the argumentation towards future US-EU relations in the cyber domain and the outlook towards future engagements and cooperation.

This essay will argue how the international cooperation in the cyber domain can be more effective by

a) the recognition of the international actors US and EU as equal partners,

b) the rebuilding of cooperative trust in order to achieve better effects in countering international cyber-threats for economies and private persons,

c) improving transparency on national and international cyber operations in order to promote trust in capabilities to counter cyber-threats,

d) the inclusion of unpopular partners in the cyber domain like Russia and China and finally

e) the improvement of cyber domain importance in international relations and in global environments.

NORMATIVE FOUNDATIONS OF GLOBAL CYBER OPERATIONS

The understanding of common normative foundations like the digital world as public space and as economic resource on the cyber domain were shared and developed in the US and the EU and reinforced as well as increasingly established in the last years.[1] This part will focus on international understanding of the cyber domain and the views towards this domain as well as current ongoing debates in the US and the EU. Furthermore, this part will describe the most common foundations of the Budapest convention and the Tallinn manual for civil and military approaches towards this topic.

INTERNATIONAL UNDERSTANDING

The international communities of states, regions, non-state actors as well as ordinary people are users, dependents and influencers of the digital world. The free

[1] German Journal of the Ministry of Defence 1/2014, *Cyber-Security – a review*, last accessed: 12 April 2015, http://www.hardthoehenkurier.de/emag/free/2014-01/index.html#/18/.

access and usage of these assets are acknowledged in the "western" world as everyone's right. In order to facilitate communication, trade and public services like health care, energy and transportation, stable and resilient networks have to be established and maintained.[2] The last years showed strong increases of international usage in the digital domain by the use of the Internet and its related increase of broadband capabilities worldwide. Especially developing countries record huge growths.[3] These increases of usage and users could also increase the number of misuse, criminal activity and on the far end of the scale, physical threats and harm to others. The international community, in our case especially US and EU official organizations, recognize the free usage of digital capabilities as a collective good for free and undisturbed usage.[4] International organizations like the Working Group on Internet Governance (WGIG) were established after conflicts between the US and China between 2002 and 2005 on Internet administration issues occurred on the case whether private businesses or public authorities should control and manage them.[5] These organizations, especially in the frame of the WGIG, can be recognized as a multi-stakeholder model in which its participants agreed on the understanding of digital domains like the Internet as public space without a central governing authority

---

[2] German Ministry of Domestic Affairs, *Cyber-Security Strategy for Germany*, last accessed: 12 April 2015, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

[3] International Telecommunication Union (ITU), *Facts and Figures. The World in 2014*, last accessed: 12 April 2015, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

[4] Freedom House, *Freedom of the Net 2014*, last accessed: 12 April 2015, https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

[5] In 2005, 190 Countries agreed on the terms under the Chair of Kofi Annan. The WGIG established regulatory bodies like the Internet Society (ISOC), Internet Engineering Task Force (IETF) or the Internet Governance Forum (IGF).

and a product of interaction between all aspects of global societies.[6] These proposed structures and (non-)management approaches are in favor of the group of "western" communities like the US, EU or Canada and in contrary to thoughts and methods of authoritarian systems like Russia or China. The next part will focus on specific US and EU initiatives in order to facilitate unlimited Internet access especially in crisis regions and domestic markets.

SPECIFIC US AND EU PROGRAM DEBATES

In the period between 2009 and 2014 several US and EU bills, regulations and programs are developed and introduced in order to regulate the national and international Internet market and its overall accessibility. The 2009 US agenda of Internet Freedom introduced goals by defining its five categories of providing Internet technologies, shaping international norms, encouraging the private sector to expand its role, using economic diplomacy and reforming export controls.[7] Further on it recommends principles like developing an international understanding in order to promote the use Internet capabilities, leading the effort to build international norms or strengthen the role of the private sector in supporting Internet freedom efforts.[8] In support of that agenda, the US government launched its official program of „21st Century Statecraft" in the same time period and invested over $100 million until the

---

[6] Wolfgang Kleinwächter (ed.), *Internet und Demokratie, MIND (Multistakeholder Internet Dialog) #5*, Collaboratory Discussion Paper Series, no. 1 (Berlin, June 2013), 8.

[7] Richard Fontaine, *Internet Freedom. A Foreign Policy Imperative in the Digital Age* (Washington, DC: Center for a New American Security, June 2011), last accessed: 14 April 2015, http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf.

[8] Ibid.

year 2012.[9] The support of anti-authoritarian regime groups like during the Arab Spring in 2011 by providing robust Internet access capabilities were elements of that program. The "21st Century Statecraft" defines its own status and understanding as a support element in times of international transition.[10] An active change by agenda and actions in the digital dimension could be recognized in the US by these new approaches in order to gain influence and project own interest in particularly critical regions of todays changing world. As usual, overall effects and future developments caused by these manipulations and small interventions could be discussed in different papers. In the EU, different approaches in the same category could be recognized as well by its 2011 support of the South Mediterranean region with its strategy to establish unlimited access to digital assets in order to achieve the goal of overall information and open communication.[11] On the contrary to these international engagements mostly during the time of crisis and change, domestic adaptations to recent developments are both a matter of concern and discussion in the US and EU. In the EU, regulations on a barrier-free access to digital infrastructure in terms of overall accessibility and data transfer means were established in 2013 after the discussion of discriminating internet access in favour of specific content providers like Facebook or

---

[9] U.S. Department of State, *21st Century Statecraft, May 2009 Overview*, last accessed: 14 April 2015, http://www.state.gov/statecraft/overview/index.htm.

[10] Ibid., „The 21st century statecraft agenda was built to address a moment of transition – an era of rapid change at the intersection of technology and foreign policy. It is fundamentally about adaptability not prediction. We believe that in a world of technology that enables pervasive, disruptive social change, the work of diplomats is to increase the speed at which government can respond to that change. We are doing that by leveraging new tools for public diplomacy, experimenting with new approaches to development partnerships…".

[11] European Commission, *A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean*, Joint Communication, COM (2011) 200 final (Brussels, March 8, 2011), last accessed 14 April 2015, http://eeas.europa.eu/euromed/docs/com2011_200_en.pdf.

Youtube occurred.[12] The same development can be noted in the US by the adaptation of the 2014 Net Neutrality Bill and its overall goal of the prevention of blocked or denied internet access by ways and means of Internet provider companies.[13] Overall, both the US and EU are strongly encouraging the free and unlimited use and access of the digital domain for its own citizens and organizations on the domestic side and to foster and establish digital access capabilities in regions of crisis and change. It is always related to their overall geo-strategic goals and aims to achieve regional influence and stability for own interests on their economic, political and security dimension. Especially countering threads from the digital dimension as well as international cooperation and teamwork on these issues will be in the focus later on. The US and EU approaches on how to achieve these goals will be matter of discussion in the second part of the paper on countering threads and future US-EU relations. International foundations and regulations are helpful and supportive to achieve these goals. The next part will focus on the Budapest Convention on Cybercrime from a civilian perspective.

BUDAPEST CONVENTION ON CYBERCRIME

Established in 2004, the Budapest Convention on Cybercrime can be considered as the first major international approach towards a common goal of

---

[12] European Commission, *Commission Adopts Regulatory Proposals for a Connected Continent*, Memo/13/779 (Brussels, September 11, 2013), last accessed: 14 April 2015, http://europa.eu/rapid/press-release_MEMO-13-779_en.htm.

[13] U.S. Congress, *Open Internet Preservation Act*, last accessed: 14 April 2015, https://www.congress.gov/bill/113th-congress/house-bill/3982.

countering threads against economies and private persons from the digital domain.[14] The range of participants towards this common understanding includes all of the Council of Europe Members as well as countries like the United States, Canada, Israel, Japan, Mexico or Australia. It focuses on the countering of threads and crimes from the digital domain like copyright issues, computer-related fraud, youth pornography and security network violations. It also specifies the rules and procedures for counter measures like computer network searches and interception in order to protect the societies against cyber-crime threads. It aims on the fostering of international cooperation and the adaption and conduction of appropriate legislation within the international environment.[15]

The goal is to prevent international economies from massive costs in context of cyber related and aggressive actions with costs of for example €4.8 million in Germany or $6.9 million in the US in 2012.[16] The biggest issue here is the raising speed of anonymous and dynamic attacks and the increasing capabilities of cyber domain criminals by its abilities of the use of skimming, phishing and the use of hidden underground markets.[17] The Budapest Convention is a first impressive step of

---

[14] Council of Europe, *Convention on Cybercrime* (Budapest, November 23, 2001), last accessed: 18 April 2015, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080f0b.

[15] Ibid., Summary and explanatory report, last accessed: 18 April 2015, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[16] Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, (Traverse City, MI: October 2012), last accessed: 18 April 2015, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[17] Lior Tabansky, *Cybercrime: A National Security Issue?*, Military and Strategic Affairs 4, no. 3 (December 2012): 117−36, last accessed: 18 April 2015, http://www.inss.org.il/uploadImages/systemFiles/MASA4-3Engd_Tabansky.pdf.

the international community in order to develop a common understanding of the interconnectivity and the importance of international relations and cooperation in order to counter cyber domain threads. Even the term international could be discussed for the reason of specifying the range of the threads and the range of its countermeasures because of the often impossible regional related specification towards the origin of threads or their targets. International borders disappear in the digital domain, so a more international, intergovernmental and interorganisational approach for effective countermeasures and cyber thread containment must be installed effectively. An international convention on a common understanding like with the Budapest Convention on Cybercrime in our case is a first step towards that ambitious goal. The Budapest Convention focuses on the civilian aspects of countering threads in the digital domain. Another approach will be assessed in the next part by describing the approach in the military dimension with the Tallinn Manual of 2013.

TALLINN MANUAL ON CYBER WARFARE

From a NATO perspective, more frequent and organized attacks inflicting government administrations, transportation networks or critical infrastructure can reach levels of endangering international prosperity, security and stability.[18] In order to counter threads from the digital domain, a comprehensive international understanding lead by the NATO Cooperative Cyber Defence Centre of Excellence

[18] NATO, *Active Engagement, Modern Defence*, (Lisbon, November 20, 2010), 11, last accessed: 18 April 2015, http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

was introduced with the Tallinn Manual on the International Law Applicable to Cyber Warfare in 2013. The main goal was to establish a common foundation and converging European and US understandings of how to counter military related cyber threads and the specification of principles in order to respond to aggressive actions on a legal base in accordance with current NATO and UN regulations.[19] The right of self-defence was a matter of discussion and specified in parts of the final document. It states for example in the first part of the document, that the right of self-defence is legitimatized when a certain level of threshold in the understanding of an armed assault has occurred. Whether it states specifications and definitions of the problem, a final legal definition and applicable related actions are specified but vague formulated. At least it defines a common understanding of the application of international laws and the justification of counter actions from a coordinated legal perspective.[20] The Tallinn Manual lays out the understanding of cyber related threads in the digital domain from a military perspective. The attempt of military related definitions (i.e., how to organize and conduct counterattacks) and its relation to international law by the description of its levels and outcomes, the Tallinn Manual definitions try to provide a basic understanding of these threads in military environments and its understandings of outcomes and countermeasures. Like the Budapest Convention outcomes from a more civilian perspective, the Tallinn Manual is a base of cooperation and another first major step in order to foster international

---

[19] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare.*, Cambridge et al., 2013, last accessed: 18 April 2015, http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf.

[20] Ibid., Part I, Section 2, The Use of Force, 42-74.

military cooperation and combined approaches towards cyber related threads. Both approaches are in principle fundamental understandings on mostly US, EU and NATO related cooperation in the civilian and military domain. As we will see in the second part of this paper, both the US and the EU are corresponding in their approach to other actors on the strategic level worldwide but they are as well different in the conduct of operations on countering cyber threads and especially unequal with their offensive (US) and defensive (EU) approaches.

COUNTERING CYBER THREADS

The acknowledgement of the threads from the cyber domain towards societies on economic, political and military means was realized. Implemented common understandings articulated in the Budapest Convention and the Tallinn Manual are a fundamental basis for international cooperation mostly fostered from a western perspective lead by the US and the EU and expanded by integrated partners from the cyber coalition of the willing.[21] NATO adopted its Cyber Defense Policy and its complementary Action Plan in 2011 by developing cyber defence structures and coordinating its member states cyber defence plans.[22] Cooperation on the US-EU level can be recognized by its common approaches and conduct of the joint exercise series of Cyber Atlantic 2011 and Cyber Europe 2012 with its aims to improve co-ordination in order to identify vulnerabilities, to increase infrastructure robustness and

[21] Cyber coalition of the willing in the understanding of the participants in the development and establishment of the Budapest Convention in the period between 2001 and 2004.

[22] NATO, *Nato/Defence: Nato Prepares Roadmap for Cyber-Defence*, Europe Diplomacy & Defence, no. 587 (February 26, 2013), last accessed: 19 April 2015, http://www.nato.int/cps/en/natohq/topics_78170.htm.

to strengthen preparedness and response capabilities for any kind of cyber security events.[23]

On the one side, the US-EU and its partners cooperation can be assessed as increasing developing and successful as well as investments in future crisis scenarios as network attacks or complex attacks on civilian companies like Sony or TV5 as we saw in the recent past. On the other side, the integration of other stakeholders like China and Russia is still an area of development and increasing cooperation with a lot of potential. Especially authoritarian systems like China and Russia are in favor of tighter controls of internet access. The understanding of cyber security in these countries are more characterized by suppressing undesired political content as well as control and repression of potential dissidents. US and EU approaches towards Russia and China on the cyber security topic took place on levels like the UN, G8 and on conferences like the Munich Security Conference and the FIRST Conferences on International Cyber Security.[24] Recent developments in the Ukraine put the cooperation with Russia to a current hold.[25] The fundamental difference of „western" approaches towards cyber security in contrast to authoritarian system in the understanding of the use of the cyber domain in military and civilian

---

[23] ENISA, *Cyber Europe Exercise 2012*, last accessed: 19 April 2015, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012.

[24] Munich Security Conference, *Cyber Security Summit*, last accessed: 19 April 2015, https://www.securityconference.de/en/activities/cyber-security-summit/; FIRST, *Conferences on Cyber Security*, last accessed: 19 April 2015, https://www.first.org/.

[25] Foreign Policy, *Current security relations*, last accessed: 19 April 2015, https://foreignpolicy.com/2015/04/17/situation-report-ash-wants-a-new-cyber-strategy-iraq-wants-a-pipeline-and-gen-dempsey-wants-ramadi-some-day/.

contexts. China and Russia cyberspace operations are aiming on different outcomes and strategies with its very own perspectives on transparency, thresholds and norms.[26] With these different approaches it is necessary to establish an international understanding and code of conduct in order to organize and control international state behaviour on cyber related topics.[27] The UN seems to be the right level of communication but bilateral engagements for example of Germany with Russia or US approaches towards China can be recognized in order to foster international cooperation even with partners with a different view.[28] It seems to be a recognizable uniform approach of western countries towards authoritarian systems related to cyber security issues. The next part will focus on differences within these approaches and understandings of the US and the EU.

US APPROACH TOWARDS CYBER SECURITY

Backed by the 2001 US Patriotic Act and the 2008 Foreign Intelligence Surveillance Amendments Act (FISAA), US authorities are able to collect and utilize user data in cases of governmental interest.[29] Even if the data origin is located physically on servers in other countries than the US, providers have to gain access to

---

[26] James A. Lewis, *Multilateral Agreements to Constrain Cyber-conflict,* Arms Control Today 40, no. 5 (June 2010): 14−19, last accessed: 19 April 2015, https://www.armscontrol.org/act/2010_06/Lewis.

[27] Tim Maurer, *Cyber Norm Emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security,* Cambridge, MA: Belfer Center for Science and International Affairs, September 2011.

[28] Jane Perlez, *U.S. and China Put Focus on Cybersecurity,* The New York Times, April 22, 2013, last accessed: 19 April 2015, http://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html?_r=0.

[29] J. V. J. van Hoboken et al., *Cloud Computing in Higher Education and Research Institutions and the United States Patriot Act,* Amsterdam: Institute for Information Law, November 2012, last accessed: 20 April 2015, http://www.ivir.nl/publicaties/download/684.

their data according to these rules. In the US understanding of its cyber space defence, authorities can be under attack and this kind of threat must be countered accordingly.[30] This example shows the importance of cyber defence and deterrence in the focus of US regulations towards a goal of defending US interest in the digital domain. In order to achieve this goal, US governmental authorities established the Cyber Command (USCYBERCOM) in 2010 with more than 5000 personnel as of today and its tasks to coordinate defence operations against computer network attacks as well as offensive capabilities in order to conduct cyber attack operations with desired outcomes like cyber-kinetic attacks.[31] Huge investments can be recognized by the improvement of the budgets up to $23 billion between 2014-2018. US authorities like CIA and NSA are in close cooperation with USCYBERCOM in order to achieve common goals and coordinate their actions.[32] Installation and operation of special collection service infrastructure especially in US embassies and consulates provide a global network in support of the three service cooperation.[33] Todays overall goals are to improve recognized deterrence and credible retaliation capabilities also in the context of raising Russian and Chinese capabilities.[34] In 2011, 231 offensive cyber

---

[30] Joseph S. Nye, *The Future of Power* (New York, 2011), Chapter 5. A critical assessment on "deterrence" written by Stevens, *A Cyberwar of Ideas?* , online review last accessed: 20 April 2015, http://www.e-ir.info/2012/05/24/review-the-future-of-power-2/.

[31] Europe Diplomacy & Defence, *Pentagon Reviews 'Rules of Engagement' against Cyber Attacks*, no. 620, July 4, 2013.

[32] James Bamford, *The Secret War. Infiltration. Sabotage. Mayhem. For Years, Four Star General Keith Alexander Has Been Building A Secret Army Capable of Launching Devastating Cyberattacks*, Wired, June 12, 2013, last accessed: 20 April 2015, http://www.wired.com/2013/06/general-keith-alexander-cyberwar/.

[33] *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, Spiegel, October 17, 2013, last accessed: 20 April 2015, http://www.spiegel.de/ international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

operations were launched by US authorities.[35] All these examples of cyber domain capabilities improvement over the last years for defensive and offensive operations are recognized worldwide as well as the geostrategic aim of these capabilities. In order to build up trust between partners, incidents like spying on partners heads of state are counterproductive within the leadership community. Countering capacities of countries like Russia or China are even more counterproductive for future relations of these regions on political, economical and geo-strategic levels. US offensive and deterrence capabilities should be used more cooperative within the community of their EU and NATO partners and used less aggressive towards authoritarian regimes like Russia or China in order to rebuild trust and international cooperation countering common threads for all societies. The next part will focus on the European approach, which will be slightly different in the sense of its aggressiveness.

EUROPEAN APPROACH TOWARDS CYBER SECURITY

EU strategies to counter cyber threads are based on a broad spectrum of communicated strategies and operational organizations. The fundamental base for the EU approach can be found in the 2013 EU Cyber Security Strategy with its goals of the improvement of civilian capabilities like resistance to cyber attacks, to restrain

---

[34] Center for Strategic and International Studies (CSIS), *Cybersecurity Two Years Later. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Washington, DC, January 2011, last accessed: 20 April 2015, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[35] Barton Gellman, *U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show*, The Washington Post, August 30, 2013, last accessed: 20 April 2015, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

cyber crime, capacity building of resources in order to improve cyber security, to formulate a common cyber strategy and rather subordinated the expansion of military cyber capabilities.[36] In addition to the strategy, further regulations are aiming on the improvement of the private sector and emphasize the improvement of critical digital infrastructure protection for non-state enterprises and especially communication service providers.[37] In order to enforce and supervise these regulations as well as fighting cyber threads from an european perspective, the European Cyber Crime Centre (EC3) was established in 2013 with its main functions of data fusion, cybercrime operations, strategy assessment and trend analysis, research and development including training activities in order to raise awareness for cybercrime issues as well as outreach activities and alignment for international partners cooperation in the public and state sector.[38] Additional anti-cyber thread activities are implemented in the overall European program Horizon 2020 which contributes towards research on cyber security €400 million from its €80 billion budget.[39] Overall it can be assessed, that the EU approach aims on the same goals and end states as the US approach. The obvious difference can be seen in the integration of these anti-

---

[36] Patryk Pawlak, *Cyber World: Site under Construction*, Paris: European Union Institute for Security Studies [EUISS], September 2013, last accessed: 21 April 2015, http://www.iss.europa.eu/uploads/media/Brief_32.pdf.

[37] *Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications*, Official Journal of the European Union, L 173, 26/06/2013 P. 0002-0008, last accessed: 21 April 2015, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF.

[38] European Commission, *European Cybercrime Centre – one year on,* Press Release, February 10, 2014, last accessed: 21 April 2015, http://europa.eu/rapid/press-release_IP-14-129_en.htm.

[39] European Union, *Horizon 2020*, last accessed: 21 April 2015, http://ec.europa.eu/programmes/horizon2020/en.

cyber thread institutions and capabilities in military-security environments like USCYBERCOM, CIA and NSA versus the European approach with an Europol lead Cyber Crime Centre integrating EU authorities as well as other stakeholders even from the private sector, civil society organizations and other EU institutions to counter contemporary threads.[40] The question can be raised if both approaches conducting the same kinds of operation in comparable manners, the Europeans are just better in communicating their approach in more feasible fashion for the European public. On the financial view of the assigned resources towards future developments of these anti-cyber threads capabilities, the US are significant ahead and they will see themselves always in the forehand in the matter of US-EU equality and recognition of their partnership on these issues. EU authorities must improve their investments as well as the cooperation on organizations like NATO to foster US-EU cooperation especially on contemporary threads.[41] The next part will focus on specific topics towards anti-cyber threads in order to specify contemporary issues both the US and EU are facing.

US-EU SPECIFIC TOPICS ENDANGERED FROM THE CYBER DOMAIN

Risks for critical infrastructure, data protection, civil rights, human security as well as copyright issues are the most common topics in today's cyber domain and its

---

[40] European Cyber Crime Centre, *Joining Forces*, last accessed: 21 April 2015, https://www.europol.europa.eu/ec3/joining-forces.

[41] James Stavridis, *Five ways to reboot NATO*, last accessed: 21 April 2015, http://www.politico.eu/article/5-ways-to-reboot-nato/.

integral understanding of misuse and fraud.[42] This part cannot process all topics because it this paper's limits and will focus therefore on critical infrastructure and data protection. Critical infrastructure in the understanding of this paper are the energy and transportation sector as well as Internet search engines, cloud computing services, Internet payment gateways and online application markets.[43] The number of recorded critical infrastructure cyber-attacks in the US increased from annually 9 to 198 in the period between 2009 and 2013.[44] Even more cyber-attacks occur but stay unreported or they were even not perceived. The same problems occur in the EU, but numbers are not present because of the absence of official statistics or reports.[45] The US voluntary report system of such incidents is generating an area of uncertainty and is a matter of concern for governmental authorities. The cooperation with private sector actors as well as the exchange of information between businesses, authorities and security organizations are essential in order to achieve the common goal of cyber threat engagement. The obligation of cyber related incidents is a strong matter of concern and currently discussed more within US and less within EU authorities whether the reporting should be more institutionalized or other solutions could be

---

[42] Joseph S. Nye, *What Is It That We Really Know about Cyber Conflict?*, The Daily Star, April 24, 2012, last accessed: 21 April 2015, http://www.dailystar.com.lb/Opinion/Commentary/2012/Apr-24/171186-what-is-it-that-we-really-know-about-cyber-conflict.ashx.

[43] U.S. Securities and Exchange Commission, *Disclosure Guidance* , Washington, DC, July 16, 2013, last accessed: 21 April 2015, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[44] *Sharp Increase in Cyberattacks on U.S. Critical Infrastructure*, Homeland Security News Wire, July 3, 2012, last accessed: 21 April 2015, http://www.homelandsecuritynewswire.com/dr20120703-sharp-increase-in-cyberattacks-on-u-s-critical-infrastructure.

[45] Louis Marinos, *ENISA Threat Landscape 2014*, Heraklion, December 2014, last accessed: 21 April 2015, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014.

adapted.[46] Other than to similar US-EU approach towards protection of critical infrastructure the understanding in the area of data protection must be assessed differently. Data protection in the understanding of this paper is aimed on the acceptable access to private data in order to counter criminal or terrorist acts.[47] The US approach within the context of national security issues, a high priority is given towards the surveillance of suspicious activities and meta analysis conducted by organizations like the NSA.[48] All activities are backed by formal regulations in order to legalize surveillance activities.[49] On the contrary, EU regulations strongly encourage the data protection of European citizens and released the 2012 draft version of the EU General Data Protection Regulation which should come into effect in 2016.[50] This regulation focuses on data protection especially in areas of foreign (especially US) online services and providers adapting to European rules without the

---

[46] The White House, *Executive Order: Improving Critical Infrastructure Cybersecurity* (Washington, DC, February 12, 2013), last accessed: 21 April 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; U.S. Department of Homeland Security, *National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency*, Washington, DC, 2009, last accessed: 21 April 2015, http://www.dhs.gov/national-infrastructure-protection-plan; German Perspective: Deutsche Telekom/T-Systems (ed.), *Cyber Security Report 2012. Ergebnisse einer repräsentativen Befragung von Entscheidungsträgern aus Wirtschaft und Politik*, Bodman am Bodensee 2012, last accessed: 21 April 2015, http://www.cybersecuritysummit.de/downloads/131106_Cyber_Sicherheitsreport_2013_final.pdf.

[47] Constance Pary Baban, *AICGS, Security Policy in Cyberspace: The Need for a Transatlantic Debate on the Protection of Data and Privacy*, last accessed: 21 April 2015, http://www.aicgs.org/issue/security-policy-in-cyberspace-the-need-for-a-transatlantic-debate-on-the-protection-of-data-and-privacy/.

[48] Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Washington, DC, June 8, 2013, last accessed: 24 April 2015, http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

[49] David E. Sanger, *Obama Panel Recommends New Limits on N.S.A. Spying*, The New York Times, December 18, 2013, last accessed: 24 April 2015, http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html.

[50] European Union, *2012 Draft Data Protection Regulation*, last accessed: 24 April 2015, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

specific US meta data sharing when offering services on the European market. Areas of US-EU conflict occur on data exchange issues under umbrellas like Society for Worldwide Interbank Financial Telecommunication (SWIFT) or Transatlantic Trade and Investment Program (TTIP) on which the area of data origin could be unclear and the suspicion of undermining EU regulations in US contexts occurs.[51] In order to achieve a common US-EU understanding, both partners have to establish a more robust and acceptable solution towards the issues described above. Without solving these issues a more suspicious environment will be developing and future cooperation is going to be more complicated. The next part will offer arguments for more effective international and especially US-EU cooperation on cyber domain issues and regulations described earlier.

FUTURE US-EU RELATIONS, COOPERATION AND ENGAGEMENTS

Like described in all of the previous parts, a common understanding in both the US and the EU occur on the importance of the cyber domain, especially its secure, stable and protected utilization, towards national security and the well-being of their citizens as well as the importance from an economic point of view. In order to achieve this cooperative collective goal and end state of partnership and cooperation, controversial topics like the specific approaches towards the described topics of countering cyber threads with the US offensive and the EU defensive approach must

[51] Guy Verhofstadt, *Europe Must Get Tough with the U.S. over NSA Spying Revelations*, The Guardian, July 2, 2013, last accessed: 25 April 2015, http://www.theguardian.com/commentisfree/2013/jul/02/europe-us-nsa-spying.

come together on a base of collective understanding in which US and EU tensions must be more open communicated and each others doubts and worries should be negotiated for a greater goal of common international and transatlantic cyber security. Both approaches must be recognized within their geo-strategic frameworks of coalitions, influences and dependencies. To be more effective in international (anti-) cyber thread cooperation, both actors must acknowledge each other as equal partners and realize the opportunities of cooperation by its means and networks. A higher effectiveness could be established by lower US leadership and offensive approaches towards global policies and the EU could support initiatives faster by developing a common EU position with less hesitation or doubts. The greater goal of citizen well-being on cyber thread protection will multiply the common efforts. The latest developments of spying activities between partners and allies lead to uncertainty of especially EU citizens but also on the governmental level.[52] In order to rebuild trust in US-EU cooperations as well as transparency on national and international cyber operations both actors must intensify cooperation by establishing greater common understanding on the usage of the cyber domain for civilian, economic and governmental means. Establishment of global standards on for example unrestricted access towards Internet communication and Internet access countering authoritarian states rules and regulations could improve future US-EU engagements and

[52] The understanding of spying activities from all governmental institutions either in the US and the EU are probably the same just different in capabilities and financial support. The communication to the public must be noted as significantly different and the notion within the EU is often more surprised and horrified. Latest German Secret Service (BND) related activities in cooperation with NSA are ongoing discussed as of today.; New York Times, 03 May 2015, *German Prosecutors Launch Investigation of Spying Charges*, last accessed: 03 May 2015, http://www.nytimes.com/reuters/2015/05/03/technology/03reuters-germany-spying-nsa.html?_r=0.

cooperation. This would lead towards a more robust trust and faith in counter cyber threat capabilities from the perspective of private persons, local economies was well as official or governmental organizations. Cooperation for example between USCYBERCOM and EC3 could multiply effectiveness and speed. Both actors should work on future regulations on official cooperation and establish working relationships first in order to lead to a future establishment of transatlantic institutions on cyber domain issues. All initiatives should be conducted as transparent and open as possible in order to enable the public on both sides of the Atlantic to rebuild trust and confidence in governmental operations on international levels and cooperation in the cyber domain. The future increased use of digital means and capabilities will increase the need for these kinds of installations in order to regulate (or a least monitor) global digital activities. In order to keep track also unpopular authoritarian partners like China and Russia must be integrated in cyber domain related issues and a strong communicative approach will be necessary. Established US and EU relations to these actors could be used in order to co-ordinate approaches in the greater goal of cyber security. Even a common international US-EU-and other partners approach towards threads like ISIS could be possible and might be necessary in the near future. On that note maybe institutions like the UN should be pushed more in order to establish effective global cyber domain regulations and the installation of global cyber domain institutions for future challenges. The importance of the cyber topic should be pushed by both the US and the EU on every opportunity and both actors should unite their efforts in order to achieve higher effectiveness in cyber security on all the described areas before. All areas of cyber threads are highly interconnected and future

developments and capabilities are potentially dangerous. This potential danger can be countered by effective international cooperation lead by US and EU organizations by transparent cooperation and establishment of capable and effective institutions countering cyber domain challenges.

CONCLUSION

The issue on cyber related threads, especially to fight their origins, is not a problem of a specific nation or one of their institutions. In today's world of interconnectivity and globalism, a singular approach in order to counter cyber threats seems to be unsuccessful. This paper argued about the increase of effectiveness by connecting national approaches towards international cooperation especially with the actors US and EU. The first part described the normative foundations of global cyber operations by describing the role of international actors and their understandings of cyber related threads. It focused on specific US and EU debates and laid out specific understandings and foundations of these two actors. This part was expanded by the discussion about international foundations like the more civilian Budapest Convention and the more military related Tallinn Manual. The second part argued about how to counter cyber threads and focused on US and EU approaches as well as specific topics endangered from the cyber domain like critical infrastructure and data protection. The final part argued about the future of US-EU relations, cooperation and engagements towards a more effective cooperation and laid out actions in order to rebuild true between economies and private persons as well as the integration of unpopular partners like China and Russia as well as the improvement of a cyber-domain importance on the world stage. All arguments are influenced by actual

political, economic, geo-strategic, historical and demographic developments and are matter of change according to the flavour of the day and the coalition of the day. The paper showed some aspects and possibilities of future cooperation between US and EU organizations in order to achieve levels of assumed increase of cyber security in order to improve population well-being and a certain level of comfort for economies. At least the increase of transparency, the integration of unpopular authoritarian regimes and a greater co-operation between US and EU organizations could lead towards a common goal of effective capabilities to counter cyber related threads in every possible future scenario.

BILBLIOGRAPHY:

Baban, Constance Pary. *AICGS, Security Policy in Cyberspace: The Need for a Transatlantic Debate on the Protection of Data and Privacy*. last accessed: 21 April 2015, http://www.aicgs.org/issue/security-policy-in-cyberspace-the-need-for-a-transatlantic-debate-on-the-protection-of-data-and-privacy/.

Bamford, James. *The Secret War. Infiltration. Sabotage. Mayhem. For Years, Four Star General Keith Alexander Has Been Building A Secret Army Capable of Launching Devastating Cyberattacks.* Wired, June 12, 2013. last accessed: 20 April 2015, http://www.wired.com/2013/06/general-keith-alexander-cyberwar/.

Center for Strategic and International Studies (CSIS). *Cybersecurity Two Years Later. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC, January 2011. last accessed: 20 April 2015, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

Council of Europe. *Convention on Cybercrime*. Budapest, November 23, 2001. last accessed: 18 April 2015, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080f0b

Deutsche Telekom/T-Systems (ed.). *Cyber Security Report 2012. Ergebnisse einer repräsentativen Befragung von Entscheidungsträgern aus Wirtschaft und Politik*, Bodman am Bodensee 2012, last accessed: 21 April 2015, http://www.cybersecuritysummit.de/downloads/131106_Cyber_Sicherheitsreport_2013_final.pdf.

ENISA. *Cyber Europe Exercise 2012*. last accessed: 19 April 2015, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012.

Europe Diplomacy & Defence. *Pentagon Reviews 'Rules of Engagement' against Cyber Attacks*. No. 620, July 4, 2013.

European Commission. *A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean.* Joint Communication, COM (2011) 200 final (Brussels, March 8, 2011). last accessed 14 April 2015, http://eeas.europa.eu/euromed/docs/com2011_200_en.pdf.

European Commission. *Commission Adopts Regulatory Proposals for a Connected Continent.* Memo/13/779 (Brussels, September 11, 2013). last accessed: 14 April 2015, http://europa.eu/rapid/press-release_MEMO-13-779_en.htm.

European Commission. *European Cybercrime Centre – one year on.* Press Release, February 10, 2014. last accessed: 21 April 2015, http://europa.eu/rapid/press-release_IP-14-129_en.htm.

European Cyber Crime Centre. *Joining Forces*. last accessed: 21 April 2015, https://www.europol.europa.eu/ec3/joining-forces.

European Union. *2012 Draft Data Protection Regulation*. last accessed: 24 April 2015, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

European Union. *Horizon 2020*. last accessed: 21 April 2015, http://ec.europa.eu/programmes/horizon2020/en.

European Union. Official Journal. *Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.* L 173, 26/06/2013, P. 0002-0008. last accessed: 21 April 2015, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF.

FIRST. *Conferences on Cyber Security*. last accessed: 19 April 2015, https://www.first.org/.

Fontaine, Richard, *Internet Freedom. A Foreign Policy Imperative in the Digital Age.* (Washington, DC: Center for a New American Security, June 2011), last accessed: 14 April 2015, http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf.

Foreign Policy. *Current security relations*. last accessed: 19 April 2015, https://foreignpolicy.com/2015/04/17/situation-report-ash-wants-a-new-cyber-strategy-iraq-wants-a-pipeline-and-gen-dempsey-wants-ramadi-some-day/.

Freedom House. *Freedom of the Net 2014.* last accessed: 12 April 2015, https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf.

Gellman, Barton. *U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show*. The Washington Post, August 30, 2013. last accessed: 20 April 2015, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

German Journal of the Ministry of Defence 1/2014. *Cyber-Security – a review*. last accessed: 12 April 2015, http://www.hardthoehenkurier.de/emag/free/2014-01/index.html#/18/.

German Ministry of Domestic Affairs. *Cyber-Security Strategy for Germany*. last accessed: 12 April 2015, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

van Hoboken, J. V. J. et al. *Cloud Computing in Higher Education and Research Institutions and the United States Patriot Act.* Amsterdam: Institute for Information Law, November 2012. last accessed: 20 April 2015, http://www.ivir.nl/publicaties/download/684.

Homeland Security News Wire. S*harp Increase in Cyberattacks on U.S. Critical Infrastructure.* July 3, 2012. last accessed: 21 April 2015, http://www.homelandsecuritynewswire.com/dr20120703-sharp-increase-in-cyberattacks-on-u-s-critical-infrastructure.

International Telecommunication Union (ITU). *Facts and Figures. The World in 2014.* last accessed: 12 April 2015, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

Kleinwächter, Wolfgang. *Internet und Demokratie, MIND (Multistakeholder Internet Dialog) #5*. Collaboratory Discussion Paper Series, no. 1 (Berlin, June 2013), 8.

Lewis, James A. *Multilateral Agreements to Constrain Cyber-conflict.* Arms Control Today 40, no. 5 (June 2010): 14−19. last accessed: 19 April 2015, https://www.armscontrol.org/act/2010_06/Lewis.

NATO. *Active Engagement, Modern Defence*. Lisbon, November 20, 2010, 11. last accessed: 18 April 2015, http://www.nato.int/cps/en/natolive/official_texts_68580.htm.

NATO. *Nato/Defence: Nato Prepares Roadmap for Cyber-Defence.* Europe Diplomacy & Defence, no. 587 (February 26, 2013). last accessed: 19 April 2015, http://www.nato.int/cps/en/natohq/topics_78170.htm.

New York Times. *German Prosecutors Launch Investigation of Spying Charges*. 03 May 2015. last accessed: 03 May 2015, http://www.nytimes.com/reuters/2015/05/03/technology/03reuters-germany-spying-nsa.html?_r=0.

Marinos, Louis. *ENISA Threat Landscape 2014*. Heraklion, December 2014. last accessed: 21 April 2015, https://www.enisa.europa.eu/activities/risk-

management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014.

Maurer, Tim. *Cyber Norm Emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security*. Cambridge, MA: Belfer Center for Science and International Affairs, September 2011.

Munich Security Conference. *Cyber Security Summit*. last accessed: 19 April 2015, https://www.securityconference.de/en/activities/cyber-security-summit/.

Nye, Joseph S. *The Future of Power* (New York, 2011), Chapter 5. A critical assessment on "deterrence" written by Stevens, *A Cyberwar of Ideas?*. online review last accessed: 20 April 2015, http://www.e-ir.info/2012/05/24/review-the-future-of-power-2/.

Nye, Joseph S. *What Is It That We Really Know about Cyber Conflict?.* The Daily Star, April 24, 2012. last accessed: 21 April 2015, http://www.dailystar.com.lb/Opinion/Commentary/2012/Apr-24/171186-what-is-it-that-we-really-know-about-cyber-conflict.ashx.

Pawlak, Patryk. *Cyber World: Site under Construction*. Paris: European Union Institute for Security Studies [EUISS], September 2013. last accessed: 21 April 2015, http://www.iss.europa.eu/uploads/media/Brief_32.pdf.

Perlez, Jane. *U.S. and China Put Focus on Cybersecurity.* The New York Times, April 22, 2013. last accessed: 19 April 2015, http://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html?_r=0.

Ponemon Institute. *2012 Cost of Cyber Crime Study: United States*, (Traverse City, MI: October 2012). last accessed: 18 April 2015, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

Sanger, David E. *Obama Panel Recommends New Limits on N.S.A. Spying*. The New York Times, December 18, 2013. last accessed: 24 April 2015, http://www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html.

Schmitt, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge et al., 2013. last accessed: 18 April 2015, http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf.

Spiegel. *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*. Der Spiegel, October 17, 2013. last accessed: 20 April 2015, http://www.spiegel.de/

international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

Stavridis, James. *Five ways to reboot NATO*. last accessed: 21 April 2015, http://www.politico.eu/article/5-ways-to-reboot-nato/.

Tabansky, Lior. *Cybercrime: A National Security Issue?*. Military and Strategic Affairs 4, no. 3 (December 2012): 117−36. last accessed: 18 April 2015, http://www.inss.org.il/uploadImages/systemFiles/MASA4-3Engd_Tabansky.pdf.

United States. Congress. *Open Internet Preservation Act*. last accessed: 14 April 2015, https://www.congress.gov/bill/113th-congress/house-bill/3982.

United States. Department of Homeland Security. *National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency*. Washington, DC, 2009. last accessed: 21 April 2015, http://www.dhs.gov/national-infrastructure-protection-plan.

United States. Department of State. *21st Century Statecraft, May 2009 Overview*. last accessed: 14 April 2015, http://www.state.gov/statecraft/overview/index.htm.

United States. Director of National Intelligence. *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Washington, DC, June 8, 2013. last accessed: 24 April 2015, http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

United States. Securities and Exchange Commission. *Disclosure Guidance*. Washington, DC, July 16, 2013. last accessed: 21 April 2015, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

United States. The White House. *Executive Order: Improving Critical Infrastructure Cybersecurity*. Washington, DC, February 12, 2013. last accessed: 21 April 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Verhofstadt, Guy. *Europe Must Get Tough with the U.S. over NSA Spying Revelations*. The Guardian, July 2, 2013. last accessed: 25 April 2015, http://www.theguardian.com/commentisfree/2013/jul/02/europe-us-nsa-spying.