Spring 5-16-2014

Transatlantic Cooperation on Cyber Security: Data Privacy and Cybercrime

Allison Feikes
Western Kentucky University, allison.feikes182@topper.wku.edu

TRANSATLANTIC COOPERATION ON CYBER SECURITY: DATA PRIVACY AND CYBERCRIME

A Capstone Experience/Thesis Project

Presented in Partial Fulfillment of the Requirements for

the Bachelor of Arts Degree with

Honors College Graduate Distinction at Western Kentucky University

By

Allison M. Feikes

*****

Western Kentucky University
2014

CE/T Committee:

Dr. Roger Murphy, Advisor

Dr. Joel Turner

Wolfgang Brauner

Approved by

_____
Advisor
Department of Political Science

ABSTRACT

The Internet is a vital part of the global economy considering an estimated 8 trillion United States dollars flow through global e-commerce each year. However, this new, innovative tool is not only used to benefit the people; the Internet has become a place for criminal activity as well. With over one million victims of crimes globally every day, the United States works closely with the EU to ally against this Lernaean Hydra. This thesis explores how Transatlantic cooperation can be improved through formalized regulation especially in regards to organized research in tracking child exploitation, Safe Harbor Privacy Principles, and reducing terrorist threats.

Keywords: cyber security, cybercrime, Transatlantic cooperation, data privacy, European, safe harbor

Dedicated to Meeko, the most fun of all loving companions

ACKNOWLEDGEMENTS

I would like to thank my Advisor, Dr. Roger Murphy for encouragement and dedication to political science and international affairs. His work has truly furthered the goal of Western Kentucky University to be a leading American university with international reach. I am also indebted to the rest of my committee, Dr. Joel Turner and Wolfgang Brauner, whose passion for American politics and foreign cultures, respectively, has inspired me in turn.

I would like to thank my family—my mother, Nancy Robinson, my father Mitchell Feikes—for their love in support while I was in Brussels. They have always encouraged me to achieve excellence.

I am indebted to Andreas Herrman, who helped me write a shorter version of this thesis for the German Marshall Fund. I am fortunate to have had you as a partner for the project.

I am eternally grateful to Erik Barnett, Sofia Runnland, Sarah Kindig, Wally Bird, and Julie Brill for allowing me to interview them. Their insight has truly added to the quality of this article.

I would like to thank the U.S. Mission to the EU. It was through my internship in the Public Affairs Office that I was inspired to choose cyber security and Transatlantic cooperation as my topic. This experience also gave me a better understanding of the

special relationship between the U.S. and the EU. The staff within the office gave me support and time to conduct my interviews for this article.

Finally, I would like to thank my friends Amanda Florence, Emily Thomas, and Annie Schaumann who edited, baked, and supported me for my thesis defense.

VITA

October 9, 1991	Born-Michigan City, Indiana
2003	CISV International
2010	La Porte High School, La Porte, Indiana
2011	Study Abroad, Central Europe
2011	Internship, U.S. Peace Corps
2012	Internship, Senator Mitch McConnell
2012	Volunteer Abroad, Tanzania
2013	Internship, U.S. Mission to the EU
2014	Western Kentucky University, Bowling Green, Kentucky

FIELDS OF STUDY

Major Field 1: Political Science

Major Field 2: International Affairs

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

A world without Internet is unthinkable for most American and European citizens. The Internet is also a vital part of the global economy, an estimated eight trillion United States dollars (USD) flow through the global e-commerce infrastructure each year.[1] Unfortunately, this new tool is not only used for the benefit of the people, but also for criminal activity. Criminal actors have found ways to abuse this tool for personal gains and malevolent purposes, which pose threats to personal, corporate, and national security. The victims of these crimes, more than one million people worldwide every day,[2] include citizens of the United States (U.S.) and European Union (EU) member states.

Cyber security and cybercrime are succinctly defined by European Commission in the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace:*

> *Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and*

[1] Internet Matters: the Net's sweeping impact on growth, jobs and prosperity. McKinsey Global Institute, May 2011.
[2] Norton Cybercrime Report 2011. Symantec. September 2011

integrity of the networks and infrastructure and the confidentiality of the information contained therein.

Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)[3].

We must fight as new emerging problems such as identity theft, child exploitation, fraud, and cyber attacks against institutions and infrastructure threaten international economic stability. Fighting cybercrime is a complicated multi-national issue. Cybercriminals are similar to the Lernaean Hydra of Greek mythology. Every victory against cybercrime makes way for new forms of cyber criminality. Since the advent of the Internet when cybercrime was limited to computer viruses, cybercrime has expanded to include: the dissemination of illegal contents, illegal access to computer systems, system and data interference, illegal interception of non-public transmissions of computer data, and terrorism.[4]

The problem has to be tackled through cooperation of the most important players, the Transatlantic partners. According to the German Marshall Fund of the United States,

[3] European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 7 Feb.2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[4] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice

over half of EU and U.S. respondents in their 2013 Transatlantic Trends public opinion survey felt that the other partner should exert strong international leadership.[5] This data indicates that the two international entities feel that the other is not only capable of leadership but will also promote the same ideas and values in the international realm.

The relationship between the U.S. and Europe is particularly special as the key members of the Transatlantic community; the Transatlantic way of life can be defined through its historic sharing of values and culture. The Spanish were the first to settle in America, and nearly half of Americans can trace their ancestry to Europe.[6] However, the true closeness between the U.S. and Europe began after World War II. Following WWII, the North Atlantic Treaty Organization (NATO) and the United Nations (UN) were established. U.S. President Franklin D. Roosevelt coined the term "United Nations" and hoped to create an international entity that prevented another world war, especially in Europe. The U.S. was the power house that started NATO as a military alliance against the expanding Soviet Union. As the Soviet Union threatened nearby Europe, NATO's centre was placed in Brussels. With the establishment of the UN and NATO, the ideals of the U.S. and Europe grew closer, creating the western voice. Today, Europe and the U.S. join together to address a variety of issues including intervention in Iraq and Afghanistan, the economic crisis, dilemmas in NATO, and the escalating crisis in the Ukraine. The U.S. and the EU together form the voice of western policy.

U.S. and EU cooperation on this issue began in 2010 with the creation of the Working Group of Cyber Security and Cybercrime. "Since then, international cyberspace

[5] The German Marshall Fund of the United States. "Transatlantic Trends Key Findings", 2013. http://trends.gmfus.org/files/2013/09/TTrends-2013-Key-Findings-Report.pdf
[6] "First ancestry reported; Total population; 2008-2012 American community survey 5-year estimate." American Fact Finder. U.S. Department of Commerce. United States Census Bureau. Web. 26 Apr. 2014.

developments have become central concerns in the broader foreign and security policy of transatlantic partners. In addition, an increasing number of international cyber debates have raised the need for ever closer consultations on major policy positions between strategic partners."[7] The establishment of this working group established the norms for cooperation on this subject.

Within, *Transatlantic Cooperation on Cyber Security: Data Privacy and Cybercrime*, there is an outline of: three main threats to cyber security; current levels of cooperation; where the Transatlantic powers fall short of reaching their goals; and the consequences of not reaching these strategic goals if the powers are not able to uphold security.

The U.S. and the EU fail to achieve strategic goals as they allow a myriad of issues to hinder cooperation. Change must ensue in order to protect individuals, firms, and the states themselves from cyber threats. The U.S. and the EU most go beyond the normal form of cooperation that has been established for this issue. Europe and the U.S. face catastrophic consequences if they continue this failure.

[7] "Fact Sheet: EU-US cooperation on cyber security and cyberspace." European Union External Action Service. 26 Mar. 2014.

CHAPTER 2

THREE FORMS OF THREATS

This article studies three components of Transatlantic cooperation on cyber security:

- Child Exploitation
- Safe Harbour Privacy Principles (Safe Harbor)
- Terrorism

These three topics also demonstrate how cyber criminals can affect individuals, firms, and states as a whole. Children are the most vulnerable members of the population. These individuals are treated in a terrifying way, and the hurt continues as it is distributed to incalculable strangers around the globe. Individuals and firms are also affected by Safe Harbor. Agreed upon cyber security principles prevent companies from illegally selling data that individual people or small businesses give to companies. Furthermore, Safe Harbor allows firms to do business in international markets. Often, when hackers attack firms, customer loyalty falls due to poor public relations; customers no longer feel safe using that company. Safe Harbor creates a minimal level of security for firms, preventing penetration from cyber hackers. Finally, states are vulnerable to cyber attacks in modern day terrorism. If banks, legislatures, or energy companies were infiltrated, mass

destruction could occur within a state. Overall, these three examples show how individuals, firms, and states are vulnerable to cyber attacks.

Child Exploitation

Erik Barnett, U.S. Immigration and Customs Enforcement Attaché at the U.S. Mission to the EU, identified child exploitation as a top priority for his office. Children around the world will fall prey to predators who distribute horrible images to countless strangers for their own gratification. The U.S. works with the EU to fight child exploitation, one of the most heinous of all cybercrimes. The fight against child exploitation must be a global fight for various reasons. First, child exploitation often takes place in three or more countries. The product could be made in Europe, have a funding stream through Latin America, and be sold in the U.S.[8] Furthermore, "combating cybercrime is especially challenging due to problems of jurisdiction that arise at both the national and international level. The traditional forms of jurisdiction are based on the concept of boundaries, and laws are based on 'territorial sovereignty.' Because cyberspace has no physical boundaries, criminals can change their location from one country to another within seconds in the cyber-world, irrespective of their physical location."[9] Considering the various countries involved in child exploitation and the lack of boundaries in cyber space, cooperation between the U.S. and Europe is imperative in order to convict these outrageous criminals.

[8] Interview Erik Barnett 2 Oct.2013.
[9] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice

Safe Harbor Privacy Principles

Safe Harbor is a controversial set of actions that showcase the difference of thought between the U.S. and the EU. There have been many articles published on the subject. Private companies often collect extensive personal information about their customers with which they can then do a variety of actions, such as sell that information to other companies interested in marketing goods and services to those customers. In order to protect these constituents, the EU Council of Ministers created a directive to harmonize data privacy protection across the EU. In contrast, the U.S. relies on a self-regulating system within its private sector. This is due to the fact that the U.S. views data privacy as a property right rather than an inalienable right. Also, the U.S. data privacy laws reflect the general distrust Americans have for the government. Legislation that does deal with data privacy is reactive.[10] The International Safe Harbor is an agreement, though it is actually two unilateral actions, between the U.S. and the EU that helps U.S. Companies comply with the EU Data Protection Directive. The U.S. Federal Trade Commission (FTC) is the relevant authority in this context and works as a law enforcement agency that cooperates with the EU. "Before sending information to a U.S. company, EU organizations can verify that the company is participating in Safe Harbor principles by accessing the Internet site and viewing a regularly updated list of participating companies."[11] An organization may enter Safe Harbor by joining an existing privacy program or by creating its own and having that program approved by the

[10] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.
[11] "U.S.-EU 'Safe Harbor' data privacy arrangement." The American Journal of International Law, Vol. 95:1. Jan. 2001. Pp. 156-159.

Department of Commerce each year.[12] These privacy programs have minimal cyber security standards for each company to protect it and its customers from hackers. The Data Protection Directive had strict guidelines, which prevented the data flow between European and U.S. firms. Safe Harbor was a solution and compromise between the entities that allowed e-commerce to continue.

Terrorism

The most consequential threat to the U.S. and the EU is terrorism; therefore, cyber terrorism is a vastly important component of cyber security to explore. The global reliance on cyber technology has become so prevalent that the world now has new a terrorist threat. For instance, "sophisticated terrorists might take down the nation's electrical grid, so new security standards are necessary."[13] This terrorist threat is further depicted by the World Economic Forum, "So far, cyberspace has proved resilient to attacks, but the underlying dynamic of the online world has always been that it is easier to attack than defend. The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce. Fresh thinking at all levels on how to preserve, protect and govern the common good of a trusted cyberspace must be developed."[14] Cyber terrorism is the largest threat to the two states, and U.S.-EU cooperation must be enhanced in order to ally this threat.

[12] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.
[13] O'Neil, Michael. "Cyber crime dilemma: Is it possible to guarantee both security and privacy?" The Brookings Review, Vol. 19:1. Winter 2001. Pp. 28-12.
[14] *Global Risks 2014, Ninth Edition*. World Economic Forum. 2014.

CHAPTER 3

AN EXAMINATION OF CURRENT COOPERATION

The start of cybercrime can be marked with the introduction of the Morris worm, which hit the Internet on November 1988. "Since then the Internet has experienced an explosion of malware and virus attacks affecting individuals and organizations alike. More recently, the world has seen concerted efforts by organized criminals to commit IT crimes on a global scale."[15] Cybercrime has grown tremendously since 1988. Furthermore, the cyber realm is borderless and without clear territory. The amount of global e-commerce lost each year is between 750 billion and 1 trillion euros a year. The true extent of cybercrime is hard to determine considering the amount of unreported crime, as firms often fear negative public relations that accompany cybercrimes.[16] This has created the need for collaboration from the Transatlantic powers.

Law enforcement agencies

There is a strong cooperative relationship between Europol and various U.S. law enforcement agencies such as the U.S. Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), or the Secret Service. It was a significant sign

[15] Stephens, P. "Cybercime investigation training and specialist education for the European Union." Digital Forensics and Incident Analysis. Aug. 2007.
[16] Drewer, Daniel and Jan Ellerman. "Europol's data protection framework as an asset in the fight against cybercrime. ERA. 8 Aug. 2012. Pp. 382-395.

that on the day of the establishment of the European Cybercrime Centre (EC3) the ICE Director John Morton was on stage to promote cooperation between the U.S. and Europe.[17] The EC3 has a state-of-the art infrastructure that extends to all member states and third country partners like the U.S.[18] These interactions on a pan-European level are supplemented by agreements between the U.S. and single EU member states regarding the cooperation of national law enforcement agencies.

The U.S. and the EU law enforcement agencies have adapted together. For instance, counterfeit goods were commonly sold under ".com" domain names on the Internet three years ago. "Corporations rely on familiar brands to stimulate consumer awareness and to foster an affinity for their products. Successful brands yield strong brand loyalty, which generates a dependable customer base and a predictable revenue stream."[19] Often, online users will sell goods by using the same or similar brand name, but they will have no affiliation with the corporation causing consumer confusion. When those responsible for this criminal activity were prosecuted, law enforcers were able to seize the domain name as part of their prosecution. Therefore, criminals began to register under foreign domain names. By working with Europol, domain names in Europe can also be seized to investigate the sale of fraudulent goods. This adaptive cooperation is significant considering the speed at which technology changes and that the last agreement to develop multilateral investigations and evidence sharing was established in 1973,

[17] U.S. Immigration and Customs Enforcement. News Release: ICE director attends opening of European Cyber Crimes Centre at Europol. 11 Jan.2013 http://www.ice.gov/news/releases/1301/130111thehague.htm
[18] Stevenson, J. "How Europe and America defend themselves." Foreign Affairs Vol. 82:2. Mar./Apr. 2003. Pp. 75-90.
[19] Spinello, Richard A. "Online brands and trademark conflicts: A Hegelian perspective." Business Ethics Quarterly Vol. 16:3. Jul. 2006. Pp. 343-367.

before the Internet existed.[20] Unfortunately, the U.S. and the EU have not been able to achieve the same cooperation with other countries. Currently, many countries, such as Vietnam and China, refuse to allow other states to seize domain names registered in their country resulting in the highest amount of cybercrime to be conducted under these domain names. For example, many torrent blogs are currently buzzing about the Chinese-based DVD ripping company DVDFab. DVDFab sells software that aids criminals in creating fraudulent copies of DVDs. The U.S. is currently failing to shut down the website and prosecute those responsible. Additionally, the defendant Feng Tao has created additional domain names that the U.S. does not have control over. Although all U.S.-controlled domain names that DVDFab was operating under have been shut down, other domains with DVDFab software for purchase are easily found through a Google search.[21] Considering the obstacles the U.S. has encountered in many states in ending the sale of fraudulent goods, it is important to recognize the vast cooperation between the U.S. and the EU on this issue.

Despite the lack of cooperation from other states, the U.S. and the EU cooperation to fight fraud and piracy is significant. The collaborative efforts of the U.S. and the EU add pressure to other countries to crack down on cybercrime. U.S. and EU policies and laws provide a model for other states to utilize when implementing their cyber security policies. Finally, by working together, the U.S. and the EU restrict the capabilities of cyber criminals. Although cyber criminals do have foreign outlets that allow them to

[20] Interview Erik Barnett 2 Oct. 2013.
[21] Ernesto. "US copyright law doesn't apply worldwide, 'DVD ripper' tells court." TorrentFreak. 24 Apr. 2014.

carry out their crimes, U.S.-EU cyber cooperation makes it increasingly difficult for these actors.

Discussion of the issues

Another form of Transatlantic cooperation on this issue is the EU-U.S. cyber security and cybercrime working group that has so far established the norms for cooperation on this issue. This working group seeks to explore the common concerns of both the EU and the U.S. There is a national security as well as an internal market component with regard to cyber security and cybercrime.[22] This working group meets at various times in order to facilitate discussion. Members are committed to staying up-to-date on the most relevant issues.

More concrete action needs to be taken in order to ensure cohesive regulatory systems aside from the working group. Without convergent regulation, differences will hamper the digital service deployment across the Atlantic. A lack of cohesion makes business difficult to conduct in both markets. The Transatlantic Trade and Investment Partnership that is currently being negotiated between the U.S. and the EU could formalize regulation in regards to cyber security and cybercrime. As trade negotiations are made, the two entities can outline cyber security standards for companies that do business online in both markets. The U.S. and the EU can make a concrete agreement that transcends Safe Harbor and fixes Safe Harbor issues. This would be a positive step in U.S.-EU cooperation on cyber security and cybercrime. Many politicians have noted the advantages of formalizing regulation in this trade agreement to the public. If regulation is not formalized, discussion of the topic is at least likely to take place during negotiations.

[22] Interview Ann-Sofie Ronnlund 21 Oct.2013.

The Network Information Security (NIS) Directive, which is a draft piece of legislation proposed by the European Commission that aims to create high levels of cyber security across the EU, also exhibits diplomatic policy cooperation through the NIS Platform that launched in the summer of 2013. This platform is a discussion amongst private and public actors that would be affected by the NIS Directive. This platform includes international players like those from the U.S. The European Commission has agreed to support any recommendations from this platform.[23] Although this is not conventional U.S.-EU public sector cooperation, it is important to note that American voices are involved with this platform.

[23] *Ibid.*

CHAPTER 4

WHERE THE U.S. AND THE EU FALL SHORT

There are a variety of barriers that the U.S. and the EU must overcome in order to cooperate to fight cybercrime and protect data privacy. The U.S. and the EU often fail to completely overcome these challenges as they persist in affecting policy. Bureaucracy, a lack of power in the EU, the need for negotiations bilaterally and multilaterally, and contrasting views on privacy specifically prevent cooperation potential from being reached.

Fragmented governments

The U.S. and the EU are bureaucratically fragmented. The European Commission, the part of the European government that takes initiative on creating legislation and acts as the executive branch of the EU, has many departments, or Directorate Generals (DGs), that work on cyber security and cybercrime. DG Home Affairs (HOME), DG Networks, Content and Technology (CNECT), and DG Internal Market and Services (MARKT) all consider cyber security and cybercrime as part of their portfolio. For instance, DG MARKT deals with internal market issues whereas (supra-) national security issues are the jurisdiction of DG HOME.[24] Furthermore, the EU has two legislative bodies, the Council of Ministers and the European Parliament. There is also the European Council

[24] Interview Ann-Sofie Ronnlund 21 Oct.2013.

that meets four times a years to discuss on EU issues. During any cooperation with the U.S., a large amount of negotiators on the EU side need to be consulted in order for cooperation to take place on the large spectrum that is cyber security and cybercrime.

Although the bureaucracy of the U.S. is in comparison to the EU, it is also split, which leads to difficulties in building foreign policy. "The U.S. foreign policy bureaucracy can be pictured as having four issue 'complexes': diplomatic, security, economic affairs, and intelligence. Each of these issue areas has actors and agencies that are not always in agreement nor are they on the same page. Overall, the U.S. foreign policy bureaucracy is highly fragmented and decentralized."[25] The definition of diplomacy is to make a deal with another country; cyber cooperation with Europe requires bureaucrats from this sector of the U.S. government. Security is a huge component to cyber security as law enforcement agencies and military fight crime and terrorism online. Economic affairs include online business that is conducted in the U.S. and the EU. Finally, intelligence is gathered in order to fight cybercrime. Cyber security is a foreign policy issue handled by all of these complexes making it a particularly difficult concern to conquer by the partners.

Furthermore, European agencies have little power compared to those in the U.S. "The EU is not the United States of Europe. It simply lacks the kind of power necessary to effect simultaneous changes in the policies of its constituent national governments."[26] The European Network on Information Security Agency, ENISA, assists member states by collecting best practices and disseminating them throughout the EU. However, this is

[25] Hook, Steven W. "Chapter 6. The foreign policy bureaucracy." U.S. Foreign Policy The Paradox of World Power Ed. 3. SAGE Publications 2014. Web. 26 Apr. 2014.
[26] Stevenson, J. "How Europe and America defend themselves." Foreign Affairs Vol. 82:2. Mar./Apr. 2003. Pp. 75-90.

an advisory agency that does not have the power to intervene in the case of a cyber incident. The European Cybercrime Centre receives assignments from member states rather than the EU.[27] This ultimately means that each member state has different capacities to fight cybercrime and retain cyber security. Furthermore, some cooperation must be bilateral because sovereignty is retained by member states.

The EU's proposed NIS Directive is attempting to add cohesiveness to the fragmented EU. This directive outlines a set of principles including member state capability levels and cooperation.[28] Cohesion has been outlined most explicitly as a goal of the EU with the Lisbon Treaty, which profiles "serious crimes" and encourages the European Parliament and Council to establish procedure and minimum rules in regards to cybercrime. The treaty also strengthens the role of Europol and Eurojust and provides the instruments for police cooperation.[29] Coherence on issues related to e-commerce within the EU is beneficial to the U.S. and any other international partners looking to create a market in the EU.

Multilateral versus bilateral cooperation

Transatlantic cooperation in the public sector can either be multi- or bilateral. Multilateral cooperation refers to cooperation of the U.S. and the EU (as a whole); bilateral cooperation is the cooperation of the U.S. and one of the twenty-eight member states of the EU. Multilateral cooperation has challenges. For example, the capabilities of the EU with regard to national security issues are still very limited due its supranational

[27] Interview Ann-Sofie Ronnlund 21 Oct.2013.
[28] *Ibid.*
[29] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice

legal nature and the remaining sovereignty of the member states especially when it comes to law enforcement.[30] Negotiating with one member state makes it easier to determine limits as compared to a negotiation with multiple actors. Many member states face different threats of terrorism; ultimately, the U.S. must cooperate with Europe either multilaterally or bilaterally for various forms of cyber security cooperation. However, if the U.S. were to interface with every EU member state, this would lead to fragmentation and administrative burden.

EU states' lack of centralized power results in a need to conduct some business bilaterally in addition to the various need based on various forms of cyber cooperation. The U.S. has a better relationship with some EU countries than others. This can be seen best when examining the relationship between the U.S. and the United Kingdom (UK). The relationship between Great Britain and the U.S. is frequently called the "Special Relationship" coined by Winston Churchill in 1946. Recently there has been strong British commitment to the wars in Afghanistan and Iraq which only strengthen the bonds of language and history, that stretch all the way back to the birth of the Thirteen Colonies.[31] When the National Security Agency (NSA) PRISM, a clandestine mass electronic surveillance data mining program, was revealed to the world, U.S.-EU relations hurt while the "Special Relationship" barely faltered. The U.S. and the UK often make bilateral agreements in order to conduct business given the nature of their relationship.

For many states, it is not in their best interest to conduct relations with the U.S.

[30] Interview Erik Barnett 2 Oct.2013.
[31] Woolner, David. "The 'special relationship' between Great Britain and the United States began with FDR." Roosevelt Institute. Web. Accessed 26 Apr. 2014.

bilaterally as the U.S. is an international powerhouse easily bend smaller member states to its will. Especially in this regard, it is to be noted that there is certainly is a huge difference when it comes to leverage. In order to visualize this, one can compare the U.S. and the European member state Malta with regard to size, economic power, and global influence. Depending on the problem the Transatlantic partners have to choose the method most suitable for the specific situation.

Balancing liberty and security

Although Transatlantic governments are often successful in their fight against cybercrime, many worry about the methods they employ. "It must be acknowledged that it [fighting cybercrime] can lead to criminalized conducts that are extremely problematic with respect to the harm principle—if not clearly in contrast with it—so highlighting the 'shadow side' of the concept."[32] Liberty is often overlooked, and privacy is violated in order to catch criminal actors. This begs the questions, what should governments and legislators be allowed to do? There is a question of whether governments should violate fundamental rights for the prevention or persecution of serious transnational crimes through "Internet search and seizure methods, clandestinely intercepting and searching for communication via the Internet, and/or to secretly access its information technology systems."[33] Margaret Atwood, George Orwell, and Ray Bradbury all warned the masses of totalitarianism and the cost of losing privacy. The Transatlantic powers face the challenge of fighting cybercrime and securing the privacy of the people.

The best way to understand the debate over FBI investigations on cybercrime is to

[32] O'Neil, Michael. "Cyber crime dilemma: Is it possible to guarantee both security and privacy?" The Brookings Review, Vol. 19:1. Winter 2001. Pp. 28-12.
[33] *Ibid.*

compare cybercrime to physical crime. Americans or Europeans would minimize the likelihood of burglary by allowing a law enforcement agent to live in their living room. However, most people do not prefer the resulting loss of privacy for the marginal increase in security. "Along with its efficiency, Internet users clearly cherish the anonymity and privacy the new technology affords them. Many users fear that their privacy rights will be diminished if the FBI [and other various law enforcement agencies are] out hunting for cyber crooks."[34] Monitoring cyber activity for security purposes threatens the popular idea that the Internet is an unregulated platform. Sharing, creativity, and mutual inspiration are assured by the very nature and architecture of the network environment.[35]

As criminal actors continue to endanger the livelihood of individuals, firms, and states, the U.S. has found what it believes to be "genuine prescience or unshakable convictions"[36] to gaining private information from internet users. The EU, however, is more prone to allowing constituents to retain their privacy. "In America privacy is seen as an alienable commodity subject to the market. Disputes about personal information as well as mechanism for its protection are cast in economic terms: questions about property rights; who 'owns' the data collected in a commercial transaction; and who has the right to the rents flowing from its exploitation. […] In contrast, the European approach to privacy puts the burden of protection on society rather than the individual. Privacy is considered to be a fundamental or natural right which is inalienable, and comprehensive systems of social or communitarian protection take the form of explicit statues

[34] *Ibid.*
[35] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice.
[36] O'Neil, Michael. "Cyber crime dilemma: Is it possible to guarantee both security and privacy?" The Brookings Review, Vol. 19:1. Winter 2001. Pp. 28-12.

accompanied by regulatory agencies to oversee enforcement."[37] Although the Fourth Amendment of the U.S. "prohibits unreasonable search and seizure," this does not seem to be relevant when cybercrime takes place, and those responsible are prosecuted. This fundamental difference in perceiving privacy makes cybercrime hard to fight and data privacy difficult to protect by both entities together.

[37] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.

CHAPTER 5

CONSEQUENCES OF FAILURE: WHAT SHOULD BE DONE

The most heinous criminal activity

As previously mentioned, the U.S. and Europe have made large strides in cooperation when it comes to combating cybercrime, the director of ICE was present on the opening of the EC3. Furthermore, "at a strictly operational level, we have witnessed a strengthening of operational police and judiciary tools as a part of an increasingly close focus on control and sanction: the setting up of specialist teams, covert investigation techniques such as communications surveillance, and the potentially never-ending option of accessing electronic storage, are some of the consequences of global enforcement." [38] This global enforcement and increased cooperation is largely due the U.S.-EU determination to fight child exploitation.

This can be seen through previous international agreements. The United Nations Convention on the Rights of the Child is approaching its 25th year as an active international agreement protecting children. Every member state of the EU as well as the U.S. has signed the Convention. Article 34 of the Convention states, "Governments should protect children

[38] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme. 2-4 Dec. 2011.

from all forms of sexual exploitation and abuse."[39] Then, the Convention supplements this article by adding the Optional Protocols to the Convention on the Rights of the Child, which draws special attention to the most serious violations of children's rights—sale of children, child prostitution, and child pornography.[40] This international treaty encourages the U.S. and the EU to do all in their power to protect children. Fostering further cooperation to track and prosecute these criminals is in their power.

Despite the strong cooperative relationship on a law enforcement level, this cooperation can be improved with inspiration from the U.S. law enforcement approach in the fight on narcotics during the 1980s and 1990s; it was made possible for judicially authorized wiretap recordings from Columbia to be used within U.S. courts.[41] A similar system on a Transatlantic scale in order to create a Global Evidence Locker (GEL) could greatly aid both governments as they attempt to fight child exploitation. GEL would be accessible by both Transatlantic partners. Admittedly, this solution is not only Transatlantic but global. But only through cooperation and initiative of both the U.S. and the EU together such a project can be realized and put on track in order to aid not only these but human societies globally.

The use of the evidence, however, would still be under the rule of law of each requesting member state. This guarantees that the legal customs and fundaments of each state are respected and that there is no breach of sovereignty. All evidence would have to be gained through judicial order, creating a basic level of quality and trust. Already, the Council of Europe created the Budapest Convention on Cybercrime and the U.S. is a

[39] The Convention on the Rights of the Child. UNICEF. Web. 26 Apr. 2014
[40] "Optional protocols to the Convention on the Rights of the Child" UNICEF 30 Nov. 2005. Web. 26 Apr. 2014.
[41] Interview Erik Barnett 2 Oct.2013.

signatory. The Budapest Convention on Cybercrime allows those states that entered into the agreement to contact other states at any time to request evidence for a cybercrime case.[42] The Budapest Convention on Cybercrime's main goal, however, is to allow the international community to create a common criminal policy. It has become a "model law" for many countries while drafting legislation.[43] Creating the GEL would be a more seamless process that would allow for a more rapid response to these fast paced crimes. Europol has the database control systems that make it ideal for regulating the GEL. Technological advances to create and run the GEL may need to be made by the Transatlantic powers to help Europol run this system.

How safe is the harbor

The FTC has taken action against major players in the cyber realm in order to protect the values that are enshrined in Safe Harbor documents. One action resulted in a 17 million USD fine for Google under Safe Harbor.[44] This 17 million USD fine was to 37 states accompanied by Google's agreement to "avoid using software code that overrides a browser's cookie-blocking settings, to avoid omitting or misrepresenting information to consumers about how they use Google products or control the ads they see, to maintain for five years a web page explaining what cookies are and how to control them, and to ensure that the cookies tied to Safari browsers expire."[45] Federal Trade Commissioner Julie Brill sites Google as one of the best examples of Safe Harbor working and protecting European citizens.

---

[42] *Ibid.*
[43] Manacorda, Stefano. "Cibercriminality: Finding a balance between freedom and security." International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice.
[44] U.S.-European Media Hub Interview Julie Brill 23 Sep. 2013.
[45] Miller, Claire Cain. "Google to pay $17 million to settle privacy case." The New York Times. 18 Nov. 2013.

Despite Commissioner Julie Brill's testimony to the success of Safe Harbor, its achievements are widely disputed. "As of 7 May, 2003 only 338 companies had enrolled, a few of them major multinationals. The relatively low number of firms which have signed up reflects concern about Safe Harbor combined with a sense that, at least at this point, the penalties for non-compliance are not very obvious."[46] 17 million USD along with Google's other penalties do not necessarily qualify as a significant punishment for violating Safe Harbor principles. Additionally, most American firms have negatively responded to Safe Harbor principles. These firms believe that entering Safe Harbor is too costly and does not make economic sense, it may be a precedent for future legislation in the U.S., and Safe Harbor will subject them to unforeseen liabilities.[47] Safe Harbor forces U.S. firms to follow laws of a foreign entity. Legal traditions in Europe and the U.S. are drastically different, resulting in discouragement from American companies.

Critics of Safe Harbor argue that is an ineffective self-regulating system. Many Europeans and privacy-legislation advocates have referred to the American system as "the fox guarding the hen house."[48] Many Americas saw the Data Protection Directive as an opportunity for the U.S. to create formalized regulation. Critics have called Safe Harbor a "weak, seriously flawed solution for e-commerce…[and] a mechanism to delay facing tough decisions about international privacy."[49] Europeans have been disappointed by the effectiveness of Safe Harbor as the organizations that due register fail to live up to

[46] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.
[47] *Ibid.*
[48] "U.S.-EU 'Safe Harbor' data privacy arrangement." The American Journal of International Law, Vol. 95:1. Jan. 2001. Pp. 156-159.
[49] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.

Safe Harbor principles. A European Commission Staff Working Paper issued in 2002 "found that a substantial number of organizations do not meet the requirement that they publish a compliant privacy policy and indicate publicly their adherence to Safe Harbor. Less than half of those organizations post privacy policies that reflect all seven Safe Harbor principles or inform individuals how they can proceed with complaints and a dispute resolution mechanism. It observes that no company has been prosecuted for making false statements."[50] In the end, Europeans and some pro-privacy Americans feel that Safe Harbor principles do not do enough to protect constituents, and American firms are not executing the compromise of Safe Harbor properly.

The U.S. protects European citizens through Safe Harbor, yet many have called for an end to Safe Harbor with the revelation of the NSA's PRISM program. Vice President of the European Commission Viviane Reding is highly critical of Safe Harbor due to these recent events.[51] By ending Safe Harbor, Europe would make constituents more vulnerable as the U.S. could not as effectively protect EU citizens. Ending Safe Harbor could also potentially eliminate many American companies from tapping into the European market. Some European politicians find this advantageous to the European economy. European innovators would be motivated to create companies to fill the gap where American businesses are eliminated. However, this is only a theory created by European politicians, and others believe "in a world where (electronic) cross-border data

[50] *Ibid.*
[51] European Commission "Informal Justice Council in Vilnius MEMO/13/710 19/07/2013." 19 Jul.2013. http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

flows are inevitable, that regulation must reach beyond the EU if is to be meaningful."[52] Without the implementation of something like Safe Harbor, the EU would not be able to effectively carry out its own Data Protection Directive. Ultimately, cutting off Transatlantic data flow would have catastrophic impacts on the European economy. Instead of the absence of American companies and data flow, the directive would be ignored.

Altogether, Safe Harbor was created in order to allow American firms to tap into the European market. The FTC has reported the success of Safe Harbor. Neither Americans nor Europeans are happy with the effectiveness of the implementation of Safe Harbor. Without Safe Harbor, the Data Protection Directive loses legitimacy, and Europe loses out on the vast e-commerce that takes places between the U.S. and the EU. Safe Harbor is a form of Transatlantic cooperation that needs to be revisited and altered in order to progress as partners.

The threat of terrorism

The World Economic Forum has a high prediction of an incident occurring that affects global critical infrastructures. It's a threat that is beyond every day concerns, but this threat is no longer science fiction. It is the responsibility of every government and public actor to take the precautionary measure to avoid such threat.[53] The U.S. and Europe face terrorist threats. Al Qaeda identified European targets as possible threats in a video in 2002, and the U.S. has remained a target as it has lent a hand in Middle Eastern

[52] Kobrin, Stephen J. and Steve Korbrin. "Safe Harbours are hard to find: The trans-Atlantic data privacy disbute, territorial jurisdiction and global governance." Review of International Studies Vol.30:1. Jan. 2004. Pp. 111-131.
[53] Interview Ann-Sofie Ronnlund 21 Oct.2013.

conflicts over the past century.

NATO is the best mechanism for international cooperation to prevent terrorism executed in the cyber realm. The U.S. and the EU public have "expressed their continued belief in the necessity of NATO." More than half of the respondents in the German Marshall Fund's public opinion survey previously cited found 58% of Europeans and 55% of Americans see NATO as "still essential."[54] NATO can facilitate the burden sharing and help protect member countries against terrorist threats. Currently, "NATO structures could, in theory, help fill the gap by coordinating efforts at counterterrorism and homeland security."[55]

NATO already works as a force to help the U.S. and the EU fight cybercrime, despite having no formal command to do so. "NATO has no explicit treaty obligations to defend cyberspace or the Internet from either military or non-military attack. The alliance none-the-less has moved quickly to develop new digital command and control capabilities to ensure that member states are better prepared to work collectively to thwart the type of catastrophic attack that crippled Estonia in 2007."[56] At this time, a series of cyber attacks against Estonia's banks, parliament, ministries, and newspapers most likely administered by Russia brought the country to its knees. Now, NATO has created the Cyber Defense Management Authority in Brussels to centralize cyber defense across the alliance. If similar cyber attacks were to occur, the alliance would have NATO

[54] The German Marshall Fund of the United States. "Transatlantic Trends Key Findings", 2013. http://trends.gmfus.org/files/2013/09/TTrends-2013-Key-Findings-Report.pdf
[55] Stevenson, J. "How Europe and America defend themselves." Foreign Affairs Vol. 82:2. Mar./Apr. 2003. Pp. 75-90.
[56] Hughes, Rex. "NATO in cyberspace: Digital defences." The World Today Vol. 65:4. Apr. 2009. Pp. 19-21.

to aid in defense.[57] However, with no formal obligations or rights, NATO must develop formal capabilities by its members in order to establish its absolute role in fighting cyber terrorism.

By utilizing NATO as force to fight cyber terrorism, the EU's can diverge from the international alliance. The doubt towards NATO from the U.S. comes from the belief that the U.S. should unilaterally act as a military power. However, the lack of trust in Europe stems from bitterness of many European states following the Iraq war. Europeans believe that NATO is no longer able to absorb the military developments since 1989.[58] Many are already calling for the unification of the EU and NATO. The bridging of these two organizations is not only imperative considering their vast resources, but the relationship would also reinvigorate the Transatlantic relationship during the pivot to Asia.[59] The bridging of the two organizations would increase the importance of NATO and its capabilities. Increasing NATO's role in fighting cyber terrorism, therefore, attracts this unification and grows NATO's proficiencies in fighting cybercrime.

[57] *Ibid.*
[58] Rynning, Sten. "NATO, the European Union, and the Atlantic community: The Transatlantic Bargain Reconsidered by Stanley R. Sloan." International Affairs Vol. 80:1. Jan. 2004. Pp. 123-124.
[59] Drozdiak, William. "The Brussels wall: Tearing down the EU-NATO barrier." Foreign Affairs Vol. 89:3. May/Jun. 2010. Pp. 7-12.

CHAPTER 6

CONCLUSION

To conclude, the Transatlantic partners are not reaching their full potential on cyber cooperation. Cyber security is a vastly important topic considering it affects individuals, firms, and states. The case studies of child exploitation, Safe Harbor Privacy Principles, and terrorism depict how trivial barriers prevent further cooperation. Bureaucracy and trust prevents the creation of the Global Evidence Locker, which would create a seamless process in tracking and prosecuting these heinous criminals who harm children. Clashing ideals on privacy prevent firms from accessing foreign markets and make constituents vulnerable to companies and hackers across the Atlantic. Privacy differences also prevent NATO from fully understanding their limits and their capabilities in preventing cyber terrorism. These parallels are easy to draw; however, all three issues could create more Transatlantic security if the two powers were able to overcome their fragmentation, multilateral versus bilateral barriers, and attitude and outlook on privacy rights.

Although the U.S. and Europe have been successful in various forms of cooperation, they must continue to progress. Comedian Will Rogers once stated, “Even if you’re on the right track, you’ll get run over if you just sit there.” Formalized regulation should be made through the Transatlantic Trade and Investment Partnership. All the discussion that is currently taking place needs to lead to concrete action. It is clear that

even current forms of cooperation hit similar barriers. A lack of cooperation on cyber security has catastrophic effects to individuals, firms, and states.

As in many other fields, the Transatlantic players through their knowledge, infrastructure, and resources have to presume a leading role in this fairly new fight against cyber threats. Similar to Greek heroes and demi-gods it is their responsibility to take charge and to guide the efforts through example and virtue in order to tackle this now global problem. To conclude the metaphor, it was only through cooperating and finding new ideas that in the end the Hydra could be conquered. In time, as the cyber realm constantly changes, there will be significantly more hurdles to come. The U.S. and the EU must overcome their differences now in order to achieve strategic goals if they are to tackle these future heads of the hydra.