Terms of Ab(Use): The Private Sector's Role in Maintaining Cyber-Security

By Chelsea Conard

Summer 2015

SIT Switzerland: International Studies and Multilateral Diplomacy
Dr. Gyula Csurgai
Dr. Alexandre Lambert
Dr. Oksana Myshlovka

DePauw University
Economics and Computer Science

Abstract

What is the role of the private sector in maintaining cyber-security? I examine the role of private sector, Kudelski Security, to analyze its performance in providing security measures for damaged clientele. I then relate the private sector to the public sector, indicating the inconsistencies in their relationship, but noting nonetheless of their mutual goal to prevent cyber crime. When considering the public sector, I introduce the European Union, as it is one of the biggest democratic blocks working to ensure the security of 500 million consumers. I argue that while the collaboration between the private and public sector is improving, there must be internationally accepted standards regarding cyber-security, or international threats will persist.

Preface

As expressed by the audacious Edward Snowden:

> The greatest fear that I have regarding the outcome for America, of these disclosures, is that nothing will change. People will see, in the media, all of these disclosures…But they won't be willing to take the risks necessary to stand up and fight to change things…in the months and years ahead it's only going to get worse, until there's a time where policies will change because the only thing that restricts the activities of the surveillance state is policy.[1]

Edward Snowden made his name by leaking classified information and terrorizing the world of the power held by national intelligence agencies. Despite the long existence of espionage in global economies, Snowden's abrupt news provoked massive disputes between national security and data privacy. Having followed the modern concerns surrounding data sharing and cyber defense, I was inspired to look further into the dangers of cyberspace. My interests in economics and computer science, and the optimal location of Geneva, Switzerland, afforded me an entry point to this complex field through the lens of a private sector. Additionally, I wanted to incorporate the voice of the most integrated regional block in the world, the European Union, to provide a public sector opinion. I hope that my analysis of the private sector may highlight the impending dangers in the cyberthreat landscape.

[1] "Edward Snowden: The Man Who Exposed PRISM." 10 July 2015.

Acknowledgements

While I feel that no message can quite convey the extent of my gratitude, I must first thank my parents, Barth and Lisa Conard, for their ceaseless support. I would also like to thank my sister, Ashley Conard, for serving as my mentor during my time here in Geneva.

I would also like to thank Jesper Haglund for his dependability, and for fueling my interest in the field of Political Science. Likewise, I would like to extend my gratitude to the Academic Directors, Dr. Gyula Csurgai, Dr. Alexandre Lambert, and Aline Dunant, for their contribution to this program's prestige. Additionally, I would like to thank my DePauw University Professors, Dr. Andrea Sununu and Dr. Brett O'Bannon, for offering their time and feedback on my paper. I would like to thank Bradley Dice for helping me prepare for interviews. I must, of course, also thank my host family, Therese Espinosa, for welcoming me into her home this summer.

Lastly, I would like to thank my fellow peers for sharing their remarkable insight and contagious enthusiasm with me. I will surely miss this community.

Table of Contents

Abbreviation List

EPP	*European People's Party*
EU	*European Union*
FYEV	*The "Five Eyes"*
IT	*Information Technology*
MEP	*Member of Parliament*
NATO	*North Atlantic Treaty Organization*
NSA	*National Security Agency*
SIT	*School for International Training*
TTIP	*Transatlantic Trade and Investment Partnership*
ULB	*Université Libre de Bruxelles*
UN	*United Nations*
U.S.	*United States*

I. *Introduction*

Edward Snowden sparked an international debate when he leaked details surrounding various National Security Agency (NSA) programs in July 2013. His outbreak revealed United States (U.S.) intelligence agencies' capacity to monitor phone calls and Internet communications of foreign citizens,[2] affirming the predominance of industrial espionage. Nevertheless, according to Business Development Manager for Kudelski Security, Mr. Patrick Antonietti, "everybody was spying on everybody, this is a fact. What was surprising was the scare in which it happened."[3] So, while the technology was long existent, its immediate alarm is what invigorated the demand for tougher privacy laws.

Despite the increased attention to cyber-security measures; however, cyber attacks have grown more sophisticated. As a result, the private sector has invested in high-level technologies to most efficiently respond to cyber threats. The objective of my study, therefore, is to examine the role of the private sector in maintaining cyber-security. From one lens, I will analyze a Swiss private sector, Kudelski Security, to see how it provides cyber security support. From another lens, I will study the European Union's (EU) current involvement with the private sector. The EU is indispensible to my research because of its role in the Internal Economy—it manages the cyber-security policies for all 28 member states surrounding Switzerland.

i. *Research Methodology*

Research for this paper was conducted through interviews and academic research in Geneva, Switzerland. Interviewees were walked through an ethical protocol, in which they were informed about the purpose of the research and assured their rights to privacy,

[2] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

[3] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

anonymity, and confidentiality. Upon their agreement, I held two interviews in person and a third over the phone. There were no ethical concerns with my topic; however, my first interview was conducted in French, so the interviewee signed a contract as a safeguard against a potential language barrier. In order of the interview, I spoke with Dr. Liran Lerman from Université Libre de Bruxelles (ULB), Patrick Antonietti a Senior Business Development Manager at Kudelski Security, and Tunne Kelam an Estonian Member of Parliament (MEP) for the European People's Party (EPP). I contacted all participants through my personal network.

The academic research was conducted at the United Nations (UN) Library and the School for International Training (SIT) Graduate Institute in Geneva. The UN databases, ProQuest and ResearchGate, provided original reports on Kudelski Security as well as documents about cyber security. I tailored my research methods to bear a multi-stakeholder design by including a representative from the private sector, a parliamentarian as an intergovernmental actor, and myself as a civil society member. The research design parallels the issue of cyber defense in my paper, as I am considering the role of the private sector and its ultimate relation to governmental bodies and private citizens.

ii. *Definitions and Analytical Framework*

Core to my paper, the private sector is the part of the economy run by individuals. Comparatively, the public sector encompasses all companies and corporations that are government run.[4] The two sectors differ primarily in that the private sector operates for profit while the public sector administers regulation.

When analyzing the private sector, I use such terms as: "The Five Eyes" (FYEV),

[4] "Private Sector." Investopedia, 25 Nov. 2010.

the deep and dark webs, competitive intelligence, cloud computing, zero-day, and the Transatlantic Trade and Investment Partnership (TTIP). FYEV is a secretive, global surveillance arrangement between Australia, Canada, New Zealand, the United Kingdom, and the United States. FYEV is one of the most comprehensive known espionage alliances in history. [5] The deep web is the portion of the Internet that is hidden from conventional search engines, while the dark web is a subunit to the deep web and is only accessible with a special web browser. [6] Competitive intelligence is the act of gaining knowledge about products, customers, and competitors in order to gain an economic advantage.[7] Cloud Computing allows service provider personnel to inexpensively store data, but hackers can theoretically gain control of huge stores of information through a single attack.[8] Zero-day is a technology that exploits a security vulnerability on the same day that the vulnerability becomes publicly or generally known.[9] Zero-day's information comes from the dark and deep web and must be used in secrecy.[10] TTIP is a free trade agreement between the U.S. and Europe with the intent of producing multilateral economic growth.

iii. *Literature Review*

The first group of existing research on my topic relates directly to the role of the private sector in maintaining cyber-security. In Susan Aaronson's "Data Protection and Digital Trade in the Wake of NSA Revelations," she explains that while the Internet belongs to all people in all states and no single government, and company or individual control its

[5] "The Five Eyes." Privacy International. 16 July 2015.

[6] Tyson, Bruce, and Mark Muller. "What's the Difference Between Deep Web and Dark Web?"

[7] "What Is Competitive Intelligence?" Fuld + Company, 2015.

[8] Lydon, Bill. "Cloud Computing."

[9] "Zero-Day Exploit." QuinStreet Inc., 2015.

[10] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

processes,[11] both she and the article "Edward Snowden: The Man Who Exposed PRISM" agree that the private sector takes advantage of its abilities and manipulates the data of its clientele.[12] Another source by Ben Worthen argues that despite the repeated efforts by the U.S. government to get the private sector to share information, private companies keep their work confidential and information is shared only voluntarily.[13] However, contrary to the idea that the private sector is endangering national cyber security, my interviewees Mr. Antonietti and Mr. Kelam recognize that the nature of the private sector is confidentiality; it will not risk its brand's credibility.[14][15]

The second group of my research was specific reports on Kudelski Security and specific reports related to Tunne Kelam. Kudelski Security is an innovative, independent Swiss provider of over 130 security experts who deliver tailored cyber-security solutions to financial institutions, the defense sector, government administrations, and the media industry. [16] Tunne Kelam is an MEP that advocates for more collaboration between the public and private sectors.[17]

The third group of my research related to terminology such as FYEV, Deep web, Dark Web, Cloud Computing, Zero-day, and information about the Estonian cyber attack in 2007. I defined the terms in the prior section. The cyberattack on Estonia was arguably

[11] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

[12] "Edward Snowden: The Man Who Exposed PRISM." 10 July 2015.

[13] Worthen, Ben. "Business Technology: Private Sector Keeps Mum on Cyber Attacks" 19 January 2010.

[14] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[15] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[16] "Kudelski Security." *Proactive Cyber Security Solutions in Europe*. 2015.

[17] Kelam, Tunne. "TUNNE KELAM." 13 July 2015.

inflicted by Russia in order to disable the Estonian government. But since the attack, Estonia has developed one of the most advanced cyber-security strategies.[18]

My fourth group of research is my interviews. The personal dialogue proved invaluable to my research because of the difficulty I faced to find relevant information in books or the Internet; specifically, on the relationship between the EU and the private sector, the functionalities of Kudelski Security, and the future possibilities in the competitive intelligence field.

II. The Role of the Private Sector

The private sector has the goal to protect the privacy of citizens; however, its ability to collect data on citizens has aroused serious debate about data privacy. Paradoxically, Mr. Kelam finds that "we as consumers are not as concerned with the private sector collecting and using our data. But that data is used to manipulate citizens."[19]

Since the dawn of the Internet, private sector companies built markets based on manipulating personal data in order to generate greater profit margins.[20] However, these private sectors are not always at fault, as they are functioning in a world deprived of internationally accepted standards regarding cyber-security.

i. Kudelski Security

Kudelski Security is a private sector that identifies vulnerabilities in its clients' networks in order to protect intellectual property, financial information, and brand reputation from cyber attacks.[21] According to Mr. Antonietti, Kudelski Security uses the dark and deep

[18] Aasmae, Kaly. "The Poster Child for Cybersecurity Done Right. 5 Fed. 2013.

[19] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[20] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

[21] "Kudelski Security." *Proactive Cyber Security Solutions in Europe*. 2015.

web to monitor their clients' physical network and detect any abnormalities.[22] However, Dr. Liran Lerman from ULB argues that "preventative measures against attacks are theoretical" because the invisibility of cybercrime makes full security unattainable.[23] But understanding the challenge, Mr. Antonietti notes that Kudelski overcomes with preparedness: "we must always be ready for a response under a legal framework…the definition of defense, in the military point of view, includes counter attacks and not just the need to defend oneself."[24] As a result, the company uses leading technology and works with such groups as the army and the secret service to provide best-informed protection.[25]

Another challenge to Kudelski Security is the sensitiveness of its field. Therefore, all appropriate measures are taken to gain the trust of its customers. According to Mr. Antonietti, trust is built "step by step by demonstrating capabilities, such as performing a background check."[26] Nevertheless, more skeptical customers demand that their partnership with Kudelski be concealed from FYEV, giving Kudelski the permission to engage in top-secret projects.

ii. New Technology

The maturation of the competitive intelligence field has encouraged the use of new technologies. The newest trend is cloud computing, which virtually provides unlimited computing resources without the cost of maintaining and owning powerful computers.[27] However, trans-border information is essentially traded in the cloud, and with 65 percent

[22] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[23] Liran Lerman, interviewed by Chelsea Conard, July 5, 2015.
[24] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[25] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[26] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[27] Lydon, Bill. "Cloud Computing."

of the world's population not yet online, the increased sharing of information could turn into e-commerce business objectives rather than the conservation of privacy rights.[28] Mr. Antonietti argues that the cloud is not a viable option unless it is managed, saying "in terms of security, you really have to trust your provider…in Switzerland, data protection lies in the demand to have data physically on Swiss soil."[29] As a result, unlike many, Mr. Antonietti does not use the cloud.

Another new technology with undefined issues is called zero-day. Valued at half a million dollars, zero-day has developed into a business in which individuals are buying it to use it as a tool or, in the case of Microsoft, using it to protect customers.[30] Mr. Antonietti believes zero-day to be "the best way to attack another system, because the value can be very high, depending on how specific or strong companies are."[31] Zero-day's impressive power rests in its invisibility; it must be secret to be used, so power struggles exist between those that own the technology and those that do not."[32] The use of zero-day is not technically illegal, so companies are implementing the technology, without questioning, not only to remain internationally competitive, but also secure.[33]

III. Relationship of the Private Sector with the Public Sector

While the private sector has an enormous aptitude in the field of cyber-security, it fears a loss in business because the general public doubts its ability to privatize data.[34] As a result, the private sector relies on the public sector to maintain its image and promote its

[28] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

[29] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[30] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[31] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[32] "Zero-Day Exploit." QuinStreet Inc., 2015.

[33] "Zero-Day Exploit." QuinStreet Inc., 2015.

[34] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

services. Likewise, the public sector depends on the private sector, but for means, experience, and staff. With matters of state security predominantly classified, the public sector must gather all information to fill its obligation, but then depend on the private sector to provide the technology. [35] Nevertheless, the sectors differ in the timing of their approach: the private sector advances quickly and focuses on the short term, while the public sector adapts to new technology more slowly, but has a long-term perspective upon the moment of investment.[36]

i. *Kudelski Security's relationship with Public Sector*

Public sectors have frequently partnered with Kudelski Security, owner of 4,500 issued and pending patents worldwide.[37] Currently, Kudelski Security has an agreement with Upc Cablecom, a cable operator, in which Kudelski technologies are used to ensure the secure exchange of information, and to implement assessments for an improved security posture for Upc Cablecom customers.[38] Likewise, Kudelski has an agreement with both Google and The Walt Disney Company, but their relationship grew out of a legal discussion for the use of particular technologies.[39] Ultimately, the companies decided upon a mutual sharing of patents. Now, Kudelski works with The Walt Disney Company, serving as its provider of media protection and value-added service technology, and helping to deliver their world-class entertainment platforms to the market through streaming video properties such as ESPN.com and ABC.com.[40] Lastly, Kudelski also partners with Zurich Insurance Group because Zurich had previously been providing

[35] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[36] "Private Sector." Investopedia, 25 Nov. 2010.

[37] "Kudelsi Group; Kudelski Group and the Walt Disney Company Sign Patent" ProQuest.

[38] "Kudelski Security and Upc Cablecom streghten." 24 Dec, 2014.

[39] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[40] "Kudelsi Group; Kudelski Group and the Walt Disney Company Sign Patent" ProQuest.

companies cyber-securing insurance. In the agreement, Zurich confirmed the use of Kudelski technology to implement 360-degree evaluations, for a tailored insurance policy to specific companies. Therefore, Kudelski assesses the risks of insuring a company, and, in the event of an attack, revitalizes the company.[41]

ii. *Inconsistencies between the Sectors as per the European Union*

Both the private and public sectors operate under mutual respect. For instance, if a private company has been the target of a cyber attack, it may safely report the event to relevant institutions in the public sector without compromising its social status. However, Mr. Tunne Kelam, an Estonian politician and member of the European Parliament (MEP) highlights the need for more cooperation between the sectors.[42]

As cyber problems are related to national and high-level security, both the public and private sectors work in very delicate spheres. Discussing the relationship between the private sector and the EU, Mr. Kelam says their partnership boils down to mutual trust: "if we can develop a certain measure of trust, we can work as partners. I would say the relationship is not symbiotic, but a constructive partnership; it is based on complementarity."[43] The EU finds its interactions with the private sector critical to fighting cybercrime and cyber attacks because the private sector owns most of the infrastructure.[44] Therefore, the European Commission has meetings with representatives from the private sectors. Nevertheless, the private sector plays no official role in negotiations because negotiations take place between institutions.[45]

[41] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[42] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[43] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[44] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[45] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

While the EU wants to involve the private sector as much as possible, Mr. Kelam argues that the relationship between the public and private sector is “counterproductive and needs an established balance.”[46] Their inconsistency is due to their conflicting instincts. The private sector is motivated be profit,[47] because according to Mr. Antonietti, “if you do not have money in the private sector, it is difficult to be effective. Credibility comes in the form of investment in products and solutions.”[48] Plus, working in a highly competitive field, the private sector is reticent to share delicate information. Unlike the private sector, however, the public sector works towards more and more regulation. But when regulated by the public sector, “the private sector finds a multitude of justified arguments,” Mr. Kelam argues, “and may find public sector intervention too harsh or too deeply involved in their business.”[49] Therefore, Mr. Kelam suggests that a constructive attitude by the public sector could stimulate the private sector to establish a balance between profit and common interests.[50]

iii. Estonia: Ideal Cyber-Security Management

Despite its victimization in a 2007 cyber attack, Estonia is now rated as having the most advanced national cyber-security strategy.[51] According to Dr. Lerman, the attack on Estonia was significant due to the involvement of multiple machines, for the cyber attack posed a threat from an incomprehensible number of offenders.[52] Yet Mr. Kelam argues that while some view the attack as untraceable, he found the connection to the crime quite

[46] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[47] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[48] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[49] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[50] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[51] Aasmae, Kalev. "The Poster Child for Cybersecurity Done Right” 5 Feb. 2013.
[52] Liran Lerman, interviewed by Chelsea Conard, July 5, 2015.

obvious.[53] The attack followed a riot organized by militant Russians and Russian agencies, making Mr. Kelam believe that the intervention was politically motivated to put pressure on Estonia, and to block its banks and ministries.[54] Nevertheless, Estonia only lost connection for half a day, so the attack was "nothing more than a nuisance," Mr. Kelam details.[55] Still, Estonia turned the negative event into a positive one by using the opportunity to refine its cyber-security policy. Today, 99.6 percent of banking transactions are done electronically and 40 percent of Estonians use their identification cards as digital signature, for the virtual form is as legal as a handwritten signature.[56]

So while the attack was later considered insincere, it did induce an immediate reaction process all over Europe. However, despite the trail that Estonia has blazed, Mr. Kelam believes "the process towards advancement is not yet complete, and could never be complete, because the hackers and criminals are running ahead."[57] He did mention, however, that the EU has caught up considerably.[58]

IV. Conclusion: Solutions to Private and Public Sector Tensions

The complications between the private and public sector all reduce to a difference in instincts. While the private sector looks for short-term, profitable opportunities, the public sector seeks long-term investment with increased regulation. Thus, as both sectors function on dissimilar foundations, tensions naturally arise between the two bodies. Nevertheless, current mechanisms have been effective with the intent of uniting both sectors in cause. Looking ahead, both sectors realize the value in their interdependent

[53] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[54] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[55] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[56] Aasmae, Kaly. "The Poster Child for Cybersecurity Done Right. 5 Fed. 2013.
[57] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[58] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

relationship, so they are advantageously working together to implement safeguards against future cyber attacks. Additionally, other solutions are in discussion to ameliorate the competitive intelligence field. Mr. Antonietti, for instance, revealed that there are projects to redesign the Internet.[59] On the part of the Parliament, Mr. Kelam disclosed that EU member states are creating a mechanism on how to help companies in cases of serious cyber incidents with the goal to create symbiotic outcomes.[60]

i. Core Findings

The objective of my research was to critically analyze the role of the private sector in maintaining cyber-security. I have discerned that the private sector's power is typically appropriately administered, as well as when paired with the public sector. However, with details hidden, and their work commonly top-secret, it remains difficult to make a decision. More research will need to be made if more information is ever publicized from the private sector. Notably, however, the use of undefined technologies—such as zero-day—makes for a gray-area as to the legitimacy of the private sector's work. Therefore, I have concluded that internationally accepted standards must be generated through collaboration of the part of the public and private sectors.

ii. Implications for the Future

With security issues becoming a high priority, Mr. Antonietti affirmed that companies are shifting towards investment: "Not as fast and as much as expected, but companies are going the right way. I am optimistic for the future."[61] He also stated that individually, citizens must be trained to be more careful, for "the more dependent we are on the

[59] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.
[60] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.
[61] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

Internet and connected devices, the more vulnerable we become…people must be more careful. It always was the case, now it is just most visible."[62] Education on cyber-security matters must therefore increase.

Looking to the future, Mr. Kelam contends that most cyber-security attention has been concentrated on the relations between the U.S. and Europe, when the primary threats are coming from China, Russia, and Islamic terrorists. [63] Therefore, he suggested that TTIP could provide a historic change to unite the forces of the two biggest democratic blocks based on the rule of law.[64] Mr. Kelam says, "it has been stressed that if we do not succeed now in creating a unified free market, then in ten years time, there will be other powers that create agendas in a not so democratic way. Therefore, we must realize who are our friends and who are our competitors or adversaries."[65] However, data protection rules are a big issue bedeviling negotiations for TTIP, so internationally accepted standards will continue to be long overdue. [66]

[62] Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

[63] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[64] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[65] Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

[66] Aaronson, Susan Ariel. "Data Protection and Digital Trade in the Wake of NSA Revelations." *281-285*.

Bibliography

Aaronson, Susan Ariel. “Data Protection and Digital Trade in the Wake of NSA Revelations.” *EU Data Protection Reform: Opportunities and Concerns.* By Rob Maxim. N.p.:ZBW – Leibniz Information Centre for Economics, 2014. N. pag. Print.

Aasmae, Kalev. "The Poster Child for Cybersecurity Done Right: How Estonia Learnt from Being under Attack." *ZDNet*. CBS Interactive, 5 Feb. 2013. Web. 13 July 2015.

"Edward Snowden: The Man Who Exposed PRISM." *RT Question More*. Autonomous Nonprofit Organization, 25 June 2015. Web. 10 July 2015.

Kelam, Tunne. “TUNNE KELAM.” *Eesti East Euroopas.* Tunne Kelam, 2 Dec. 2008. Web. 13 July 2015.

"Kudelski Group; Kudelski Group and the Walt Disney Company Sign Patent License Agreement." Journal of Engineering (2015): 910. ProQuest. Web. 15 July 2015.

"Kudelski Security." *Proactive Cyber Security Solutions in Europe*. Kudelski Security, 2015. Web. 13 July 2015.

“Kudelski Security and Upc Cablecom strengthen.” *News Bites*. 24 Dec, 2014. ProQuest. Web. 15 July 2015.

“The Five Eyes.” *The Five Eyes.* Privacy International. Web. 16 July 2015.

"Transatlantic Trade and Investment Partnership (TTIP)." *European Commission*. European Commission, 1 Apr. 2015. Web. 16 July 2015.

Tunne Kelam, interviewed by Chelsea Conard, July 14, 2015.

Tyson, Bruce, and Mark Muller. "What's the Difference Between Deep Web and Dark Web?" *Bright Hub*. BrightHub, 12 Aug. 2013. Web. 16 July 2015.

Liran Lerman, interviewed by Chelsea Conard, July 5, 2015.

Lydon, Bill. "Cloud Computing." INTECH 62.3 (2015): 12-5. ProQuest. Web. 15 July 2015.

Patrick Antonietti, interviewed by Chelsea Conard, July 8, 2015.

"Private Sector." *Private Sector*. Investopedia, 25 Nov. 2010. Web. 16 July 2015.

“What is Competitive Intelligence?” *Fuld + Company.* Fuld + Company, 2015. Web. 16 July 2015.

Worthen, Ben. "Business Technology: Private Sector Keeps Mum on Cyber Attacks --- Companies are Loath to Disclose Or Share Information on Breaches for Fear of Bad Publicity and Loss of Business to Rivals." Wall Street Journal, Eastern edition ed. Jan 19 2010. ProQuest. Web. 15 July 2015

"Zero-Day Exploit." *Webopedia*. QuinStreet Inc., 2015. Web. 16 July 2015.

ISP Work Journal

Wednesday, June 10th

Read:

- Past projects on International Economics and Trade relating to e-commerce, conflicting currencies, and international financial regulation

Friday, June 12th

Read:

- Past projects on Global Commerce and Corporate Inversion

Saturday, June 13th

Emailed:

- Jesper Haglund for a potential interview with EPP

Thursday, June 18th

Discussed:

- Potential topics with Dr. Lambert. Focused on cyber security issues.

Saturday, June 20th

Discussed:

- Cyber security with Mr. Christophi and received contact information for Patrick Antonietti

Monday, June 22nd

Emailed:

- Jesper Haglund about a follow up for email options with EPP
- Patrick Antonietti from Kudelski Security about my interest in an interview
- Bradley Dice about a potential interview with an expert on cyber security at CERN

Read:

- Articles from the Electronic Frontier Foundation

Wednesday, June 24th

Emailed:

- Patrick Antonietti to confirm our meeting for July 8th.

Read:

- Articles on data protection to consider the topic

Monday, June 29th

Read:

- Articles on EU legislation-specifically the EU report on cyber security

Tuesday, June 30th

Discussed:

- Potential paper topics: either data protection in the EU or cybersecurity

Saturday, July 5th

Discussed:

- Cyber security with Dr. Lerman at Université Libre de Bruxelles

Wednesday, July 8th

Discussed:

- Kudelski Security with Mr. Antonietti

Thursday, July 9th

Emailed:

- Mr. Antonietti to thank him for his support.
- Mrs. Kadri Vanem to coordinate my interview with Mr. Tunne Kelam

Friday, July 10th

Emailed:

- Mrs. Kadri Vanem to discover that my interview is delayed temporarily

Monday, July 13th

Emailed:

- Mrs. Kadri Vanem to confirm my interview with Mr. Tunne Kelam for Tuesday morning at 9-10 CET or 10-11 in Estonia.

Tuesday, July 14th

Discussed:

- EU perspective with Mr. Tunne Kelam

Read:

- Articles on cyber attacks in Estonia and reports on Kudelski Security
- EU legislation on cyber defense and Mr. Kelam's initiative

Wednesday, July 15th

Read:

- Articles on the Private Sector and the relationship between the Private and Public Sector.

Thursday, July 16th

Read:

- Articles on The Walt Disney Company, Upc Cablecom, Competitive Intelligence, Cloud Computing, and TTIP.

Friday, July 17th

Emailed:

- Jesper Haglund, Mr. Tunne Kelam, Mr. Patrick Antonietti, and Dr. Liran Lerman copies of my finalized paper.

I. Questions for Liran Lerman[67]

- *To begin, please explain your work.*
- *Please explain your perspective of the relationship between security and technology.*
- *What attracted you to this field?*
- *What fears do you have for the future in terms of security?*
- *What is your opinion on the private sector's influence on the politics of cyber defense?*
- *Is there a particular form of legislation that you find beneficial to the world of cyber defense?*

Write-up:

Dr. Liran Lerman helped me contextualize the importance of security measures in modern society. He instructed me on the protocols to exchange information, as well as the individuals or motivations involved in a cyber attack. Essentially, preventative measures against attacks are theoretical because cybercrime has come in that we cannot see. Additionally, he said that attacks come in three forms: from an individual, a group of individuals, or a country/state. The motivations come from a variety of sources, but most predominant are from: financial interests, political reasons, religious purposes, and/or educational purposes to teach the next generations of hackers. I was most intrigued by Dr. Lerman's belief that "everything is possible to attack" and there are "no perfect solutions; otherwise they would already be in place." While Dr. Lerman advocated more collaboration between countries, he said that the possibility for secret interactions makes him fear the future of the Internet. Consequently, he thinks the only counteractive measure is to completely rethink the Internet, especially when considering the rise of artificial intelligence. Reflecting on the 2007 cyber-attacks on Estonia, Dr. Lerman said he fears the untraceable use of multiple machines in complicated attacks. Above all, however, he fears religious affiliated attacks, because unlike the status quo, the programmers wish to be connected to the attacks so to promote their cause. As a result, their crimes are expensive and have the potential to provoke worldwide conflict.

II. Questions for Patrick Antonietti

<u>Current Performance</u>*:*

- *Please begin by contextualizing the importance of your work for industries and governments.*
- *What fears do you have on your company's increased use of cloud computing? How can you assure the security of critical assets?*

<u>Functionality:</u>

- *How does Kudelski Security identify vulnerabilities before exploitation by hackers?*
- *How have your strategic international partnerships promoted your company (UPC Cablecom, Zurich Insurance Group, Google, Walt Disney Company)?*

<u>Opinion:</u>

- *How can the public industry stay a step ahead of potential threats?*
- *What is your take on the belief that all can be hacked?*

[67] Note: Interview was conducted in French, so all information is a direct translation.

Role of the Customer:

- *What is the role of the customer in reading the terms and conditions? Do you believe a client should request clarification of security compliance rules or is it feasible that he/she blindly consents?*
- *What type of regulation has your company put into place to ensure the trust of its customers?*

Write-up:

A business development manager, Mr. Antonietti works in the defense sector to take care of the security of the country through the protection of its companies. He explained that cloud computing offers an advantage to smaller sized companies to outsource the IT infrastructure in its cost saving abilities. However, he argued that the cloud is not a viable option unless it is managed. Mr. Antonietti also discussed Kudelski's relationships with other global players. To begin, they partner with UPC Cablecom, a cable operator, so that it resells their security to customers. Additionally, Kudelski has a similar type of agreement with both Google and Disney because they needed to overcome a legal discussion about the use of particular technologies. Today, they have an agreement allowing a symbiotic use of their patents. Lastly, Kudelski formed a partnership with the Zurich Insurance Group.

When asked his take on the belief that all can be hacked, Mr. Antonietti stated that the definition of defense, in the military point of view, includes counter attacks and not just the need to defend oneself. He agrees that is it impossible to be 100% protected in his field, but he must always be ready for a response under a legal framework. By working with the army as well as the secret service, Kudelski can use collaborative means to provide the best-informed protection.

When asked to consider the future of his business, Mr. Antonietti believes the future is bright. He recognizes that there is "still a lot to do, but a lot of companies are thinking of what can happen." He reflected on the news of a recent Italian Hacking Company getting hacked, "Even hackers get hacked, we don't know where we're going. It's quite scary. The more dependent we are on the Internet and connected devices, the more vulnerable we are. It's getting worse and worse. But we have to be optimistic. We must train the people to be more careful." Mr. Antonietti also stated that cyber attacks only take one success out of multiple attempts to work; so all types of missions are possible. He then discussed the implications of Zero-Day: "that's the best way to attack another system—the value can be very high, depends on how specific or strong companies are. However he identified that the problem with zero day is its invisibility; it must be secret to be used, so power struggles exists between those you own the technology, and those that do not. "More software you write, more software companies are publishing, more zero-days there will be."

When asked to discuss his NSA cyber espionage, Mr. Antonietti said that "everybody is spying on everyday, this is a fact. What was surprising was the scare in which it happened." Mr. Antonietti also shared that because the US image has been affected by NSA activities, some of his clients required that their participation be exempt from the five eyes. He concluded the topic saying, "people must be more careful with what they do-not be naïve. It always was the case, now it's just more visible. He then discussed security in general, to say, "State security has a lot of information that cannot *be shared." Therefore, Mr. Antonietti finds the field challenging because security is on a need to know basis, so he must be careful what he says, publishes, or communicates.*

Mr. Antonietti stated that as far as funding, credibility comes in the form of investment in products and solutions: "It you don't have money, it's difficult to be effective." Nevertheless, he revealed that many companies are shifting towards investment, as security issues are becoming high priority: "Not as fast and as much as expected, but companies are going the right way. I am optimistic for the future"

III. Questions for Tunne Kelam

General

- *Working in a parliament that represents 500 million consumers, how do you safeguard your personal data in this parliament? I ask to learn more about the security measures the EU institution has put into place to protect itself from illicit activity while simultaneously regulating one of the largest markets in the world.*
- *What is your role in the multinational dialogue of cyber defense?*
- *What efforts have been made to work jointly with other EU institutions on this sensitive topic?*

Private Sector

- *How will private sectors be affected by EU legislation?*
- *Please describe the interaction between the EU and the private sector. Is the relationship symbiotic?*
- *Further, what is the role of the private sector in current negotiations?*
- *What challenges do you face when working with the private sector?*

Technology

- *How has the newest trend of cloud computing been perceived on the part of the EU?*
- *Is Zero-day a significant discussion topic at the EU?*

Estonia

- *What were the lessons learned by the EU on the cyber attacks on Estonia in 2007?*
- *How did the EU legislatures (Parliament; Council of Ministers) respond to the attack?*
- *Please speak to NATO's establishment of a cyber defense center in Estonia.*

Opinion

- *In considering the current direction of your field, do you think that sovereign states may lose their sovereignty in years to come?*
- *With foreign countries seen as more powerful in particular areas of technology, how does Europe cope with its potentially defensive posture?*

Write-up:

Mr. Kelam recommended the requirement of all Parliament staff members to undergo training on cyber-security to ensure that all portable devices have anti-virus programs. In response to his suggestion, Mr. Kelam states, "this is one of the ideas presented in my report on cyber-security and cyber defense. This was only a call for action, but the action has yet to happen. Mr. Kelam's report reacted to the need for better national cyber-security strategies. He suggested such ideas as: improved EU relationship with the rest of the world, cooperation with US and NATO, and increased training and *education. His most highlighted point was his desire for a mainstreaming of cyber-security into external policies.*

Mr. Kelam spoke to the relationship between the public and private sector. He said that the private sector has an obligation to critically protect infrastructures. Nevertheless, a minimum standard for more cooperation has been encouraged. Discussing the EU and the private sector, Mr. Kelam believes their relationship to be improving and he is optimistic. The relationship between the EU and the private sector boils down to mutual trust. Mr. Kelam says, "if we can develop a certain measure of trust, we can work as partners. I would not say the relationship is symbiotic, but a constructive partnership; it should be based on complementarity." He also explained that the European Commission has meetings with representatives from the private sector. Their interactions are due to the private sector owning most of the infrastructure, so their involvement is critical to fighting cyber crime and cyber attacks. Nevertheless, the private sector plays no official role in negotiations because negotiations take place between institutions. The EU wants to involve the private sector as much as possible, in order to develop a constructive corporation while ensuring that confidential incident reporting takes place.

Mr. Kelam states "the private sector is essentially motivated by profit. It's a fact of everyday life." He also explains that profit means for hard competition, so there are problems with sharing delicate information. Therefore he suggests that a constructive attitude by the public sector could stimulate the private sector to establish a balance between profit and common interests. Yet of course, the private sector finds a multitude of justified arguments and may find intervention on the part of the public sector as too harsh or too deeply involved in their business. In other words, both partners have their basic instincts: the private sector has its profit instinct and the public sector has its instinct for more and more regulation. This relationship is counterproductive and needs an established balance.

Mr. Kelam spoke to the systematic cyber attacks on Estonia. He finds it interesting that Estonia could turn a negative event into a positive one by concentrating on cyber-defenses and cyber-security so to do something positive after an attack. Estonia was the first to develop its national cyber security strategy, and they involved all governmental institutions. According to Mr. Kelam, the attack was not a very serious signal, but it did induce a reaction process all over Europe. The process is not yet completed, and could never be completed because the hackers and criminals are running ahead. However, Mr. Kelam believes that the EU has been catching up considerably.

Interactive Log

Organization	Key Contacts	Email Address	Date	Type
Université Libre de Bruxelles	Liran Lerman	llerman@ulb.ac.be	July 5	Formal
Kudelski Security	Patrick Antonietti	patrick.antonietti@nagra.com	July 8	Formal
European Parliament	Tunne Kelam	kadri.vanem@europarl.europa.eu	July 14	Informal