Leiden University

Faculty of Humanities

Master of Arts in International Relations

MA Thesis International Studies

Cyber threats and cybercrime – a disruption of human security?

Master Thesis

Tutor: Dr. Andrew J. Gawthorpe

Student: Silja-Madli Ossip

Brussels 2017

Table of Contents

1. Introduction

Cyberspace is everywhere in the world nowadays – all our activities are connected to the internet, devices are connected to each other and at least part of our life takes place online. Although it makes daily life easier and faster most of the time, sometimes people do not apply the level of protection in the online sphere, as they do offline. Crime takes place no matter the space, and the digital sphere has enabled a new world where crime is becoming even more common due to the easy access and anonymity. Cybercrime does not have geographical boundaries or time restrictions; instead, it is becoming easier to commit fraud online. We expect that companies and/or state bodies are the most common targets of cybercrime through stolen data, information leakages, cyber espionage, etc. while less attention has been drawn to the people affected by these attacks. Nevertheless, even though individuals may not be the primary targets of cybercrime, they can become indirect victims.

Cyber threats might seem less harmful than physical threats, but as our everyday lives have partly moved online, more attention should be paid to these threats and individuals should secure themselves online as much as possible. Whether or not cybercrime has a direct threat on or even a connection to human security has not been discussed much. However, it should be an important debate considering the digital era of today, creating the need for people's online protection against security disruptions. Human security in relation to cyberspace is shifting away from physical threats and towards psychological harm. Cyber awareness among people, such as knowledge about existing threats and their prevention in the online world is often considered the weakest link in the chain of committing a crime. Meaning people's unawareness of cybersecurity practices might be causing their own human security disruptions. This is an important topic to discuss considering how the digital era might be changing the concept of human security.

Firstly, the author will search for the relationship between the individual and cybersecurity through a deeper research on the subject of cyberspace and the threats that it poses to internet users. In addition, the author will make a connection between *cyber* security and *human* security to see whether the two can be connected. Second part of the paper will analyse the level of awareness of potential cyber threats among internet users using the empirical data taken from an online survey of 220 participants. Finally, the results of the survey will be analysed through human security concept to explore the level of disruption created by different threats and suggest ways in which individuals can live safely in the online world.

2. Literature review

This section will cover academic knowledge and expert views concerning the online world and the threats it poses to internet users. The first part will introduce the topic of cyber space and provide an overview of the current debates about its potential damages upon states and individuals in today's world. The second part will explain in detail existing cyber threats from an individual's perspective and will provide a basis for further analysis. Finally, yet importantly, the connection between the human security concept and the cyber sphere will be made, which will act as the central importance to the analysis.

2.1. Cyber space in today's world

The extensive cyber operations against the Estonian governmental and telecommunications' websites in 2007 acted as a wake-up call around the world. Beforehand, cyber incidents had been dealt with in isolation but since then the scope of malicious cyber activities has expanded and states have come up with new strategies to address these issues. Many security experts have since declared that advanced information technology systems must be dealt with great safeguard.[1]

The focus of the paper will be individual-based, but it is first necessary to understand the larger debate on cyberspace and how the cybersecurity field is perceived in relation to increasing level of cyber threats. Not only are cyber incidents becoming instruments to show strength in the online world, some experts claim they are even considered to represent a new type of war. There are two sides to this argument – some do believe that future wars will occur in cyberspace, whilst others believe that cyber wars as such do not exist and will not come to being in the future either. Until today, very few cyber-attacks have caused any serious harm and none of them have created casualties.[2] Rid, a strong supporter of the reasoning against cyber wars, believes according to Clausewitz, that war has traditionally been associated with a strong notion of violence and is arranged on the political level between states. In his view, all the scenarios of lethal cyber-attacks remain fiction.[3] On the other hand, Stone challenges Rid on his interpretation of Clausewitz's definition of war, asserting that it should be seen as an act

[1] Tikk, Eneken. (2011). "Ten Rules for Cyber Security". *Survival*, Vol. 53, No. 3, p. 119
[2] Baylis, John, James J. Wirtz & Colin Gray. (2015). *Strategy in the Contemporary World*. Oxford: Oxford University Press, Ch. 16, p. 285
[3] Rid, Thomas. (2012) "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, pp. 7-10

of physical force rather than a direct notion of violence[4]. He believes that the historical claim about every act of war needing to be lethal and attributed does not mean this idea stays the same in future wars.[5] Rid and Buchanan argue that attribution in the cyber sphere is what the states make of it and has evolved significantly in past years, becoming more nuanced and common[6]. They believe that attribution is necessary so that cyber-attackers would not feel they "can cause serious harm and damage under the veil of anonymity and get away with it"[7]. However, whether attributed or not, future wars through cyber-attacks could potentially cause violence and lethality, according to Stone[8].

To bring the narrative of the much-debated cyber wars to a more realistic level, maybe cyber power should be rather dealt with as a particular way to support warfare, not as warfare itself[9] and cyber incidents as "acts of force whose outcomes are augmented by technology"[10]. According to Singer and Friedman, the hardest to clarify is the middle ground between incidents of actual destruction and incidents of major disruption, like the DDoS attacks in Estonia in 2007[11], which involved attackers from 178 countries, including botnets but also internet users carrying out the attacks voluntarily based on instructions given in internet forums[12]. The reason why the cyber-attacks against Estonia have been considered as a benchmark was that "never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back"[13]. What is more, the attacks might have been directed against the Estonian state, but the majority of the general public was in fact affected, as major banks, telecommunication providers, media outlets, etc. fell victims to the attacks[14]. Although the Estonian government believed the attack had been a security threat to the sovereignty of the country and turned to NATO for help, other member states saw it more as "bullying" in cyber space and gave their support to help handle the effects

[4] Stone, John. (2013). "Cyber War Will Take Place!", *Journal of Strategic Studies*, Vol. 36, No. 1, p. 106
[5] Ibid., 105
[6] Rid, Thomas, Ben Buchanan. (2015). "Attributing Cyber Attacks". *The Journal of Strategic Studies*, Vol. 38, Nos. 1–2, p. 7
[7] Ibid., 31
[8] Stone, 105
[9] Baylis, Wirtz & Gray, 286
[10] Stone, 106
[11] Singer, Peter W. & Allan Friedman. (2014). *Cybersecurity and Cyberwar; What everyone needs to know.* New York: Oxford University Press, p. 124
[12] Tikk, Eneken, Kadri Kaska & Liis Vihul. (2011). "International Cyber Incidents; Legal considerations". *Cooperative Cyber Defence Centre of Excellence (CCD COE)*, p. 23
[13] Wired Magazine. (2007). *Hackers Take Down the Most Wired Country in Europe*. Available at: www.wired.com/politics/security/magazine/15-09/ff_estonia [Accessed July 21, 2017]
[14] Ibid.

of the attacks in Estonia[15]. As there were no physical casualties or damages, the cyber-attacks were not considered as an act of war, and NATO's Article 5 of collective defence was not implemented.[16] Even though cyber warfare might still remain fiction in today's world, or cyber power without a clear definition and attribution, this does not mean that cyber threats are less concerning to states and citizens.

Since the attacks against Estonia ten years ago, many new cybersecurity regulations have been created in order to protect civilians in the cyber sphere. According to Tikk, malicious cyber activities also "test the limits of the existing legal framework for data protection, electronic communications, and access to public information", which is directly linked to people's protection online[17]. The Tallinn Manual 2.0, consolidated by a group of legal and technical experts from the field, explores ways in which the international law is applicable to cyber space and cyber operations, offering a close view on laws, regulations and treaties protecting civilians and their security around the world[18]. Cyber-attacks by Tallinn Manual rule 92 have been defined as operations that create physical "injury or death to persons", but also "damage or destruction to objects"[19]. This definition includes disruptions against individual-owned objects in the same way as it includes attacks against humans. Rules 93 and 94 from the manual prohibit cyber-attacks targeting civilians or civilian objects by declaring these actions as unlawful when the intent is to deliberately create damage[20]. However, rule 33 of Tallinn Manual states that international law does not regulate cyber-attacks performed by non-state actors, meaning that in the eyes of the law, they do not violate states' sovereignty, represent intervention, nor are defined as an act of force[21]. However, from the perspective of an individual, it cannot be assumed that only state actors can commit cyber-attacks, especially as the attribution of an attack is complex. This is why this paper will not be looking at the attribution issue; neither will it focus only on state actors. More importantly, the matter of this paper is to observe cyber threats and attacks where civilians and their security are considered to be in danger.

Ülgen concludes in his report about governing cyberspace that although the Internet has made people's lives easier in many ways, it has also made them more vulnerable. Hackers steal money, identities, or research, which creates greater threats to the economies and

[15] Singer & Friedman, 122
[16] Ibid.
[17] Tikk, 119-120
[18] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Tallinn: Cambridge University Press, pp. 2-3
[19] Ibid., 415
[20] Ibid., 422-423
[21] Ibid., 175

infrastructures of states and to the prosperity of companies and people.[22] Ülgen does mention that the debate regarding cybersecurity has been brought out to the public more and the general awareness among people of how their personal data could be used for malicious purposes is growing[23]. However, existing studies are still very much focused on states' policies on cybersecurity, not so much upon the impact on the individual. Vacca argues in his study, that morale plays a particularly important role in the cyber domain, as it is very closely connected to the emotional behaviour among the general public[24]. This type of security threat in the cyber sphere is called a social engineering attack, when people are influenced through psychological manipulation to comply with the demands of an attacker or to reveal personal information[25]. Singer and Friedman also provide examples of how much cybersecurity and human behaviour are connected. They believe that cyber attackers play on people's trust, so often people themselves, unconsciously or trustingly, insert computer worms or viruses into systems by clicking on infected links and attachments or inserting external drives into their computers.[26] It is for this reason humans can be seen as the weakest link in combatting cybercrime. That does not mean all the people in the world should be knowledgeable about every detail connected to the internet and the online world, but that people should be more aware of the threats out there that can be harmful to their own personal security, not just on a state level. This paper will be using the term cyber awareness as "real-time understanding of the security risks online"[27], reflecting on people's individual knowledge about existing cyber threats, their abilities to identify and react to them; it will not consider people's capabilities to use connected devices. All the potential cyber risks will be explored in the next chapter.

2.2. Cyber threats' landscape

The discussion around cyber threats has gained significant momentum in the past years. Countries are taking stands and creating strategies to predict cyber threats, but also to prepare the public from potential risks.[28] Cyber threats are seen as equal to cybercrime – "a term used

[22] Ülgen, Sinan. (2016). *Governing Cyberspace; A Road Map for Transatlantic Leadership*. Carnegie Endowment for International Peace, Ch. 6, p. 51
[23] Ibid., 52
[24] Vacca, W. Alexander. (2011). "Military Culture and Cyber Security". *Survival,* Vol. 53, No. 6, p. 167
[25] Mouton, Francois, Louise Leenen & H.S. Venter. (2016). "Social engineering attack examples, templates and scenarios". *Computers & Security,* Vol. 59, p. 187
[26] Singer & Friedman, 65-66
[27] Amoroso, Edward G. (2011). *Cyber attacks: Protecting National Infrastructure*. Burlington: Butterworth-Heinemann, p. 179
[28] Lewis, James A. (2014). "National Perceptions of Cyber Threats". *Strategic Analysis,* Vol. 38, No. 4, p. 568

to describe violence below the level of state-to-state armed conflict, which includes non-state actors and which can involve disruptions of critical infrastructures or politically disruptive acts"[29]. This section will give an overview of the threats and crime in the cyber sphere an internet user individually might be exposed to. Additionally, it will explore people's awareness in relation to the measures of "hygiene" that should be kept online to protect human security.

An internet user generally faces three different types of security risks: 1) *stolen data* that might reveal their own personal work or strategic plans; 2) *misused credentials*, which might have the ability to destroy or change personal data; and 3) *hijacked resources* such as taking control of an individual's online finances.[30] To identify the exact threats that will be discussed and later analysed in this paper, the author has used a threat landscape report assembled by the European Union Agency for Network and Information Security (ENISA)[31]. This report covers the top 15 cyber threats that have interchangeably been affecting internet users in 2015 and 2016 (Appendix 1). It gives an overview of the most common cyber threats and their trends, and a brief explanation of each threat is provided below. It is important to note, that very often neither of the threats are lone-standing and might be a result or a prerequisite to one another.

1. Malware, short for malicious software, might act as a "worm" that spreads itself through the network, or creates so-called instructions to the victim of what to do after being hit. Malware might cause loss of data and/or device malfunctions.[32]

2. Web-based attacks exploit vulnerabilities in web components and add-ons, and use them as a surface to compromise a server or a website. Internet users are attacked on infected and manipulated web sites; often a certain target group are specially focused upon[33].

3. Web application attacks have overlaps with web-based attacks, but their main sources are web-based or mobile applications. Public applications are an easy target, and create so-called threat agents who continue transferring and sharing vulnerabilities.[34]

[29] Ibid., 567
[30] Singer & Friedman, 39
[31] European Union Agency for Network and Information Security (ENISA). (2017). *ENISA Threat Landscape Report 2016*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Accessed March 20, 2017]
[32] Singer & Friedman, 43
[33] Ibid., 43-44
[34] ENISA 2017, 27

4. Distributed denial of service (DDoS) attacks target web servers or other subsystems that "that handle connections to the Internet"[35]. Thousands or millions computers involved overwhelm target's connection by flooding it with data and so disable a computer system[36].

5. Botnets also known as "zombie computers", take over internet users' devices so that they might never know their computers are or have been part of a botnet[37]. Botnets commit other cybercrimes and are capable of fooling security controls, as spam filters for example[38].

6. Phishing is one of the most sophisticated social engineering form, using emails that look like they have been sent from a trustworthy source. The emails themselves do not cause damage, but invite to open malicious webpages, insert credentials or transfer money.[39]

7. Spam, similar to phishing, does not create harm just by existing and might be even hard to recognise as a cyber-threat. However, spam is the most common way of transferring malware by victims opening suspicious attachments, malicious URLs, etc.[40].

8. Ransomware is a type of malware, whose main goal is to extort money by locking target's devices or encrypting their data. Victims are left with two options – paying off the ransom (usually in Bitcoins) or trying to fight back through decryption[41].

9. Insider threats might be caused intentionally or unintentionally. Unintentional cases might involve data mishandling, privilege abuse, using non-approved hardware, etc. Insider threats are purposefully committed usually for money.[42]

10. Physical manipulation might not be considered as a cyber threat per se, but theft, loss or damage to any device might have gradual outcomes, such as information leakage, data breach, etc. One of the most common physical manipulation threats is an ATM fraud.[43]

---

[35] Buchanan, Ben. (2016). "The Life Cycles of Cyber Threats". *Survival*, Vol. 58, No. 1, p. 45
[36] Ibid.
[37] Singer & Friedman, 44
[38] ENISA 2017, 34
[39] Junger, Marianne, Lorena Montoya, F.J. Overink. (2017). "Priming and warnings are not effective to prevent social engineering attacks". *Computers in Human Behaviour*, Vol. 66, p. 76
[40] ENISA 2017, 41
[41] Zetter, Kim. (2017). "What is Ransomware? A guide to the global cyberattack's scary method". *Wired*. Available at: https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ [Accessed July 27, 2017]
[42] ENISA 2017, 46-47
[43] Ibid., 49

11. Exploit kits search for system vulnerabilities or security holes to spread malware. Exploit kits offer "expedited crimeware-as-a-service (CaaS) channels" where people can pay to spread their wished malware on the compromised sites.[44]

12. Data breaches usually happen due to stolen credentials, which might create a "snowball effect"[45] and lead to further breaches. Breached credentials are usually sold on the "black market" at a very low price, which may be then used for spreading phishing mails and spam[46].

13. Identity theft is considered a special case or an outcome of a successful data breach. It happens once attackers get the ownership over one's credentials, such as financial, banking, health, etc. data, which misuse might pose great damage to the victim.[47]

14. Information leakage means accessing someone's confidential data and information either accidentally or maliciously. Although, both can cause severe trouble, the malicious leakages are usually much more harmful.[48]

15. Cyber espionage is mainly conducted on a state-to-state level, which uses other types of cybercrimes as its means. Cyber espionage can be characterised by strategically creating either winners or losers among state-to-state actors.[49]

Once any of those above-mentioned cyber threats result in having actual victims, they are no longer just threats but become committed crimes. That is why this paper will be using the definitions of cyber *threats* and cyber*crimes* interchangeably, in the sense of one being a prerequisite or a cause and the other an outcome of a "successful" execution of a threat. All the cyber threats/crimes above are often interconnected, therefore, especially for this reason, people should be very careful. The landscape of cyber threats' landscape is in constant movement and the risks that might seem revolutionary today might tomorrow become conventional and vice versa[50]. As Buchanan has explained, all cyber innovations, as well as any other invention in history, have been created thanks to great visionaries[51]. Consumers might not imagine the possibilities out there, so innovators play a huge role in the "life cycle

[44] The Recorded Future Blog. (2016). *New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016*. Available at: https://www.recordedfuture.com/top-vulnerabilities-2016/ [Accessed July 27, 2017]
[45] ENISA 2017, 54
[46] Ibid.
[47] Ibid., 57-58
[48] Blasco, Jorge, Julio Cesar Hernandez-Castro, Juan E. Tapiador, Arturo Ribagorda. (2012). "Bypassing information leakage protection with trusted applications". *Computers & Security,* Vol. 31, pp. 557-558
[49] Singer & Friedman, 95
[50] Kello, Lucas. (2013). "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft". *International Security,* Vol. 38, No. 2, p. 38
[51] Buchanan, 39

of cyber capabilities". Unfortunately, not every discovery in the cyber field is benevolent, and great cyber minds might also discover technological vulnerabilities that could be used for malicious purposes.[52] As internet users are not expected to discover security risks and threats by themselves, what can be done is to increase personal awareness of the cyber threats and operate in a more "cyber hygienic" way in the online sphere. Cyber hygiene should be ensured in the online world in the same way as practices of public hygiene in healthcare to prevent the spread of diseases[53].

Greater awareness of cyber sphere will lead to better cyber hygiene by increasing the level of knowledge among internet users about online threats and measures of protection. Cyber hygiene is "a fundamental principle relating to information security", as being more hygienic in the online sphere renders the individual less vulnerable to cyber threats[54]. Practicing cyber hygiene, according to ENISA review, includes for example having a record of all of one's own hardware and software, scanning incoming mail, backing up data, using secured configurations for all devices and accounts, etc.[55]. Although, some experts have argued against the positive notions of cyber hygiene, such as its low visible correlation with less vulnerabilities[56], it cannot do harm either and the more people are prepared to "fight" the security risks in the online world with due diligence in doing so, the better. This is why the author wants to look at ways of how the cyber threats are disruptive towards the security of people, whether more awareness maintains a better security, and what could be done in order to keep that security safe. Accordingly, next chapter of this paper will be looking at topic of cyber threats' landscape from a human security perspective.

2.3. Human security in relation to cyber

This paper has so far explored the background of cyber incidents and the existence of cyber threats and cybercrime by explaining them in detail. The following part of the literature review will explore how the human security concept can be placed in the online sphere. There have been complaints that once human security fulfils all of its different components, it will lose its

[52] Ibid., 40
[53] Singer & Friedman, 176
[54] European Union Agency for Network and Information Security (ENISA). (2016). *Review of Cyber Hygiene practices*. Available at: https://www.enisa.europa.eu/publications/cyber-hygiene [Accessed July 27, 2017], p. 14
[55] ENISA 2016, 15
[56] Ware, Bryan. (2013). „Why cyber hygiene isn't enough". *Network World*. Available at: http://www.networkworld.com/article/3086834/security/why-cyber-hygiene-isnt-enough.html [Accessed July 27, 2017]

meaning and relevance[57]. However, as the world is constantly changing and moving more into the online space, there are new threats appearing all the time. As the digital world will only be expanding even more in the future, the amount of new threats and crime will continue growing alongside it. Therefore, the author doubts that human security in the online context will lose relevance in the near future. The research below will explain why the usage of the human security concept as a framework for analysis is suitable for existing cyber threats and crime through the eyes of an individual. For that, a modernised definition of the concept will be given for a better analysis of the study.

The human security concept is often quoted from the 1994 United Nations Development Programme (UNDP) Human Development Report (HDR) that was the first mention of the concept. It consists of two main components: "freedom from fear" and "freedom from want". This follows the shift from national security towards human beings, where individuals either look out for security threats concerning crime and war or concerns including hunger, poverty, disease, and natural disasters. Based on the report, there are seven categories in the human security threats' list: economic, food, health, environmental, personal, community, and political security.[58] These are all security threats that might already involve the cyber sphere today or in the future warfare, especially personal, community, economic and political, whereas this paper will be focusing on the personal aspect. The UNDP HDR writes: "human security is not a concern with weapons – it is a concern with human life and dignity"[59]. Building on the framework provided by the UNDP, Nef defines the human security concept by five subtopics: "ecosystem, economy, society, polity, and culture"[60]. He sees that all those subtopics are linked together in different ways and believes that the human security concept can be applied wherever and whenever in the world[61]. However, Nef's publication does not include cyberspace per se, as he might not have thought of it eighteen years ago. Although King and Murray think of the UNDP definition of human security as being controversial, they do agree that it has had a revolutionary impact upon different policy debates[62]. In their view, the concept should be focused on the life without poverty[63]. MacFarlane and Khong, on the other hand,

[57] King, Gary & Christopher J. L. Murray. (2002). "Rethinking human security". *Political Science Quarterly*, Vol. 116, No. 4, p. 591
[58] United Nations Development Programme. *Human Development Report 1994*. Oxford: Oxford University Press, Ch. 2, pp. 24-25
[59] Ibid., 22
[60] Nef, Jorge. (1999). *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment*. Ottawa: International Development Research Centre, Ch. 1, p. 25
[61] Ibid.
[62] King & Murray, 587
[63] Ibid., 592

view the UNDP HDR critically, arguing that the focus on human beings does not solve the issue of state-centrism, neither is it clear who defines human security, when talking about food, health, economy security[64]. The critical view on UNDP definition is not very relevant for this paper, as cyber threats are generally not state-centred. Additionally, many scholars use the definition widely and it is important that some sort of a view on human security exists, otherwise there can never exist a debate or analysis about it.

Although, the definition of human security is still very often related to the UNDP HDR, other scholars have provided different definitions of the term. Kaldor, Martin and Selchow have seen the role of human security concept only in the cases of conflicts. Although they say that human security concept as such is not always used in security policies, indirectly it is something that for example European Security and Defence Policy already deals with.[65] They describe 'insecurity' not just as caused by military violence, but also a consequence of material losses, crime, or human rights violations. For them, human security is a response to both – urgent physical or material threats in crisis management.[66] Although their stand comes mainly from the perspective of conflicts, they do also take a humanly approach on security. Owen approaches the human security concept from a threshold perspective – he believes that threats to human security should be measured by their severity, regardless of whether the threat is the result of a war, a disease, or something else[67]. By definition, this should work in the cyber sphere, but considering the non-existing violence level of cyber threats today, then they probably would not exceed the threshold. Paris brings attention to many different ways of seeing the human security concept, asserting that "human security seems capable of supporting virtually any hypothesis"[68]. Paris does not see human security as a framework for any analysis as it is such a broadly defined concept. He sees it rather as a new and large category of research in the field of security studies, focusing on individuals, groups, and societies, and giving some contrast to military threats. He believes that security studies have developed beyond state-centric usage of force.[69] The author agrees with Paris on the fact that the human security concept should not be state-centric and should focus on individuals, groups and societies, which

[64] MacFarlane, S. Neil, Yuen Foong Khong. (2006). *Human Security and the UN: A Critical History*. Bloomington: Indiana University Press, pp. 11-12
[65] Kaldor, Mary, Mary Martin and Sabine Selchow. (2007). "Human Security: A New Strategic Narrative for Europe". *International Affairs (Royal Institute of International Affairs 1944-)*, Vol. 83, No. 2, p. 274
[66] Ibid., 279-280
[67] Owen, Taylor. (2004). "Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition". *Security Dialogue*, Vol. 35, No. 3, pp. 382-383
[68] Paris, Roland. (2001). "Human Security: Paradigm Shift or Hot Air?". *International Security*, Vol. 26, No. 2, p. 93
[69] Ibid., 96-99

is also accurate in regards to this paper and in the cyber sphere. However, the author does not agree with the fact that human security concept cannot act as a framework for analysis, as will be explained below.

Following these different views, either positive or negative, regarding the human security concept, this paper will establish an original definition. The majority of current interpretations of the term are more than 10 years old and are outdated for today's world, given the fast rate at which the technology is developing. The author will also object to Paris and explain how human security concept can be suitable for an analysis framework in the context of cyber. Until the creation of the human security concept, the global focus of security studies had always been on military and state security, only human security started putting a person into focus and looking at the world's issues through individuals[70].

Even though the different definitions of the human security concept are not adequate in the global security issues of today, this paper finds it important to put individual's safety first. A new interpretation of the human security concept inspired by the UNDP HDR will be established. The author will not look at the human security prospects to do with "freedom from want", such as poverty or natural disaster, but rather with "freedom from fear". As the 'fears' in today's world have changed and are also emerging online, so should the variety of threats covered by human security concept expand. Back in 1994 when UNDP HDR was published, human security as a concept was expected to "revolutionise society in the 21st century"[71]. The author believes that the concept has been underused, especially considering how important role cyber sphere plays in today's world and how it is lacking connections to humanly perspective. The 21st century is all about internet and technology, so the human security concept will not be able to revolutionise unless it considers cyber sphere as part of it. The Group of Experts have concluded in Tallinn Manual 2.0 that people are expected to have "the same international human rights with respect to cyber-related activities that they otherwise enjoy"[72]. Especially important by the experts were individual's ability to freely express, state their opinions, keep their privacy and have a due process[73].

To provide clarity regards to the usage of the human security concept in the next chapters, the author of this paper will define the it as: "an individual-focused consideration of people's

[70] Williams, Paul D. (2013). *Security Studies; An Introduction.* London Routledge, Ch. 19, pp. 282-283
[71] UNDP, 22
[72] Tallinn Manual, 187
[73] Ibid., 187-188

fundamental rights in the context of existing threats and crime (including the cyber sphere) that might be disrupted by physical or psychological harm". The human security concept will be used further on to analyse the online survey results about people's cyber awareness about threats and cybercrime experiences. This concept has not been used in relation to cyber sphere before, so this paper acts as a "test run" on whether cybercrime can be considered to disrupt people's human security, as well as whether more cyber awareness reduces the risks and threats to one's security. This paper intends to establish a fresh research through original data and analysis to complement the existing academic research about *human* security and *cyber* security.

3. Research objective with structure and method

The existing literature on this topic has laid a foundation for understanding the theoretical background of cyber space and cybercrime online, as well as the relation between cyber threats/crime and human security. The aim of this research is to explore comprehensively online users' awareness and understanding of cyber space and the existing threats within it. Accordingly, the prime objective for this research is to determine the level of awareness of the impact of cyber threats among the general public and to analyse what kind of experiences they have had with cybercrime. Consequently, the disruptive measures of cyber threats will be analysed towards human security, suggesting ideas to improve people's awareness so that there would be less cybercrime committed online.

3.1. Research structure

The central research question of the paper will be "How does cybercrime disrupt one's human security and how does being cyber aware improve it?"

In order to respond to the central research question, the structure of the analysis will be the following. The author will start by exploring the level of awareness of cybercrime and online threats among people, as well as looking at which kind of malicious activities they have encountered in the online world. The second part will focus on the human security concept and will analyse it in relation to cyber activities. This part will focus on the disruptions of human security through cyber-attacks and explore ways to keep safe in the digital sphere.

3.2. Research methodology

In order to find out how cybercrime disrupts and cyber awareness improves the level of human security, this paper is using two components.

Firstly, the author has conducted an online survey (Appendix 2) about people's experiences with cyber threats and cybercrime to detect their (expected) level of cyber awareness. In order to cover the (exhaustive) list of cyber threats, the ENISA Annual Threat Landscape Report 2016 has been used as a basis for research. The survey was created through *Survey Monkey* portal and targeted at internet users of all ages and backgrounds. The online survey was distributed through e-mail, but also via social media channels like Facebook, LinkedIn and

Twitter, counting on re-posts and additional sharing. The data from respondents was collected anonymously, unless the respondent wished to leave their personal coordinates. In total, 220 people responded to the online questionnaire.

Based on the survey, the data received is mainly about two topics. The first part of the questionnaire focused on people's cyber awareness through their own impression and some guiding questions, including their knowledge of existing cyber threats. The second part of the survey focused on the same threats, but through the prism of their own experience and emotions. The survey was designed with the idea to potentially advise some of the respondents of existing threats and make them more careful about the crime that happens online. The online survey was used as a primary resource for two purposes. First of all, no prior research regarding the connection between cyber threats and human security exist, so in order to come to any conclusions, there needs to be some data to base it on. From a human security perspective, people's individual experiences are important to understand. The other purpose was to deliver an original idea with a useful and usable outcome that could potentially be developed further.

The information received will act as data that will be further analysed below, trying to highlight the most interesting findings and statistics, as well as some of the respondents' views about cyber threats and crime. The online survey allowed the author to access the general public of internet users. The author is aware that the language of the survey and the specific networks in which it was distributed in means it is an imperfect sample of the internet as a whole. Nevertheless, it was conducted within the author's resources and capabilities and 220 responses do act as a valuable outcome. The composition of the survey population is discussed in the next chapter.

Secondly, the survey results will be compared to the human security concept that was developed above in the literature review. This will help to further understand how the existence of cyber threats and victimisation by cybercrime is disruptive towards human security. This part of analysis brings the research closer to the central research question and provides an outcome to the research.

4. Results of the research

The purpose of the research results is to deeply analyse the survey responses and then come up with additional findings through human security concept to realise whether cyber threats/crime are a disruption or a harm to it. The data analysis part will be giving an overview of the respondents' backgrounds, their views about the cyber threats' landscape and the level of cyber awareness among people. The survey will also discover people's past experiences with cybercrime, their concrete examples and how it made them feel. Analysis through human security concept will look at the data analysis and find the connections to human security. This part intends to add up to the existing literature about human security in the digital era.

4.1. Data analysis

The online questionnaire reached 220 people from 36 different countries, with 166 people fully completing the questionnaire. The questionnaire ran during the course of about four weeks, in the period of April 13 until May 8, 2017 and included (Appendix 2) closed-ended (e.g. multiple choice, scaled) and open-ended questions, as well as one matrix question. Open-ended questions included free text boxes, where respondents were given space to express their own thoughts and opinions. The author will be using these comments to illustrate the analysis below.

The results of the survey show that out of the 220 respondents about two thirds were female (64.5%) and one third male (35.5%). Ages of the respondents varied from 18 to over 65; half of the respondents fall in between 25-34 years, more than 80% of the people were under 35. Even though there were respondents from 36 countries, only four countries were represented by more than 10 people – 127 respondents were Estonians (58%), followed by Dutch (7%), France (6%), and the UK (4%). Three results of the nations can be explained by the fact that author is a native Estonian, and has lived in France and in The Netherlands. A quarter of the respondents were composed by all the other 32 nationalities.

People's backgrounds are very different; they most commonly work in public administration and services (21%) which seems to be related to Brussels job market, where the author works and where this thesis has been written at; thus, many respondents may come from the author's social network. The second large group of respondents are students (22%) which can be explained by the author's studies in Leiden University. Only 9% of the respondents work directly in Information Technology department, which is good for having a more horizontal

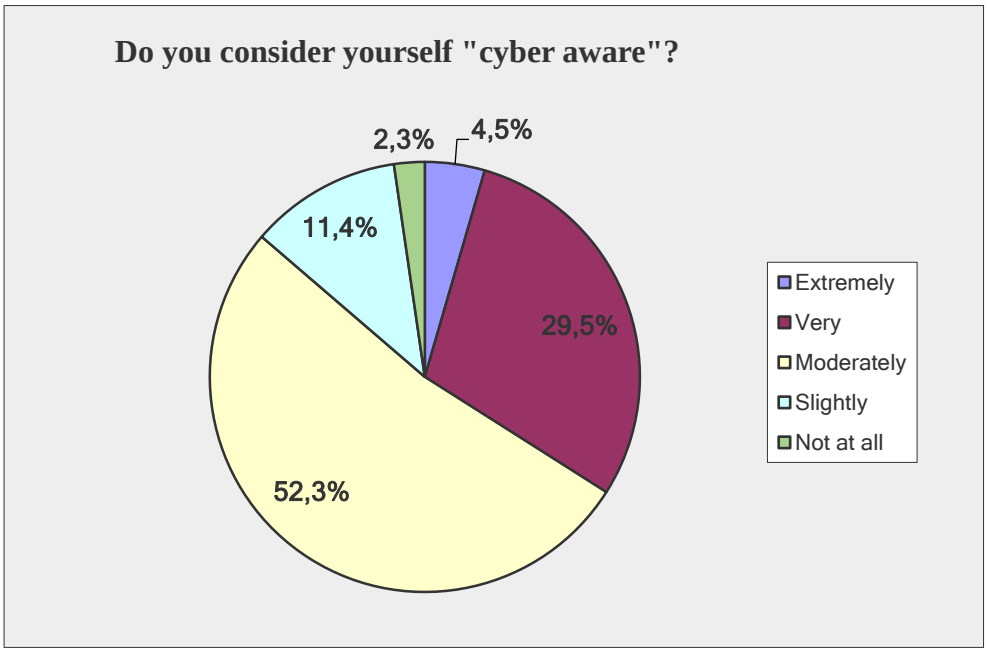
view of the thesis topic. Other three most popular fields were 1) business and consulting; 2) marketing, advertising and PR; or 3) accountancy, banking and finance. Even though the amount of respondents working in the IT department was not that large, about one third of the people considered their work or studies related to cyber (30%), and another third at least partly related to cyber (33%). This shows again that the background of the respondents is very varied.

Although the respondents might not represent a perfect sample of internet users' backgrounds and were concentrated more in a particular geographical area for instance, the overall outcome of the research is more about general views on cyber threats and concrete experiences/stories. These are relevant for a personalised approach to tie the topic to the human security concept, rather than analysing based on age groups, nationality, etc.

Cyber awareness among respondents

More than half of the respondents (Figure 2) considered themselves moderately knowledgeable about cyber, and another almost 30% believed their knowledge to be very good. If taking into account the extremely cyber aware people, more than 85% of the people believed their knowledge of cyber is average or above.

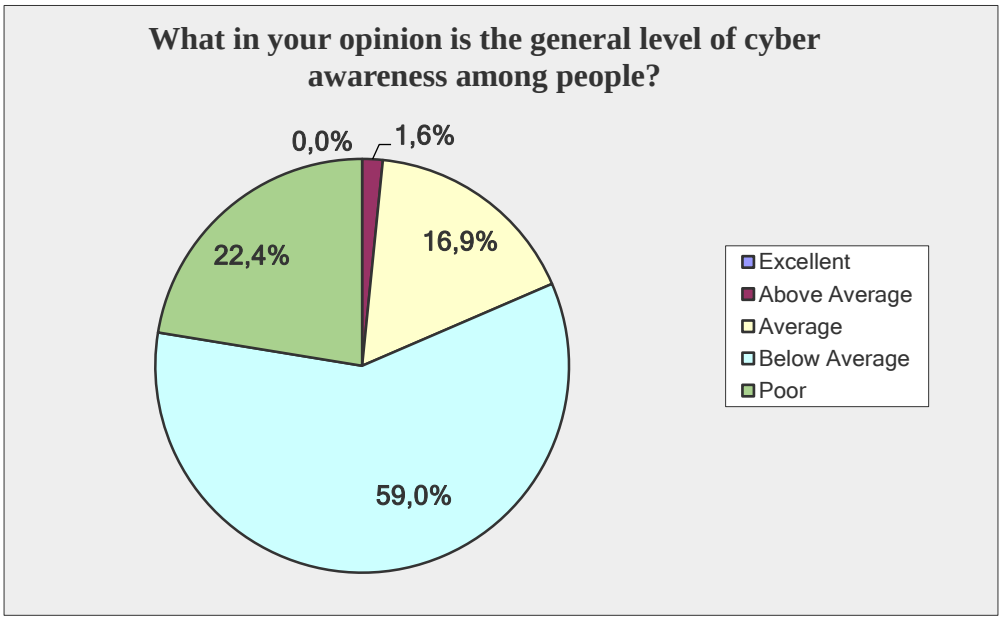
Figure 2. Respondents' perception of their knowledge of cyber.



Source: Survey data from question no 7 (Appendix 2)

On the other hand, when looking at Figure 3, which concerns the respondents' opinion about other people's knowledge of cyber, the level drops a lot. Almost 60% of respondents believed that the general level of cyber awareness was below average; an additional 22% believed that the level was even poor. This means that over 80% of the respondents measured the general level to be below average, leaving a huge gap between what people believe their own cyber awareness level to be, compared to what they think about others'. Especially, as mentioned before, the respondents also have very different backgrounds and exposure to cyber at work or studies. That raises a debate whether or not people overestimate their own knowledge and awareness, or how they may underestimate that of others.

Figure 3. Respondents' perception of others' knowledge of cyber.



Source: Survey data from question no 9 (Appendix 2)

The general sense of cyber threats exposure nowadays was believed to be rather moderate by about half of the respondents (53%). However, while 21% of people think that the topic of cyber threats gets very much attention, 18% believe it does not get enough. It is interesting to note that 11 people have said that in their view cyber threats receive no exposure at all. It is important to note according to the the author, that the two big ransomware threats *WannaCry* and *NotPetya* had not happened by the time of the data collection, which might have affected respondents' views.

When asked about the top 15 cyber threats and whether people have heard about them, the results were relatively positive. Spam and malware were recognised as cyber threats by almost all respondents, and another six (web-based attacks, phishing, data breach, identity theft, information leakage, cyber espionage) were known to 85-90% of the respondents. Most of the others were known by more than 60% and there are only a few not so known cyber threats. This indicates a relatively high level of awareness of cyber-threats. Importantly enough, as one of the respondents drew attention to: "having read or heard of something (which is getting easier and easier now) does not necessary mean to be aware of its nature and potential consequences"[74]. About 40% of the respondents claim at the end that answering this questionnaire had been useful for them as they learnt something new or it tackled interesting points. Forty-three people said they were not aware of the existence of so many different forms of cyber threats before answering the survey, which refers to the achievement of a crucial outcome of this research – the needed improvement of cyber knowledge.

Accordingly, education about existing cyber threats is essential to almost all respondents: 96% of people said that they believe it is important or very important, while no one answered negatively. Just two respondents believe they know all about cyber threats, whereas 83% of people would like to learn more. As mentioned before, about half of the respondents believed their knowledge of cyber threats to be moderate, which implies that they are willing to educate themselves about the topic. Even the people, who considered themselves very knowledgeable, see that cyber space is in constant movement and recognise that one can never know too much. One of the respondents explained an idea: "software companies, browsers, websites and app owners should take a lot of responsibility for preventing cybercrime because most people will simply not have the time or knowledge to keep up with the latest developments in cybercrime"[75].

Cyber education preventing cybercrime?

When asking people about their opinion on whether more cyber education would help avoid cybercrime from happening, it turned out to be quite a divisive subject among the respondents. Many people believed that cyber education is the way forward to keep cybercrime from happening. At the same time, many others thought the opposite and believed that cybercrime,

[74] Survey response to question no 22 (Appendix 2)
[75] Survey response to question no 13

as any other crime will keep on happening regardless of education. In order to find a common ground, argumentation from both sides will be brought forward to come to a conclusion on the issue.

As the answers to question 12 about the necessity of cyber education showed, one of the main arguments for cyber education keeping away cybercrime was that prevention is the key to fighting against any type of crime. Many people believed that either trust or ignorance makes people vulnerable subjects to cybercrime, and that the only way over this is to have a wider awareness about cyber. As one of the respondents put it, "people do not take cyber threats seriously and many still believe that cybercrime is something against states and/or enterprises"[76] indicating they might not even know what they should be protecting themselves from. Junger, Montoya and Overink have written in their paper about how internet users' knowledge generally is limited and often they are unaware of their actions online[77]. One of the respondents explained the same idea: "people simply might not think about the possibility that their data might be stolen, used against them, get bugged or similar"[78]. It was also mentioned in the responses that education could act as a "vaccine" that would at least make the crime execution more complicated for cyber criminals.

As the author mentioned earlier, more awareness creates caution and caution might lead to better cyber hygiene and people learning how to protect themselves against possible threats. For example, one of the respondents explained the necessity of cyber education as: "The development of technology cannot be stopped and awareness-raising should be able to keep up; the same way as once people were needed to explain why doors should be locked"[79]. People should be able to "lock the door" in in the cyber sphere too, or otherwise for example exploit kits might find vulnerabilities and security holes[80], as explained earlier. There will always be large-scale cyberattacks that cannot be predicted, such as the recent *WannaCry* incident. However, everyone should at least be able to keep away from the smaller scale-threats, such as phishing and spam. Based on question 12, most victims are expected to be children, who might be careless, and older people, who might not be knowledgeable enough. Some ideas put forward by respondents included establishing a better cyber education by adding it to school

[76] Survey response to question no 12
[77] Junger, Montoya & Overink, 77
[78] Survey response to question no 12
[79] Ibid.
[80] The Recorded Future Blog

curricula, and the creation of vast cyber campaigns.[81] These ideas will be further explored in the discussion section.

Most of the reasoning against cyber education among respondents did not necessarily mean that people believed cyber education is not needed, but rather did not expect it to help against cybercrime. For instance, there is a belief among a few respondents that cybercrime, as any other crime, will always happen, no matter of people's readiness or knowledge. The cyber sphere is a fast-changing environment and one of respondents explained how "the attackers are constantly looking for new options and they are always one step ahead"[82]. Cyber attackers are expert innovators in the online world with malicious purposes[83], as was discussed above in the literature review. This means that will not be possible for all internet users to be on the same level of knowledge and, as one respondent argued, "educating people sufficiently and efficiently probably only works in institutions where people are constantly faced with cybercrime issues"[84]. However, it will not be possible for institutions only to protect the human security of the general public, if people do not educate themselves. On the other hand, as mentioned rightly by one respondent, "most of people's data sits in third party systems, which they do not have control over", meaning their awareness or non-awareness makes no difference in combatting cybercrime. Another great threat mentioned by many respondents of question 12 was the efforts of cyber education acting as an accelerator for more cybercrime, as people become more interested and knowledgeable of this topic.

Although, there have been compelling arguments from both sides, the results of the analysis still point towards a need for greater cyber education. Even if it is not directly correlated to less cybercrime, it still might act as a trigger for more cyber hygiene for many internet users and might help people to be more cautious and create a safer cyber environment. Even if cyber education does not prevent certain cybercrime from happening, it is still better than no education. In addition, cyber education needs to keep up with the constantly developing nature of technology; therefore, the earlier children (and adults) begin with it, the better.

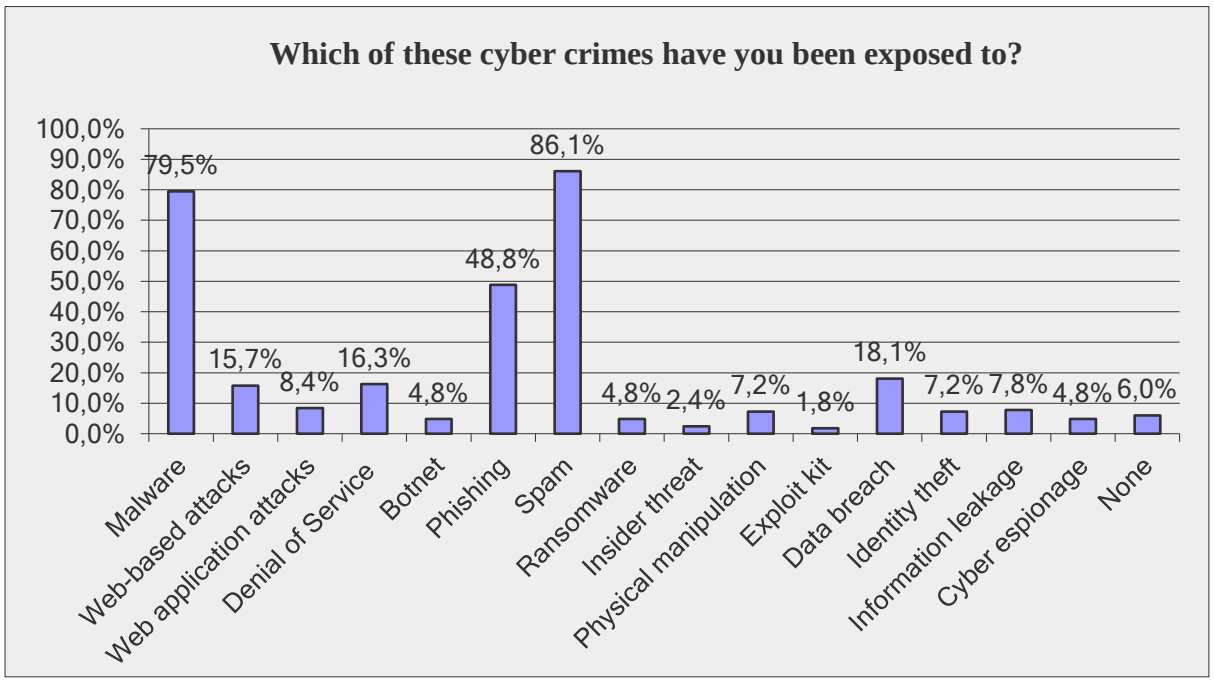
[81] Survey response to question no 12
[82] Ibid.
[83] Buchanan, 39-40
[84] Survey response to question no 12

Experiences with cybercrime

Although respondents considered themselves to be above average in terms of being aware of cyber threats, and more than 80% of people wished to learn more about cyber space, then they did not feel very threatened about cybercrime – almost 50% of the people felt moderately intimidated, and 30% just slightly. Less than 20% of the respondents actually felt threatened by cybercrime, which is a relatively small percentage. Either people consider themselves aware enough for recognising the threats or they have just not had severe exposure to cybercrime. The following section will explore which kind of experiences people have had with cybercrime, including different stories from the participants of the survey.

Respondents had the chance to measure their exposure to cybercrime among the same threats they needed to identify beforehand and 122 people gave their insights about the specific experiences and consequences. The most significant stories will be provided for description and information. Just 10 people (6%) claim to have never been exposed to any cybercrimes (Figure 4).

Figure 4. Respondents' exposure to cybercrime.



Source: Survey data from question no 15 (Appendix 2)

The three most common cybercrimes the respondents have been subjected to are spam (86%), malware (80%) and phishing (almost 50%). Although most of the people have been exposed to spam, it was considered the least worrisome to people based on the questionnaire; rather a nuisance than an actual threat. Many people were surprised spam would be even considered a cyber threat. Malware, on the other hand, is also one of the most commonly experienced cybercrimes, and consequently, one of the most disruptive, based on questions 16 and 17. There were multiple stories about needing to repair computers after malware attacks by either rebooting the system or formatting the hard drive, resulting in a loss of data. Some even said they needed to buy new computers. Malware was also considered "to bridge" to other cybercrimes by some of the respondents, like data breach or information leakage. Some people shared in questions 16 and 17 that they were able to get rid of malware thanks to antivirus software or firewalls. Phishing is believed to be spotted easily by most of the respondents, although one did express the concern of "phishing emails getting more sophisticated, so that it is becoming more difficult to figure out whether the email is from a client, friend or from a malicious actor"[85]. A few people had had very bad experiences with phishing, like a broken computer and even losing money. One respondent told the story of how "the phishing email really had seemed from a dear friend and the message had been very accurate"[86].

The next three threats have already been experienced a lot less – data breaches, DDoS and web-based attacks, all between 15-20%. Web-based attacks can be connected to the distribution of malware. Often the reason for being exposed to malware is from visiting malicious websites that act as attackers, as explained before. This might happen for example when streaming series online on untrustworthy websites.[87] Web-based attacks might also be connected to data breaches, when one enters personal data on suspicious websites, which then gives criminals access to user's account(s) online. A large amount of data breaches happen due to the low level of security by internet users, for example weak or reused passwords. The year 2014 was described as the "year of the data breach", although since then the level of data breaches has grown another 45%.[88] Many big online platforms have had huge data leaks in the past years, like LinkedIn in 2012, Yahoo in 2013, Sony in 2014, etc.[89]. Therefore, from a security

[85] Survey response to question no 16
[86] Ibid.
[87] ENISA 2017, 21-22
[88] Ibid., 54-55
[89] information is beautiful. *World's Biggest Data Breaches*. Available at: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [Accessed July 28, 2017]

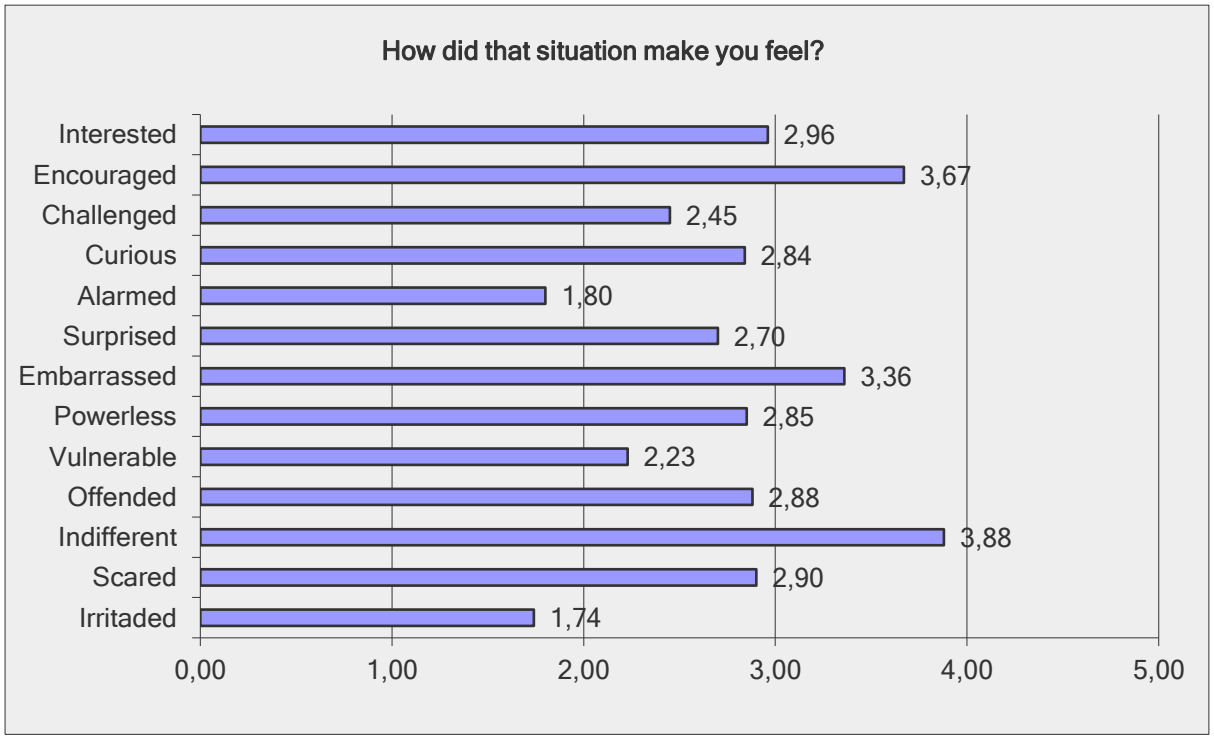
perspective, it is necessary to change passwords as soon as the breach happens. One of the respondents, whose data had been breached a couple of times during the past years, came up with an especially worrisome theory about criminals accessing people's health data: "What if they were able to manipulate people's blood types in health systems and people are given the wrong type of blood because the computer says so?[90]" The same person had also experienced a DDoS attack at her workplace in a news agency, when their online website had not been reachable and some fake news had been posted[91].

The rest of the cyber threats were experienced only by less than 10% of the respondents. However, as the crimes happen less, their consequences are also more severe. Something that was mentioned by a few respondents that should raise the general caution level among internet users was, "one should rather be afraid of the crimes that he/she has not been exposed to nor is aware of"[92]. Many people claimed in their responses to question 17 to be scared of identity theft, as it might create personal harm, like reputation damage. Worst cases that some of the respondents had experienced were loss of money (even amounting to thousands of dollars). There were also examples of cyber threats that might not be directed towards specific individuals. Ransomware might just be currently the best-known cyber threat around the world since 12 May 2017, when the large wave of *WannaCry* cybercrime took place (achieving a new record by reaching to 100 countries in 48 hours)[93]. Already in 2016, ransomware was showing the largest growth among all cyber threats[94]. Quite a few respondents had experienced ransomware; none of them paid the ransom though, so some lost all their data due to it. One of the respondents told the complex story of how "all the files on the computer had been encrypted and there had been a sign on every webpage saying 'in order to see the files again, you need to pay X amount of bitcoins'"[95]. Another respondent said, "it had taken weeks for the IT support to crack down encryption and get the files back"[96]. As ransomware has had a lot of attention lately, it might have changed some of the results of the questionnaire.

[90] Survey response to question no 16
[91] Survey response to question no 17
[92] Survey response to question no 16
[93] Kessem, Limor. (2017). „WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerability". *SecurityIntelligence*. Available at: https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/ [Accessed July 24, 2017]
[94] ENISA 2017, 43
[95] Survey response to question no 17
[96] Ibid.

Respondents had a chance in the questionnaire to voice their feelings regarding the experienced cyber threats (Figure 5). They rated the level of each emotion on a scale from "1" to "5" according to their experiences; "1" meaning strong disagreement to the emotion and "5" strong agreement. Surprisingly enough, the top three emotions that had the rating over "3" are very different in nature – encouragement, indifference and embarrassment. As expected, the most popular is the sentiment of indifference, as in the cases of cyber-attacks where the consequences are not very severe, people do not feel much emotion. Encouragement probably means that people have become more interested in the topic. In regards to the feeling of embarrassment, most likely people, in regards to data breaches and identity thefts, were afraid for their personal information leakages. Embarrassment is a feeling that can be related to human security disruption. People felt the least irritated and alarmed, meaning cyber threats do not generally create much worry among people.

Figure 5. Respondents' feelings towards cybercrime experiences.



Source: Survey data from question no 18 (Appendix 2)

About 73% of people said that they have been more careful online, not opening any suspicious files and raising the level of spam filters. This means people's own security errors act as a source of cyber education. More than 60% of the respondents changed their passwords and 37-

38% searched for more info or warned friends and family. Only 12% of people claim they did not do anything, which is quite a small percentage, and might result in undermining the collective security of their social networks. Some other ideas people proposed to do based on the responses of question 19 after being a victim of cybercrime were to use a better antivirus software, cloud services and external hard drives, and two-step verification in online platforms.

4.2. Analysis through human security concept

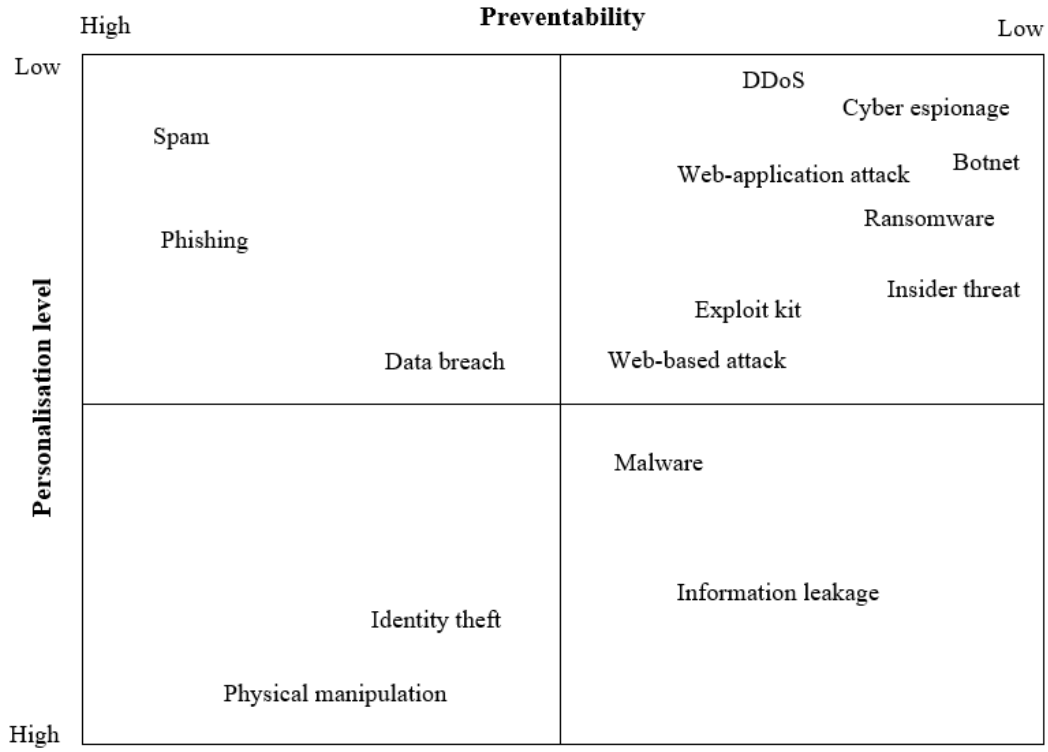
There are multiple reasons why the concept of human security as a basis for analysing data is appropriate for this research. First, as has been shown from the results of the online survey, it seems that cyber threats are not taken seriously enough among people, especially in regards to their own security. The author sees the need to analyse how cyber threats can be disrupting to one's human security. Secondly, cyber threats have not been researched in regards to human security concept before, thus it is time to bring the human security concept up to date with the digital era. Lastly, the human security concept gives a personalised view on security and threats in order to analyse the data from an individual's perspective, as the study has done so far. The data analysis through the human security concept will use the previous chapter's results together with relevant literature. The online questionnaire was created with the human security concept in mind. The concept was deliberately omitted from the questionnaire in order not to confuse people. The questions were formulated in a way that they could be used for human security analysis later on. This part of analysis will explore how people's cyber awareness and their experiences with cybercrime are related to human security. The following analysis is going to be divided into two major parts: human security disruptions through cybercrime and the importance of cyber awareness to human security, in order to have a conclusive narrative and to answer the central research question.

Human security disruptions through cybercrime

Three different perspectives will be used to analyse cybercrime from the perspective of human security. In order to better analyse and group the top 15 threats, the author has come up with her own matrix model by clustering different types of cybercrimes in the individual's perspective of human security (Figure 6). There are two topics that matter the most when looking at cybercrime through the scope of human security: 1) whether the crime has a personal or a non-personal character (meaning whether it has specifically been targeted at the victim or

at a larger community); and 2) whether becoming a victim could have been prevented and to what extent. Despite the fact that the matrix is not scientifically proven, nor is it the only correct and exhaustive version of looking at the issue, the matrix model is a useful tool for a better comprehension and categorisation of threats, acting as the basis for analysis of cybercrimes. Additionally, ENISA threats' landscape report will give input about the latest trends and comparisons, which can be compared to the descriptive material provided by the online survey respondents.

Figure 6. Types of cybercrime from human security perspective



Source: Author

The least serious but most common cybercrime affecting human security seems to be the non-personalised attacks that can potentially be prevented by people themselves. These attacks include spam, phishing and data breaches. As seen from the online questionnaire, those three are also in the top four of the most commonly experienced cybercrimes among respondents (Figure 4). Spam and phishing are the two threats to human security that people often get exposed to through email, but no actual harm is done until opening attachments, malicious

websites, or following other instructions indicated. While spam has been gradually decreasing in the past years, phishing has been rapidly increasing (Appendix 1), so that even technology experts are starting to fall victim to them[97]. Many of the respondents of the questionnaire felt that phishing had not worked on them, but a few expressed their worry for the constant growth in quality of phishing mails or had had a harmful experience, as mentioned in the previous chapter. Data breaches are already more serious threats towards human security due to their less preventable character. Often people themselves can prevent data breaches through better cyber hygiene, however considering the large web platforms' breaches that have been caused by security holes[98]; it might not always be possible to protect oneself fully. According to some survey respondents, they have had severe consequences with data breaches, such as information or money loss, with one of respondent explaining: "it is difficult to identify them before any harm is done"[99], reflecting on the severity of data breaches.

The next group of cyber threats are with a low level of personalisation and predictability, which is also the largest category of cybercrime based on the author's views; half of the threats fall under that grouping. There are a few attacks, which act widely but in a very impersonal manner, like botnets, web-application and DDoS attacks, but are appear in the very top of the rankings of the ENISA threat landscape report. In order to conduct these attacks, infected personal devices can become attackers themselves, unknowingly creating more harm to others in owner's social network by automatically sharing malware[100], which can be very upsetting for both sides of the attack. Ransomware, cyber espionage and insider threats are often connected to people's workplaces and they cannot be predicted by individuals very easily, neither do they usually become direct victims. However, that is not always the case either, as *WannaCry* for example also hit individuals next to services for courier, telecommunication and medical care[101]. Based on a few respondents' comments to questions 16 and 17, ransomware can be seen as very disruptive towards human security, creating both psychological and physical harm. Insider threats, on the other hand, are one of the hardest out of all the existing threats to prepare for as prevention comes down to the awareness of all the users in the network[102]. One of the

[97] Truta, Filip. (2017). "Black Hat 2017: Researcher shows how phishing scams are getting so good they can even trick techies". *Hot For Security*. Available at: https://hotforsecurity.bitdefender.com/blog/black-hat-2017-researcher-shows-how-phishing-emails-are-getting-so-good-they-can-even-trick-techies-18558.html [Accessed July 29, 2017]
[98] information is beautiful
[99] Survey response to question no 16
[100] ENISA 2017, 34
[101] Kassem
[102] ENISA 2017, 46

respondents had experienced cyber espionage at work and revealed that "personnel was advised to extreme caution"[103]. Exploit kits and web-based attacks act as a service that delivers malware to people's devices via compromised websites. These attacks often happen on suspicious websites, which can be avoided through effective practices of cyber hygiene. Illegally streaming movies from untrustworthy websites or installing software from unknown malicious sources makes the individual an easy target for cyber attackers[104].

The more personalised the attacks, the more harm created to people's human security. By looking at the matrix model, it can be seen that the worst potential breaches of human security are posed by the personalised attacks that are difficult to prevent, as they are directed towards individuals, who might have hard to "fight" them. In the author's view, there are not many attacks with this character, and she has identified just two crimes – malware and information leakage. Although they could be both considered as non-personalised threats, this paper considers them personalised for the following reasons. There are multiple means to spread malware, such as botnets, phishing and exploit kits. However, in order for the malware to successfully be installed on the target's device, the attackers must try variations of malware that would be the "right" suit to one's device[105]. Knowing this, it becomes evident that user training and awareness can lead to significant reduction of malware infections[106] and stronger human security, especially considering that malware was one of the most commonly experienced and harmful cybercrimes among the respondents (Figure 4); there were many stories from respondents that included malware creating physical harm, like laptop damage. Malware is also the biggest threat to human security in the online world according to Appendix 1. Information leakages might happen to companies, communities, platforms, but nonetheless it has a huge negative impact on human security, as sensitive data about certain people is usually exposed. One of the latest well-known examples is the Democratic National Committee information leakage prior to the U.S. presidential elections in 2016, where Hilary Clinton's mail threads were breached and leaked. This crime can also be considered cyber espionage, as it has been attributed to the Russian military intelligence.[107] The survey respondents' main worry for the information leaks were reputation damage and lack of knowledge of hackers'

[103] Survey response to question no 17
[104] ENISA 2017, 26
[105] Ibid., 23
[106] ENISA 2017, 21
[107] Rid, Thomas. (2016). "All Signs Point to Russia Being Behind the DNC Hack". *Motherboard*. Available at: https://motherboard.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack [Accessed July 25, 2017]

intended usage of stolen information, "this is not a case where one can just change a password"[108].

The fourth category of cyber threats are also personal-focused, but could be prevented to a certain extent, involving identity theft and physical manipulation to the author's view. It was said earlier that physical manipulation is not a cybercrime by default, but a loss, theft or damage to one's device might lead to information leakage, and identity theft[109]. However, physical manipulation has not been very high in the ranking of cyber threats in the past years (Appendix 1). Identity theft is a crime, which is as serious in the physical world as it is in the online world. Several respondents of the questionnaire had lost money due to identity theft or had found fake accounts under their own names, which in the eyes of the respondents could have led to reputation damage. One of the respondents had been scared because "false information got spread until the page was closed, which luckily did not hurt the reputation"[110] and another was concerned in relation to children's cyber activities, giving an example from real life: "kids for instance might not realise that even posting on Facebook on someone else's name is an identity theft"[111]. An interesting consideration was given in one of the responses to question 17: "what would have been the absolute exposure to identity theft in the 19th century?". The online sphere is changing already from one year to another, and breaching someone's full profile is easier than ever, especially compared to centuries ago.

Importance of cyber awareness to human security

The previous chapter looked closely at all the existing cyber threats and crime in today's world. Whether the threats are personal or non-personal, there is often a certain level of prevention possible to the disruptions of human security in the online space. The major issue with human security in cyber space is that people do not understand the severity of attacks they might be encountering on a daily basis. People only start to become more cyber hygienic once they have been exposed to a cybercrime, such as regularly changing passwords, using two-step verification, etc.[112]. When asking people in question 14 whether they feel threatened by cybercrime, 80% of respondents said they felt only moderately or slightly threatened. This is surprising as earlier in the questionnaire about the same amount of people reported their cyber

[108] Survey response to question no 16
[109] ENISA, 49
[110] Survey response to question no 16
[111] Ibid.
[112] Survey response to question no 19

awareness to be above average. From the data, it can be drawn that people generally think they understand which human security issues exist in the cyber sphere, but when it comes down to their own practices, they are not so engaged. This is very relevant to what one of the respondents had said, that being aware of the threats does not mean understanding what the outcomes of cybercrime actually might be[113].

According to the author, two of the most important outcomes of the analysis of the survey data about awareness were 1) people finding the questionnaire useful in the sense of learning about new cyber threats and creating interest, and 2) the understanding of the usefulness of cyber education among people – 96% believed that it is important or even very important[114]. Becoming more educated about cybersecurity creates more awareness among people, and consequently a better-protected human security. As many of the respondents declared in question 12, cyber education may prevent cybercrime by better cyber hygiene. Even if cybercrime prevention does not lead to a complete defeat of all the threats, education may at least reduce crime among the threats that are preventable and therefore create a more secured cyber sphere. Although, the results of the questionnaire cannot be projected on all internet users, it does strongly support the idea of implementing cyber education in school curricula early on and in campaigns for other age groups. The benefits of cyber education and its possibilities expressed by the respondents will be explored in the next chapter to initiate further discussions on the issue.

[113] Survey response to question no 22
[114] Survey response to question no 11

5. Discussion & conclusion

While the Internet and the online world are probably the best things that have happened to humankind, these innovations are also generating a lot of trouble and interruptions to everyday life. The purpose of this study was to explore how general public perceives cybercrime and their level of awareness of the threats while using internet. Furthermore, the topic has been analysed through the human security concept so it would set the focus of the study on an individual. In this section, the final answer will be provided to the original research question: *how does cybercrime disrupt one's human security and how does being cyber aware improve it?* Additionally, the author wants to look at the opportunities on how to apply a better cyber education among general public and give recommendations for further research.

5.1. Human security concept within cyber space

People should implement a similar level of caution in the online world, as they do in the physical world. However, as non-physical threats seem less tangible and dangerous, it makes the general less worried for their security. This study has shown how different cyber threats can disrupt human security and the following part will conclude the discussion.

The review of the literature affirmed that the cyber space is borderless and accessible for all – creating issues like too much anonymity, difficulty of attribution and lack of cyber hygiene among the general public. The debate in the academic literature about cyber incidents is state-centric and the concerns are war-related. There is not much information about individual threats or how cyber-attacks are connected to people's security in the online sphere. However, human security in the cyber space should be as important as it is in the physical world. It is for this reason, the author decided to look at the cyber world from a human security perspective, which this study has achieved to do through conducting an online survey to see how the general public itself feels towards to the issue of cyber.

The results of the study have been somewhat predictable and somewhat surprising. The online questionnaire has brought new and interesting results that gave a wide range of data to work with for the success of the study and its objectives. The survey was created in the hope that people would be able to learn something from the questionnaire, and many of the people assured they did. Although the level of cyber awareness according to people themselves came out to be quite high, the rest of the results did not always conform to this. The majority of the

respondents felt that cyber education is important in today's world and that fulfils the author's initial objective for conducting this study – to make sure online users stay safe in the cyber world. The use of the human security concept in relation to the cyber sphere and its threats has been very useful. Not only has it provided a new approach to the subject, but it also gave ideas for further research and supported the necessity of cyber education implementation.

However, using the human security concept as a basis for research and analysis definitely had its pros and cons. As the concept had never been used in relation to the cyber sphere, it was complicated at first to find the associated pieces; only indirect connections between the two exist, which had to be identified and interpreted by the author. Accordingly, human security is quite a vague concept for the basis of an analysis, as there is no one certain definition or framework. On the other hand, the lack of defined structure gave the author the chance to look at the concept from her own perspective and facilitated an original approach to cybercrime. Furthermore, human security is a good way to look at the topic, as securing people's actions online should be necessary and this concept gives the right extent of flexibility and authority to do that.

Every type of cybercrime, as explained in the analysis, can be disruptive towards one's human security, just on a different level of creating harm. All cyber threats that ENISA report considers in the top 15 were reviewed through a matrix model that divided them into four categories. The more personalised the approach of a cyber-attack and the less preventable it is, the more harmful towards human security. Cyber hygiene plays a major role in keeping away cybercrime, as some of the threats are more preventable than the others, like spam, phishing, or data breaches, while others are often less predictable from an individual's perspective, such as cyber espionage or insider threat. In order to practice better cyber hygiene, internet users need to be more aware of what to look out for and avoid. This is why an important outcome of the study is to strive for more cyber education that would make people more aware, which will be explored further below.

The results of the study are not applicable to the world population as the sample size of the survey responses was just 220 people. In addition, the survey did not tackle any certain age groups, geographical areas or national identities, which could be implemented in future research for a more comprehensive study. On the other hand, this was never the purpose of the study. The objective was to give a horizontal view of the topic – human security disruptions in the cyber sphere – and get a sense of public opinion from people of all backgrounds. The interpretation of the human security concept and the matrix model were established for the

purposes of the study, which are not scientifically proven approaches. At the same time, the author felt these were needed to be able to write the study about individuals and their perceived feelings of security in the cyber sphere. As a result, this study does give a horizontal comprehension of people's awareness, their experiences and missing gaps in the relations between human security and the online sphere, which introduces an innovative approach to the academic research.

For further research, author could personally approach the 22 survey respondents (10% out of all)[115], who voluntarily left their credentials to research the topic of cyber awareness and experiences with cybercrime more in depth, which would create additional qualitative data. It would also be useful to talk to the experts in the field of cybersecurity to get a sense of their real-life understanding of people's awareness in the cyber sphere and knowledge about existing cyber education programmes. The results of this study will be useful for researchers in the fields of cybersecurity or human security, as the connections between the two have never been studied before, but should be an important area of research in the digital era. Furthermore, the results could also be used in policy-oriented debates, especially in relation to cyber education planning. The next chapter will look more closely at some of the practical outcomes of the study that could be applicable to the real world.

5.2. Cyber education needed

"Cyber security depends on every one of us"[116] is how the Estonian Annual Cybersecurity Assessment 2017 opens. It has been just over ten years since the country was hit by cyber-attacks in April 2007. Despite being seen as a state-level incident at the time, today the State Information System Authority calls for better cyber hygiene among every citizen to ensure a cyber-secured environment both in the perspective of the state and the individual.[117] This inspires the debate of the following chapter to explore ways in which human security can be improved in the online sphere through the responses of the online survey and through reference to relevant literature.

The human security definition, "*an individual-focused consideration of people's fundamental rights in the context of existing threats and crime (including the cyber sphere) that might be*

[115] Survey responses to question no 23
[116] Estonian Information System Authority. (2017). *Annual Cyber Security Assessment 2017*. Available at: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF [Accessed August 1, 2017], p. 4
[117] Ibid.

disrupted by physical or psychological harm", was provided by the author in the literature review section. The types of disruptions have already been observed in this paper, but to prevent crime and to keep the level of human security untouched in the online world, more awareness of the existence of those psychological and physical threats is needed. "Discovery and development" is one of the stages of the "life cycle of cyber capabilities", during which different vulnerabilities are exposed in the online sphere[118]. Once those vulnerabilities have been brought to light, people can start protecting themselves against them. The way to prevent further exploits is to practice better cyber hygiene that, according to ENISA, is just an analogy of what we are already used to doing in the physical world to keep personal hygiene. Some of the measures include using antivirus software, stronger passwords and two-step verification.[119]

"The awareness of the threats and how to protect oneself against them should be paid systematic attention" was said by one of the respondents of question 12 in the online survey. This is why the author wants to discuss three of the most popular ideas among the respondents for expanding and implementing cyber education in the real world to prevent cybercrime from happening.

1) *Begin cyber education at school*. Many respondents of the question 12 reflected that the level of cyber education training at school is inadequate for preparing children for what they need to know. One of the respondents believed that cyber education is "more about general digital literacy from early on that needs to be developed already in primary schools"[120]. Another respondent added that "schools do not teach computer science properly; children should know at least the basics in order to understand the importance of cyber and to protect themselves"[121]. These are very relevant ideas to start growing a generation of "tech savvies" since a young age.
2) *Organise training and practical exercises*. Looking at the current generation adults who have not had cybersecurity education at school, there was another idea proposed by some that included either training sessions or hands-on exercises. One of the respondents believed that these kind of activities would "lead people to be able to actually see a threat or a crime and experience what it means"[122]. Many different training programmes already exist in the world delivered by organisations, like Locked

[118] Buchanan, 40-41
[119] ENISA 2016, 14-15
[120] Survey response to question no 12
[121] Ibid.
[122] Ibid.

Shields by NATO CCDCOE – "world's largest and most advanced international technical live-fire cyber defence exercise"[123].

3) *Create vast campaigns*. For those who have not had the opportunity to learn about cyber at school, nor to voluntarily participate in cyber exercises, a few respondents suggested campaigns on a state level: "More education will result in more caution that will eventually reduce crime"[124]. This suggestion is very relevant for today's world, where different campaigns are frequently conducted in order to attract citizens' attention to specific issues.

The author does not have a comprehensive overview of different cyber education programmes in the world (in the above-mentioned categories), which could potentially act as valuable sources for further research. In order to come up with a proper cyber education "planning" and establish those practices in reality, there would need to be in-depth research both on the academic and political sides, in order to have a balanced view of the topic. The author strongly believes in an advanced cyber education for people from all ages that would encourage better cyber hygiene and therefore ensure individuals' own safety, as well as their social network's security in the online sphere. "Cybersecurity depends on every one of us"[125], as mentioned above, is an idea the author invites every reader of this study to keep in mind and urgently act upon.

[123] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Locked Shields*. Available at: https://ccdcoe.org/locked-shields-2017.html [Accessed August 1, 2017]
[124] Ibid.
[125] Estonian Information System Authority

6. Bibliography

Amoroso, Edward G. (2011). *Cyber attacks: Protecting National Infrastructure*. Burlington: Butterworth-Heinemann

Baylis, John, James J. Wirtz & Colin Gray. (2015). *Strategy in the Contemporary World*. Oxford: Oxford University Press, Ch. 16

Blasco, Jorge, Julio Cesar Hernandez-Castro, Juan E. Tapiador, Arturo Ribagorda. (2012). "Bypassing information leakage protection with trusted applications". *Computers & Security*, Vol. 31

Buchanan, Ben. (2016). "The Life Cycles of Cyber Threats". *Survival*, Vol. 58, No. 1

Davis, Joshua. (2007). "Hackers Take Down the Most Wired Country in Europe". *Wired Magazine*, available at: www.wired.com/politics/security/magazine/15-09/ff_estonia [Accessed June 21, 2017]

Estonian Information System Authority. (2017). *Annual Cyber Security Assessment 2017*. Available at: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF [Accessed August 1, 2017]

European Union Agency for Network and Information Security (ENISA). (2017). *ENISA Threat Landscape Report 2016*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Accessed March 20, 2017]

European Union Agency for Network and Information Security (ENISA). (2016). *Review of Cyber Hygiene practices*. Available at: https://www.enisa.europa.eu/publications/cyber-hygiene [Accessed July 27, 2017]

Herzog, Stephen. (2011). "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses". *Journal of Strategic Security*, Vol. 4, No. 2

Information Is Beautiful. *World's Biggest Data Breaches*. Available at: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [Accessed July 28, 2017]

Junger, Marianne, Lorena Montoya, F.J. Overink. (2017). "Priming and warnings are not effective to prevent social engineering attacks". *Computers in Human Behaviour*, Vol. 66

Kaldor, Mary, Mary Martin and Sabine Selchow. (2007). "Human Security: A New Strategic Narrative for Europe". *International Affairs (Royal Institute of International Affairs 1944-)*, Vol. 83, No. 2

Kello, Lucas. (2013). "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft". *International Security*, Vol. 38, No. 2

King, Gary & Christopher J. L. Murray. (2002). "Rethinking human security". *Political Science Quarterly*, Vol. 116, No. 4

Lewis, James A. (2014). "National Perceptions of Cyber Threats". *Strategic Analysis*, Vol. 38, No. 4

Mouton, Francois, Louise Leenen & H.S. Venter. (2016). "Social engineering attack examples, templates and scenarios". *Computers & Security*, Vol. 59

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Locked Shields*. Available at: https://ccdcoe.org/locked-shields-2017.html [Accessed August 1, 2017]

Nef, Jorge. (1999). *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment*. Ottawa: International Development Research Centre, Ch. 1

Owen, Taylor. (2004). “Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition”. *Security Dialogue*, Vol. 35, No. 3

Paris, Roland. (2001). “Human Security: Paradigm Shift or Hot Air?”. *International Security,* Vol. 26, No. 2

Rid, Thomas, Ben Buchanan. (2015). “Attributing Cyber Attacks”. *The Journal of Strategic Studies,* Vol. 38, Nos. 1–2

Rid, Thomas. (2012) “Cyber War Will Not Take Place”, *Journal of Strategic Studies*, Vol. 35, No. 1

Rid, Thomas. (2016). “All Signs Point to Russia Being Behind the DNC Hack”. *Motherboard*. Available at: https://motherboard.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack [Accessed July 25, 2017]

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Tallinn: Oxford University Press

Singer, Peter W. & Allan Friedman. (2014). *Cybersecurity and Cyberwar; What everyone needs to know.* New York: Oxford University Press

Stone, John. (2013). “Cyber War Will Take Place!”, *Journal of Strategic Studies*, Vol. 36, No. 1, p. 105

The Recorded Future Blog. (2016). *New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.* Available at: https://www.recordedfuture.com/top-vulnerabilities-2016/ [Accessed July 27, 2017]

Tikk, Eneken, Kadri Kaska & Liis Vihul. (2011). “International Cyber Incidents; Legal considerations”. *Cooperative Cyber Defence Centre of Excellence (CCD COE)*

Tikk, Eneken. (2011). “Ten Rules for Cyber Security”. *Survival,* Vol. 53, No.3

Truta, Filip. (2017). “Black Hat 2017: Researcher shows how phishing scams are getting so good they can even trick techies”. *Hot For Security*. Available at: https://hotforsecurity.bitdefender.com/blog/black-hat-2017-researcher-shows-how-phishing-emails-are-getting-so-good-they-can-even-trick-techies-18558.html [Accessed July 29, 2017]

Ülgen, Sinan. (2016). *Governing Cyberspace; A Road Map for Transatlantic Leadership*. Carnegie Endowment for International Peace, Ch. 6

United Nations Development Programme. *Human Development Report 1994*. Oxford: Oxford University Press, Ch. 2

Vacca, W. Alexander. (2011). “Military Culture and Cyber Security”. *Survival,* Vol. 53, No. 6

Ware, Bryan. (2013). „Why cyber hygiene isn't enough“. *Network World*. Available at: http://www.networkworld.com/article/3086834/security/why-cyber-hygiene-isnt-enough.html [Accessed July 27, 2017]

Williams, Paul D. (2013). *Security Studies; An Introduction.* London Routledge, Ch. 19

Zetter, Kim. (2017). “What is Ransomware? A guide to the global cyberattack’s scary method”. *Wired*. Available at: https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ [Accessed July 27, 2017]

7. Appendices

7.1. Appendix 1. Overview and comparison of the current threat landscape 2016 with the one of 2015

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	⊃	6. Phishing	⊃	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	⊃	8. Ransomware	⊃	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	⊃	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	⊃	11. Exploit kits	↑	↓
12. Identity theft	⊃	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Source: ENISA Threat Landscape Report 2016

7.2. Appendix 2. Online survey questionnaire

Background information

My name is Silja-Madli Ossip and I am a Master's student at Leiden University International Studies programme. I am currently conducting research for my MA thesis about cyber threats online. This study means to look at the harmfulness of cyber threats and the level of cyber awareness. Your responses will help me better understand what is the general level of knowledge regarding cyber threats and exposure to cyber crime.

Thank you very much in advance,
Silja-Madli Ossip
MA IS student at Leiden University

1. What is your gender?*
   - Female
   - Male

2. What is your age?*
   - Under 18
   - 18 to 24
   - 25 to 34
   - 35 to 44
   - 45 to 54
   - 55 to 64
   - 65 or older

3. What is your nationality?* (open question)

4. What department / sector do you work in?*
   - Accountancy, banking and finance
   - Business and consulting
   - Charity / voluntary work
   - Arts and design
   - Energy and utilities
   - Engineering and manufacturing
   - Environment and agriculture
   - Healthcare
   - Hospitality and events management
   - Information technology
   - Law
   - Law enforcement and security
   - Marketing, advertising and PR
   - Public services and administration
   - Recruitment and HR
   - Retail
   - Sales
   - Science and pharmaceutics
   - Social care
   - Education
   - Transport and logistics
   - I'm a student
   - Other (please specify)

5. Can you elaborate where? (open question)

6. Is your job / studies in any way related to cyber?*
   - Yes
   - No
   - Partly

- Other(please specify)

7. Do you consider yourself “cyber aware”?*
   - Extremely
   - Very
   - Moderately
   - Slightly
   - Not at all

Knowledge about cyber threats

The following questions will focus on the knowledge about the existing cyber threats today. Please use your own experience and background, so for the accuracy of the results, I invite you to be fully honest.

I have used ENISA Threat Landscape Report to identify the top 15 cyber threats. Please take the time to consult the explanations of terms you might not be familiar with (in brackets or through the hyperlink).

8. In your view, does the topic of cyber threats have enough exposure nowadays?*
   - Extremely
   - Very
   - Moderately
   - Slightly
   - Not at all

9. What in your opinion is the general level of cyber awareness among people?*
   - Excellent
   - Above average
   - Average
   - Below average
   - Poor
   - Other (please specify)

10. Which of the following cyber threats have you heard of?*
    - Malware (malicious software instalment, so-called "viruses")
    - Web-based attacks (use of web sites as an attack surface, e.g. streaming)
    - Web application attacks (attacks against web applications and web services, mobile apps included)
    - Denial of Service (DoS, network resources intentionally made unavailable for users, e.g. no access to online banking)
    - Botnet (creation of "an army of zombie computers", device gets affected and acts upon your name)
    - Phishing (attempt to obtain information by disguising as a trustworthy entity, e.g. someone pretending to be your colleague)
    - Spam (bulk advertising for malicious intentions, e.g. tricking you into payments)
    - Ransomware ("data hostage" so you cannot access it anymore, need to pay a ransom to get it back)
    - Insider threat (intentional or unintentional attack within an entity, e.g. in a work place)

- Physical manipulation (theft, loss, damage of a device)
- Exploit kit (identification of software vulnerabilities of a device)
- Data breach (release of secure or private/confidential information, e.g. password gets hacked)
- Identity theft (compromise of identity information of humans or machines)
- Information leakage (abuse of system weaknesses/mistakes to leak important info)
- Cyber espionage (practice of obtaining information without the permission, usually by state actors)
- Other (please specify)

11. Is it important to be educated about cyber threats?*
    - Extremely important
    - Important
    - Moderately important
    - Somewhat important
    - Not very important
    - Not needed

12. Do you think more cyber education would help avoid cyber crime from happening? Please explain.* (open question)

13. Would you like to be more educated about cyber space and its threats?*
    - Yes, it is very much needed
    - Yes, somewhat
    - Moderately
    - Not needed
    - No, I already know it all
    - Other (please specify)

Exposure to cyber crime

You have shared your opinions and knowledge regarding cyber threats, but now imagine a setting where a cyber threat turns into an actual cyber crime. Please reflect on your own experience(s) carefully and consider also situations which seemed suspicious and a crime was close to happening.

14. Do you personally feel threatened about cyber crime?*
    - Extremely
    - Very
    - Moderately
    - Slightly
    - Not at all

15. Which of these cyber crimes have you been exposed to?*
    (same explanations as in question no. 10)
    - Malware
    - Web-based attacks
    - Web application attacks
    - Denial of Service
    - Botnet)
    - Phishing
    - Spam
    - Ransomware
    - Insider threat
    - Physical manipulation

- Exploit kit
- Data breach
- Identity theft
- Information leakage
- Cyber espionage
- None
- Other (please specify)

16. Which of the above mentioned cyber crimes that you have been exposed to, do you consider to be the worst? Please give an explanation. (open question)

17. What were the consequences? (open question)

18. How did that situation make you feel?

	Strongly agree	Agree	Undecided / neutrual	Disagree	Strongly disagree
Irritaded	○	○	○	○	○
Scared	○	○	○	○	○
Indifferent	○	○	○	○	○
Offended	○	○	○	○	○
Vulnerable	○	○	○	○	○
Powerless	○	○	○	○	○
Embarrassed	○	○	○	○	○
Surprised	○	○	○	○	○
Alarmed	○	○	○	○	○
Curious	○	○	○	○	○
Challenged	○	○	○	○	○
Encouraged	○	○	○	○	○
Interested	○	○	○	○	○

Other (please specify)

19. What have you done differently since the cyber crime experience?
    - Changed my password(s)
    - Searched for more information
    - Asked for advice
    - Been more careful online
    - Warned my friends / family
    - Didn't do anything differently
    - Other (please specify)

<u>Final inquires</u>
Thank you very much for your cooperation and willingness to help!

Here are some final questions to support further development of the thesis research. Also, if you happen to know other people, who would be interested in responding to the questionnaire, please feel free to share it with them.

Dank u wel! Merci! Aitäh!
Silja-Madli Ossip

20. Did you personally learn something useful from this survey?*
    - Yes, I learnt something new
    - Yes, it tackled interesting / important points
    - Undecided / neutral
    - No, not much
    - No, I already knew all of it
    - Other (please specify)

21. If you did, please explain what it was. (open question)

22. Do you have any suggestions / recommendations for the research? (open question)

23. If you would be interested and willing to talk to me personally about the topic, please leave your e-mail address and / or phone number, so that I could contact you. Thank you! (open question)