TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Liia Svimonishvili

CYBERSECURITY: ACQUIRING A DOMINANT POSITION IN CONTEMPORARY INTERNATIONAL RELATIONS?

Bachelor's thesis

Programme HAJB, specialisation International Relations

Supervisor: Lecturer Vlad Vernygora, LL.M., MA

Tallinn 2021

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 7000 words from the introduction to the end of conclusion.

Liia Svimonishvili
……………………………………………
(signature, date)

Student code: 177752HAJB
Student e-mail address: svimonishvili.liia@gmail.com

Supervisor: Lecturer Vlad Vernygora, LL.M., MA:
The paper conforms to requirements in force
……………………………………………
(signature, date)

Co-supervisor:
The paper conforms to requirements in force
……………………………………………
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
…………………………………
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

This paper talks about the legal framework for cybersecurity, observing both national and international context. In order to test the claim – the international system lacks a commonly accepted drive on cooperation in regards of cybersecurity, which leads to further fragmentation of the issue-specific policy-making processes – the timeline of cybersecurity-associated actions is outlined, and national, region-bound and global frameworks are observed in detail. Comparative and critical methods of research, including legal discourse analysis are employed in the process of data gathering and discussing the argument.

Keywords: cybersecurity, information technology, cyberwar, legal framework, cybersecurity law, national security.

INTRODUCTION

The availability of the Internet has significantly expanded over the past three decades, making something that was only available to a limited circle of people to be easily accessible from nearly everywhere in the world[1]. The humankind's current dependence on information technology has already become a factor of political economy, legal and security studies, and cross-cultural communication, and, according to the World Data Bank[2], while the total number of Internet users in 1995 was around 70 million, in 2020 it was more than 5 billion. Evidently, the issue is not only about accessibility and distribution of information for the greater good, but it rather reflects a healthy mix of both positive and negative traits of global society just as any other segment of societal development. Therefore, shortly after virtual spaces got introduced to the public, cybercrime emerged. This term can cover many activities, such as fraud, cyber terrorism, cyber warfare, and many more. Cyberspace has both produced crimes that could not be committed before, as well as made some traditional ones more advanced[3]. For example, Richard McFeely, FBI Assistant Director, once stated that "since 2008, our economic espionage arrests have doubled; indictments have increased five-fold; and convictions have risen eight-fold". Consequences of such attacks may include many direct and indirect effects on different spheres of life, from temporarily disturbing operations of businesses, organisations or individuals, to complete and permanent destruction of mechanisms and processes, not necessarily limited to online space. In 2000 it was estimated that network intrusions lead to the damages of more than fifteen billion US dollars globally[4].

Logically, when a new threat to national security and public safety emerges, countermeasures are predictably to be taken, with a operational preference for those measures to be proactively designed rather than imposed as a reflection to the danger. This is when cybersecurity with its inborn proactiveness comes (or should come) into play. Traditional security has been associated with the use of force, confrontation, and protective measures. Cybersecurity, on the other hand, is the safety

[1] Vine (Keefer & Baiget, 2001)
[2] (The World Data Bank)
[3] (Trautman, 2015)
[4] (Gold, 2000)

online. The term covers different technologies, practices, and tools, which have the goal of preventing unauthorised access or criminal use of networks, computers, and data, as well as the practice of maintaining information security, integrity, and availability[5].

In the 2010 UN Resolution 64/187[6] on cybersecurity, the importance of promoting and encouraging cybersecurity culture was recognised, along with confirmation that information technology is now an essential and vital part of our daily lives. But is cybersecurity considered a legit and important policy, which triggered a proactive approach, or is it still a background disturbance, to which we can only see countries react on an *ad-hoc* basis without having a proper strategy in place?

The Internet is a shared space, and most countries have full access to it. During the past few decades access to the online world has been spreading rapidly, and more and more entities get involved in it every day. The issue that comes with this process is the legal grounds behind protecting this space. First of all, creating an international cybersecurity framework requires close cooperation of participating parties, which always means a struggle for equality and fairness of the process. Secondly, the nature of cyber threats and attacks is very different from physical ones, as there are numerous tactics and processes, which are hard to predict and properly document. Thirdly, getting to the roots of such an attack and finding a responsible party may be hard or even impossible which means that cybersecurity as a policy should be evolving and changing constantly to match the current situation[7]. Last but not least, cyber domain is international, it does not know borders and limits, so the question of jurisdiction is also a part of the discussion.

The role of digital technology in security studies and international relations has been explored before[8]. Plenty of theoretical reviews and research works on ethics in regards of cybersecurity have been presented by different schools of thought, beginning with Arquilla and Ronfeldt (1993) idea on cyberwar. The one thing that seems to make many previous studies incomplete is the fact that they often use outdated principles to investigate new phenomena[9]. The consequences of the world's dependence on technology used to be one of the central issues brought up in the cybersecurity debate, rather than looking at how cybersecurity can or is already being utilised and

[5] (Cybersecurity and Infrastructure Security Agency, 2009)
[6] (The General Assembly of United Nations, 2010)
[7] (Valeriano & Maness, 2018)
[8] (Valeriano & Maness, 2018)
[9] (Domingo, 2015)

by whom. Lucas Kello stated that emergence of cyber wars shall have a drastic influence on international relations[10], while Lindsay[11] and Gartzke[12] argued that it would be long before cybersecurity reaches the level when it could affect the way states interact with each other due to its complexity and novelty.

Another approach to cybersecurity as a policy would be the legal grounds for it, both national and international. Such analysis of cybersecurity-related most important events and their influence on international relations and legal framework is yet to be conducted. It is unclear if the legal field is on the right track with cybersecurity, and whether the legal framework that currently exists answers the needs of the modern cyberspace.

Back in 1997 Timothy Wu highlighted the importance of creating international institutions and legal grounds to manage cybersecurity[13]. The main claim of this paper is that though cybersecurity is gaining more and more influence and importance, there is still no international unified legal framework for cybersecurity, and national lower-scale legal structures are neither sufficient for preventive purposes, nor can stand the test of international scalability. The first goal of this paper is to define if cybersecurity can be considered a significant matter of national security. In order to confirm or refute this, data about major cybercrime events will be collected and evaluated, and cybersecurity as a policy will be also tested against the three main international relations theories.

The second research question which will further support the initial claim is whether or not an adequate national legal framework exists locally in the European Union's (EU) Member States, United States of America, the Russian Federation and the People's Republic of China, and if there is an international legal for cybersecurity, which is effective and proactively contributed to. To be able to reach a conclusion on this, this paper will use comparative and critical research, featured by legal discourse analysis. Specifically, legislations and institutions that are part of the legal framework for cybersecurity will be listed, discussed and evaluated based on the pre-defined criteria.

[10] (Lucas, 2013)
[11] (Lindsay, 2013)
[12] (Gartzke, The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth, 2013)
[13] (Wu, 1997)

1. THE PERCEPTION OF CYBERSECURITY AS A POLICY

This chapter carries a purpose of looking at how and for what reason the perception of cybersecurity has been changing. Is it already a valid matter recognised internationally, or has it not been yet acknowledged what influence cybersecurity can have on pretty much every area of life? In order to answer this question, the major cybercrime events and international relations theory are analysed.

1.1. Cybercrime events involving states

Has the cyberwarfare scene been evolving and advancing, and can it be considered a legitimate national or international security threat? I would like to showcase some of the most important events, associated with cybercrime, where either directly or indirectly a state was involved on either side.

1.1.1. USA and Israeli joint operation

One of the first and most famous attacks is known as Stuxnet[14], being named after the malicious software that was used for it. Stuxnet is thought to have been developed by the US and Israel in 2005 or 2006 to thwart Iran's nuclear weapons development without the latter being aware of the attack. It was a new and important stage in the development of cyberwars due to the complexity and particular success of that attack. Though the official documentation on the attack is still classified, and neither of the countries confirmed its involvement, it seems reasonable to believe that the attack was a game-changer that played a big part in Joint Comprehensive Plan of Action, also known as the Iranian nuclear deal). It was an unprecedented event for the time and was also the first attack to have affected a physical infrastructure. Ralph Langner, who is famous for performing a thorough analysis of the malware, noted that it

[14] (Ivezic, 2018)

> could be considered a textbook example of a ‘just war’ approach. It didn’t kill anyone. That’s a good thing. But I am afraid this is only a short-term view. In the long run, it has opened Pandora’s box[15].

1.1.2. North Korean cyberwarfare

North Korea is also a famous player in the cyber field. In a 2003 study conducted by Giacomello[16], North Korea was ranked 10th out of 57 countries based on its capacity to initiate cyberattacks. It is also believed that they have a dedicated budget for cyber warfare operations[17]. This operational unit is allegedly responsible for hacking into the USA and South Korean military networks with the purpose of collecting sensitive data and disturbing service[18]. Another memorable event where North Korea used its advanced expertise is several attacks on Western enterprises, one of them being Sony Pictures. Hackers stole and then released private information on the company’s employees, their families, and other connections[19]. They also threatened to go forward with physical attacks on cinemas which were to screen ‘The Interview’, a Sony Pictures comedy featuring a made-up story of Kim Jong-un, a North Korean leader, assassination. Even though North Korea denied its liability[20], consequences followed. U.S. Secretary of Homeland Security Jeh Johnson said that the event “was not just an attack against a company and its employees", but “an attack on our freedom of expression and way of life”[21] Later in 2015, President Obama issued an Executive Order, which introduced new economic sanctions on North Korea, once again confirming whom the US considered responsible for the hack. Though it did not come as a complete surprise due to the fact that North Korea had already been exposed to sanctions by the US, this event still revealed that a cyberattack on a privately owned business is just as important as an attack on a governmental body and can change the course of diplomatic relations between involved countries completely.

1.1.3. Russia-sponsored and Russia-related cyberwarfare

Another entity that cannot be left out is Fancy Bear, a Russian cyberespionage group, which is known for a series of attacks. On different occasions, it was claimed that Russian Bear is affiliated

[15] (Langner, 2011)
[16] (Giacomello, 2003)
[17] (Hearn, Williams, & Mahncke, 2010)
[18] (FOX News Cybersecurity Center, 2009).
[19] (Siboni & Siman-Tov, 2014).
[20] (Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law, 2020).
[21] (Johnson, 2014)

with Russia's military intelligence agency[22] or is generally sponsored by the Russian government[23]. A 2018 US Special Counsel indictment named Fancy Bear a GRU (The Main Directorate of the General Staff of the Armed Forces of the Russian Federation) Unit 26165.[24] Fancy Bear has targeted many entities, such as Eastern European governments and military organisations, Georgia, Ukraine, NATO, US-based private organisations, and Russian-based "enemies" of the current regime[25]. FireEye, an American major cybersecurity company, called Fancy Bear an advanced persistent threat, which is a label used for most well-known and harmful groups and individuals, which have participated in cyberattacks or espionage mainly for political or economic reasons. Seeing the list of targets and considering the consequences, it can be without a doubt concluded that the attacks were carried out for the purpose of pursuing the political interests of the Russian government, which again is a great example of how cyberattacks can be used in the modern world international relations.

One more Russia-related series of attacks targeted Estonia in 2007[26], which is also by some considered the first cyberwar. The Estonian parliament, banks, ministries, and media were affected. It was not fully established if the Russian government took part in the attack in any way, but a Russian citizen was found guilty. Evidently, these events led to creation of the NATO Cooperative Cyber Defence Centre of Excellence based in the Estonian capital city Tallinn[27], and later, the release of the Tallinn Manual on the International Law Applicable to Cyber Warfare[28].

1.1.3. Chinese cyberwarfare

One more active pursuer of cyberattacks for the sake of promoting personal political interests is China. It was accused of having attacked Australia, Canada, India, the United States, Vatican, and Taiwan, but some of the claims have not been confirmed by reliable agencies. One of the hacks orchestrated by the Chinese government[29] in 2014 was aimed at the United States Office of Personnel Management. It is considered one of the biggest attacks with a governmental body being a direct target. As a result of the attack, there was a major leak of sensitive US personnel's information. The attack was called "a very big deal"[30] from a national security and

[22] (ESTONIAN FOREIGN INTELLIGENCE SERVICE, 2021)
[23] (Wintour, 2018)
[24] (Graff, 2018)
[25] (Satter, Donn, & Myers, 2017)
[26] (Traynor, 2007).
[27] (Writers, 2008).
[28] (Schmitt, 2013).
[29] (Fruhlinger, 2020)
[30] (Nakashima, 2015).

counterintelligence perspective, as well as “praised” by the US officials for its advanced execution[31].

1.1.4. Summary

Cyberattacks are getting more advanced, expensive, dangerous. It changes the very understanding of traditional state security significantly – states which are known for high attention to their national security and big investments into military and other agencies, can now be attacked in a new and unexpected way. These events are one of the reasons why cybersecurity started being treated as an important part of maintaining national security and ensuring public safety. They are also a great illustrative example of how international cyber domain is; every state can become a target regardless of its location, size or role on the political arena. The question that is yet to be answered is whether the states actually acknowledge the threat and take measures to improve their own security and/or start using their resources to actively engage in cybersecurity matters. What is also still unclear is whether the fact that cyberattacks know no borders and can easily involve more than one state at the same time is taken into consideration.

1.2. International relations theory and cybersecurity

In order to better understand the place cybersecurity as a policy in international relations, it is crucial to consider how the changes digital era brought with it interact with international relations theory. Realism, liberalism and constructivism are the main theoretical perspectives to be analysed. What does each of the theories have to say about information security?

Realism assumes that states are more important than leaders or organisations; that states primarily act in their own interests, and that the most important values of a state lie with power and national security[32]. When there is no above supervision, states are better at concentrating on their national needs, and having advanced security is the guarantee of success. The fact that the digital era changed the perception of security and life in general does not mean that anything about the original realist theory will not stand. The question here is whether cybersecurity should be seen as part of general security, which is mostly military-centred or should it be a separate phenomenon,

[31] (Pepitone, 2015)

[32] (Reus-Smit & Snidal, 2008).

falling under the area of economics[33]. Taking into consideration the examples of cyberattacks and other related events that have been presented earlier along with their consequences and significance, it could be argued that, at this point in time, cyberwarfare should definitely be recognised as a vital part of national security under the realist theory. Following the realist principles, creating a legal framework for cybersecurity on the national level is a top-priority. Committing to international cooperation on this matter would mean that the least influential states' interests might be neglected, and there is also a strong reason to believe that this will not be as beneficial as national security development. This approach seems to sit well with the direction Russia is taking in terms of information security. While not showing any effort to contribute to an international legal framework for cybersecurity, they are proactively using cyber domain to their advantage (section 1.1.3) and have a national legal system in place for that as well (section 2.1.3).

Liberalism, in general, suggests that state security is not the central issue; that international behaviour of the states is affected by internal events; that international organisations play a big role in shaping principles of states' behaviour; international cooperation is important; international cooperation is important; national interests are just one of many aspects driving states' decisions[34]. The way these principles can be interpreted in the context of cybersecurity is that information security is not necessarily an important part of domestic policy, but rather yet another way to establish relations with other states with a united agenda. It is also important to note that since according to liberal theory, international bodies shape states' behaviour and affect internal political organisation, this means that the focus should not be on cybersecurity national legal framework but on contributing to international cooperation and finding a unified way to tackle the issue. In the digital era and globalisation, separate cybersecurity actors have a possibility to gain more power and have a bigger say in how the policy is managed on a national level. This seems to reflect well the current cybersecurity network of the EU, where, while the legal framework is contributed to, international organisations play just as big of a role, taking on such responsibilities as peace, justice, security and others (section 2.2.1).

Constructivism, a major sub-theory of the field, emerged to challenge some of the realism-associated postulates. The main principles it presents are that historical and social factors play a very important role in shaping International Relations ; that decisions and ideas are driven by social interaction; that a state is not the central actor as the focus is placed on the identity and subjective

[33] (Walt, 1991)
[34] (Hollis & Smith, 1990)

perception of single political actors[35]. Constructivism does not see cybersecurity as a central issue and creation of strong national or international cyber defence is not the main agenda. Cybercrime is a product of individual contribution, and in order to fight it, the very reason should be eliminated. This approach is not limited to cybersecurity, but rather applies to any military-related threats, be it physical or other.

2. THE LEGAL FRAMEWORK FOR CYBERSECURITY

2.1. Local legal framework for cybersecurity

Now that we have identified the most significant cyberattacks and operations, it is time to look at what legal frameworks currently exist, how one differs from another case by case, and what goal it pursues. Specifically, this part will cover the existing legal context of the EU, the United States, Russia, and China. What can be considered a solid legal framework for cybersecurity? First of all, the nature of the policy should be well-defined. It is impossible to move forward with further layers if there is no clear understanding how a particular legal system perceives cybersecurity, and how it sees its components, elements, context. Secondly, there should be an organised and fair system of sharing responsibilities – what institution or agent is dealing with every particular element. Last but not least, since legal framework constitutes a set of legal documents, they should be as well present, and, once again, cover every aspect that was previously stated in the definition.

2.1.1. Europe and the European Union

In 2001, the Council of Europe Convention on Cybercrime was issued. It was the first international treaty on cybercrime, and it mostly covered copyright, fraud, child pornography, and network security. A communication from the Commission to the European Parliament, the Council and the Committee of the Regions "towards a general policy on the fight against cybercrime" issued in 2007 stated that cybercrimes can be identified as "criminal acts committed using electronic communications networks and information systems or against such networks and systems", and can be divided into three forms, including traditional forms of criminal activities, distribution of

[35] (Barnett, 2018)

illegal content, and crimes that are limited to e-networks. This is a very general though comprehensive definition, which was the first-ever attempt to come up with a decent legal cybersecurity framework. Since then, the field developed in the EU significantly. As cybersecurity is not something that concerns a limited number of member states, it is being developed both on the EU and national level[36].

The first direction is peace, justice and security, and it is being covered by several institutions. On the EU level it is Europol (EU law enforcement agency), Eurojust (the EU law enforcement agency), and EU-LISA (the EU agency focused on technology), while data protection authorities of the member states are responsible for this on the national level. Single market, which in this context means contributing to the common level of cybersecurity across member states, on the EU level is covered by: The EU Agency for Cybersecurity (ENISA), CSIRT network (Computer Security Incident Response Team composed of member states' representatives), CERT-EU (Computer Emergency Response Team composed of IT experts from the main EU institutions); on the national level: authorities involved with NIS (network and information systems) and national CSITs.

The common Security and Defence Policy, Cyber Defence agenda (CSDP) on the EU level is covered by EDA (European Defence Agency), GSA (European Global Navigation Satellite Systems Agency); and national agencies responsible for defence, security, military cover it on the national level respectively. The Common Foreign and Security Policy (CFSP), and cyber diplomacy in particular, on the EU level is covered by European External Action Service, EU diplomatic service that assists foreign affairs chiefs in carrying out the Common Foreign and Security Policy (EEAS), Agency responsible for EU digital transformation (SAIC), EU Hybrid Fusion Cell (agency, gathering information and intelligence from member states with the purpose of communicating it to the EU authorities), Emergency Response Coordinator Centre supporting the EU Civil Protection Mechanism (ERCC); and the member states' foreign ministries manage it locally.

2.1.2. The United States of America

The United States is a recognised leader when it comes to cybersecurity. According to the Cyber Research Databank, there are more than 3500 cybersecurity US-based vendors, a great deal of

[36] (Bendiek, 2018)

which are considered top companies in the field internationally. Cybersecurity is not only an important agenda of private companies but is also a part of the politics of the United States.

Arguably, the United States' economy and national security are reliant on information technology and infrastructure. As such sectors as energy, finance, transport, healthcare, military and many others' ability to function depends on IT, one could assume that protecting that space is a matter of great importance. According to the investigation Atlas VPN, an IT company providing information security services, conducted, the US government is to allocate more than 18 billion US dollars for cybersecurity spending in 2021, which is to be divided between different government agencies. It is yet hard to say if this number is significant, and if it will be enough, but if we compare the government spend on different agencies and fields, seems that the whole area of cybersecurity is valued at a lower number than most single security-related agencies, such as the Department of Veterans Affairs, the State Department, the Department of Homeland security and the National Nuclear Security Administration[37]. It is important to note, though, that such agencies deal with a variate of matters at the same time, which can possibly mean that their maintenance deemed of higher value. All in all, considering the above-mentioned facts, seems that cybersecurity is a valid concern for the US, but it is not the first one on the list, so in terms of financing they prioritise it accordingly.

Currently, the fundamental privacy regulations that apply on the national level and cover cyber domain are Health Insurance Portability and Accountability Act of 1996, a federal law protecting sensitive health information; The Gramm-Leach-Bliley Act enacted in 1999, which is related to financial privacy; Homeland Security Act dated 2002, which established the United States Department of Homeland Security and the Secretary of Homeland Security position.

In 1949, the Armed Forces Security Agency (AFSA) was created. It was supposed to "conduct all communications intelligence and communications security activities within the Department of Defence, except those performed by the military services"[38]. AFSA failed, and in 1952 the National Security Agency (NSA) was created instead, with the goal of taking over all communications intelligence. In 1984, National Policy on Telecommunications and Automated Information Systems Security (NSDD-145) was signed by President Regan. It formed a high-level interagency committee to enforce the new policy and provided initial goals, policies, and an

[37] (U.S. Government, 2021)

[38] (Howe, unknown)

organizational framework to direct the conduct of federal activities toward “safeguarding structures that process or communicate sensitive information from hostile exploitation”.

In 2009, the US Department of Defence established a unified combatant command (United States Cyber Command), which controls cyberspace operations. Their decision to form this brunch was based on the idea of proactively combating cybercrime. This suggests that the US does intend to take the initiative in matters of cybersecurity. Specifically, they intended to target the threats posed by external and internal actors, threats that are associated with the vulnerability of network and software, and last but not least, threats to the functional activity of the Ministry.

In short, privacy is one of the main priorities for the United States in the field of cybersecurity, along with national security. Both areas are managed separately as the privacy domain is being handled by the institutions that are responsible for protecting certain kinds of information in general, while national security in terms of cyberspace is treated as any other security issue and being handled by respective national defence institutions.

2.1.3. The Russian Federation

When dealing with cybersecurity, Russia specifically concentrates on information security, which means that their approach is mostly limited to a crime involving the distribution of information, access to it, and the legality of its use. The following documents stand out among the documents that describe today's basic approaches to information security in the Russian Federation: Law of the Russian Federation of 27.07.2006 number 152-FZ “On personal data”; Fundamentals of the Russian Federation's state policy in the field of international information security for the period up to 2020; The doctrine of national information security; Strategy for Information Society Development in the Russian Federation.

Overall, Russian approach to cybersecurity is more or less aligned with what other states have on the national level, apart from the fact that cybersecurity is perceived as mostly information security, which limits the scope of their actions and interests. It is also important to note that Russia to some extent prioritises security over privacy, which is clear from the Doctrine of National Information Security. In a 2021, decree President Putin confirmed that cyberattacks, undermining sovereignty and restricting access to advanced technologies are among the main threats in the area of information technology.

2.1.4. China

China has the strictest policies when it comes to securing online space. Foreign-produced software and other web products are under heavy regulations, which has a massive industry of ICT in general. “No national security without cybersecurity,” said President Xi Jinping in 2014, which well summarises China’s past and current approaches.

Earlier Chinese laws and regulations mostly focused on system and infrastructure security. Among them are Regulations on Security Protection of Computer Information Systems, Administrative Measures for Internet Information Services; Administrative Measures for Prevention and Treatment of Computer Viruses; Administrative Measures for Hierarchical Protection of Information Security; Law on Guarding State Secrets. In 2014 Xi Jinping, the General Secretary of the CPC Central Committee and President was named head of the newly created Central Leading Group for Cyberspace Affairs. During the National People's Congress and Chinese People's Political Consultative Conference, the phrase ‘maintain cybersecurity’ was first written into the Report on the Work of the Government. In 2015, the 12th National People's Congress drafted the Cybersecurity Law. It was approved in 2016 and came into force in 2017. This legislation defined core principles, such as protection of personal information, security requirements for network operators, critical information infrastructure, restrictions on overseas data transfers, and penalties.

2.1.5. The summary of locally established legal systems for the cyber domain

As it can be concluded, states do treat cybersecurity as a matter of importance. The EU has an established legal system on both union and local levels, where the responsibilities and jurisdiction seem to be well-defined. The United States clearly invests in the field, showing monetary support of both government agencies and private companies. Cybersecurity is still in the growing stage and cannot compete with other national security matters, financially wise at least. Russia has also come up with a framework, which is contrary to the two previous cases, is heavily controlled by the government, and is considered a strictly internal affair. China is the most nationally oriented in terms of its cyber domain security, though it is their general policy in other matters too. Since their online domain is heavily regulated and controlled by the government already, their level of protective measures has been advancing even before cybersecurity started gaining popularity. “If you open the window for fresh air, you have to expect some flies to blow in,” – Deng Xiaoping, the former paramount leader of China, once said. Both Russia and China advocate for having full control of their internal cyber domain, following the principle of non-interference[39]. Each state seems to have their own definition, principles and methods, which can sometimes have traces of similarities, but still cannot be considered universally applicable.

2.2 International legal framework for cybersecurity

Each state determines its own priorities and goes through with respective regulations on cybersecurity. The first drafts and legislations have been incomplete, serving the goal of defining cybersecurity and establishing the bare minimum of principles. Now, regulations became more advanced, both in their purpose and expertise. We can see a drastic difference in the approaches of states. For example, the United States do not see the need for creating new rules and principles, but rather prefer to focus on developing working information security mechanisms and invest in the development of the field. Russia, on the other hand, intended to create a comprehensive internal legal framework, where each and every possible would be classified and documented.

As Basak Cali (2015) pointed out, international law is defined by its subject, actors and territory[40]. When it comes to cybersecurity, there are numerous actors that may be involved, such as states, companies of different sizes, individual actors, while the question of territoriality is even more complicated – cyber domain is, as was mentioned, international. As it has been covered previously in Chapter 1, the EU does have a framework that constitutes close cooperation of the member states and above institutions. However, the EU system only applies within the union and does not intersect with the rest of the world hence it cannot be considered sufficient. Have there been any attempts to create an actual unified international system, or to establish ground rules for cooperation between the states on the matter of cybersecurity? If such attempts did take place, were they successful?

2.2.1. The Budapest Convention on Cybercrime

The Council of Europe and the Organisation for Economic Cooperation Development (OECD) were among the first international organisations to take initiative to address cybercrime. In 1989, the Recommendation No R (89) 9 of the Committee of Ministers to member states on Computer-related Crime was issued. In 1995 the Recommendation No R (95) 13 of the Committee of

[39] (Budnitsky & Jia, 2018)
[40] (Cali, 2015)

Ministers to member states concerning problems of criminal procedural law connected with information technology followed. Being not legally binding, both still provided a basis for what followed next.

The first international treaty to tackle cybercrime was the Budapest Convention. Drawn up by the Council of Europe with Canada, Japan, the Philippines, South Africa and the United States actively participating, it was adopted in 2001 and entered into force in 2004. It focuses on "crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security" and contains "a series of powers and procedures such as the search of computer networks and interception". The main objective of the Convention is to create a common criminal policy with the purpose of protecting the society from cybercrime, which in particular means "adopting appropriate legislation and fostering international cooperation"[41]. As of today, the Convention was signed and ratified by 66 states and signed only by 2 more[42]. From the moment the Convention was drafted, it was revised several times, specifically because of potential issues with its procedural implementation. Some countries called the treaty "alarming and quite disturbing", while many organisations commented on its negligence of the concept of privacy rights[43]. "We cannot find an acceptable international standard in terms of privacy as it applies to this treaty", – stated Henrik Kaspersen of the Council of Europe, which means that the existing local legal frameworks for cybersecurity are too complex and different, so creating a legislation that would be able to fit in everywhere is very hard, if not impossible. The Budapest Convention on Cybercrime did not succeed in initiating a unified international legal framework – Russia declined stating that it would violate its sovereignty, India and Brazil followed due to the fact they have not taken part in the negotiations[44]. The Budapest Convention on Cybercrime failed in initiating a unified international legal framework – an attempt to cover several legal systems at once was not effective as the treaty is very general, leaves a lot of space for reactive changes based on ongoing events and does not prioritise privacy rights, neither personal nor of a state. What was also neglected is the fact that cybersecurity is far more advanced and compound than it is portrayed in the current EU processes[45].

[41] (Council of Europe, 2001)
[42] (Council of Europe, 2021)
[43] (Baron, 2002)
[44] (Clough, 2014)
[45] (Kasper & Vernygora, 2020)

2.2.2. The United Nations and cybersecurity

The General Assembly in the resolution 67/189 requested an expert group to conduct a comprehensive study on cybercrime[46]. The study mainly covered 8 topics, among which were Legislation and frameworks (3) and International cooperation (7). Some of the findings that the study presented were that national cybercrime laws are too diverse and correlative with states' particular qualities to be applicable to cybercrime globally; existing means of international cooperation do not apply to cybersecurity due to being unable to offer a timely response; the core definition and principles of cybersecurity differ significantly from state to state. The majority of countries participating in the study's survey suggested that the areas that require the most attention are harmonisation of laws, access to existing and creation of new cybercrime instruments, improving mechanisms of international cooperation, creating new law enforcement and criminal justice institutions. The main conclusion that follows here is that there is neither universal legal system for cybersecurity that the United Nations recognise nor there is a solid base for creating one yet.

The UN resolutions on Combating the Criminal Misuse of Information Technologies[47] offer many of what the Budapest Convention did, but neither were ever binding and were only expected to be treated as a recommendation for the states developing their own legislations on cybercrime. The UN-sponsored World Summit on the International Society in Geneva[48] (2003) and Tunis[49] (2005) resulted in the issue of the Geneva Declaration of Principles and the Geneva Plan of Action, which called out the measures for the governments in cooperation with the private sector to take manage cybercrime, and the Tunis Agenda for the Information Society, which suggested the governments "to develop necessary legislation for the investigation and prosecution of cybercrime" taking into consideration the existing local frameworks and the Budapest Convention. Once again, these were not binding and only provided guidelines and recommendations whithout offering a clear plan of action.

In 2007, the Global Cybersecurity Agenda (GCA) was launched by the International Telecommunication Union (ITU). It covers five areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation[50]. In

[46] (United Nations Office on Drugs and Crime, 2013)
[47] (UN. General Assembly, 2002)
[48] (The World Summit on the Information Society, 2003)
[49] (The World Summit on the Information Society, 2005)
[50] (International Telecommunication Union, 2007)

particular, it highights the neccessity of harmonisation of law and mentions that while the matter of cybersecurity in the legal context has been addressed, the outcomes have not been ample[51]. A solution to the highlighted issues has not been offered, while the principles outlines were not expected to be of a globally legally binding nature.

During the 12th UN Congress on Crime Prevention and Criminal Justice it appeared that some countries do support the idea of initiating negotions of a new international legislation for cybersecurity, while others advocate for promoting the existing Budapest Convention and suggest allocataing the resources to imporving its practices[52]. Based on the discussions and suggestions, the Commission on Crime Prevention and Criminal Justice was recommended to explore the matter of cybercrime and the United Nations Office on Drugs and Crime was recommended to provide on-request anticybercrime guidance to member states and organisations[53].

Though several attempts to address the matter of cybersecurity on the UN level were made, none of them proposed a global legally binding legislation or even offered a theoretical solution for the current problem of lack of inetrnational cooperation. It seems that there is simply not enough effort invested in this, though the importance of having a unified legal framework was highighted by the UN representetives on several occasions along with a critique of the Budapest Convention.

2.2.3. Summary

Summing up, international cooperation on the matters of cybersecurity is a popular and widely-discussed topic. The EU managed to offer the first ever solution to this problem, which up to this day remains the only significant development in terms of the cybersecurity legal framework. The United Nations have always been a part of this discussion too, but never attempted to propose their own way of enhancing global cooperation. There is a track of theoretical texts and soft-law, but neither seems to solve the issues of harmonisation, developing existing institutions and legislations and creating new ones. As it was noted be many from the very start, local legal frameworks for cybersecurity are too different to be united under the same international system as they are. This statement is still true, and barely any developments have been made, apart from the Budapest Convention.

[51] (Schjølberg, 2007)
[52] (United Nations, 2010)
[53] (The States Members of the United Nations, 2010)

CONCLUSION

Cybersecurity as a filed has been progressively developing in the past three decades. The world has already seen the first cyber war as well as many cyberattacks with high impact on states, politics and private organisations. This only confirms that the cyber domain is yet to be fully explored and far from being controlled. The discussion that is just as important is on the value and protection of privacy. Both matters proved to be interconnected and challenging. It appears that the current international cooperation on the issues of cybersecurity lacks order and resources.

Just as any other aspect of national security, the preventive, reactive and other measures for cybersecurity must be legally documented. There are always two layers to that, one being local legislations and institutions which together form a national legal framework, and the other one is international cooperation. Legally framing cybersecurity in particular turned out to be a struggle: as can be concluded based on the most important cybercrime events, cyber domain is constantly evolving, and it is impossible to predict the turn it might take in the future. In order to be able to legally support a fast-changing environment, it is crucial to have flexibility and be ready to adjust the system as new discoveries are made. Another problem is the fact that cyber domain is international, and each event can involve an unlimited number of actors, which can all be physically located in several unrelated places under different jurisdictions.

When it comes to creating a locality-bound legal framework, it is all about defining the core principles of cybersecurity and then introducing protection on every front. It appears that many developed countries have succeeded in that up to a certain point and have a clear understanding of what cybersecurity is and how to implement it. The real problem is discovered when we look at the international legal framework – as it was mentioned, cyber domain itself has no borders hence national practices are not enough to cover every aspect of it. The only existing legislation which was intended as internationally applicable is the Budapest Convention on cybercrime, and its coverage does not include some of the major powers and key regional countries like Russia, China, Brazil, India, New Zealand and others. Moreover, it caused quite a debate on privacy as many saw the treaty as a threat to it. The UN have also initiated talks about international cooperation in the area of cybersecurity, however not once a legislation was proposed.

Overall, it seems that regardless of the influence cyber domain has on each state, there is no proactive approach when it comes to finding a solution. Governments are focused on maintaining their local legal frameworks and are much less concerned of contributing to the international one. What that means in practice is that the next step the governments should take is deciding on the strategy of harmonising the existing legislations and coming up with a unified way to approach cybersecurity – first, the core principles and an extensive definition, then a universally applicable legislation. It is also important to take into consideration the previous experiences, such as the Budapest Convention, and the ways in which it was not sufficient, for example, protection of privacy.

LIST OF REFERENCES

Barnett, M. L. (2018). Constructivism. In A. Gheciu, & W. C. Wohlforth, *The Oxford Handbook of International Security* (pp. 86-99). Oxford: Oxford University Press.

Baron, R. M. (2002). A critique of the International Cybercrime Treaty. *CommLaw Conspectus*, 263-278.

Bendiek, A. (2018). The EU as a force for peace in international cyberdiplomacy, SWP Comment. *German Institute for International and Security Affairs*, 4.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 594-613.

Cali, B. (2015). *International Law for International Relations.* New York: Palgrave Macmillan.

Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University law review*, 698-736.

Council of Europe. (2001, November 11). *Details of Treaty No.185.* Retrieved from Council of Europe Portal: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (2021, 04 10). *Chart of signatures and ratifications of Treaty 185.* Retrieved from Council of Europe: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=lPpGFiX0

Cybersecurity and Infrastructure Security Agency. (2009, May 6). *Security Tip (ST04-001).* Retrieved from Cybersecurity and Infrastructure Security Agency: https://us-cert.cisa.gov/

Dewar, R. S. (2018). *NATIONAL CYBERSECURITY AND CYBERDEFENSE POLICY SNAPSHOTS.* Zürich: Center for Security Studies.

Domingo, F. C. (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System by Brandon Valeriano and Ryan C. Maness. *Oxford University Press*, 399–401.

Dunn Cavelty, M. (2012). The Militarisation of Cyber Security as a Source of Global Tension. *STRATEGIC TRENDS ANALYSIS,*, 103-124.

ESTONIAN FOREIGN INTELLIGENCE SERVICE. (2021). *INTERNATIONAL SECURITY AND ESTONIA 2021.* Tallinn: Välisluureamet.

FOX News Cybersecurity Center. (2009). Report: N. Korea Attempting to Hack U.S. Networks. *FOX News*.

Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America. *CSO*.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth. *International Security*, 41–73.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 316-348.

Giacomello, G. (2003, October). Measuring 'Digital Wars': Learning From The Experience of Peace Research and Arms Control. *Infocon Magazine Issue One*, pp. 10-16.

Gold, S. (2000, November 15). *Security Breaches Cost $15 Bil. Yearly*. Retrieved from News Bytes: www.newsbytes.com/news/00/158197.html

Graff, G. M. (2018). Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet. *Wired*.

Hearn, K., Williams, P. A., & Mahncke, R. J. (2010). International Relations and Cyber Attacks: Official and Unofficial Discourse . *Australian Information Warfare and Serucity Conference* (pp. 8-9). Edith Cowan University Research Online.

Hollis, M., & Smith, S. (1990). *Explaining and Understanding International Relations.* Oxford: Clarendon Press.

Howe, G. F. (unknown). *The Early History of NSA.* Retrieved from National Security Agency: www.nsa.org

International Telecommunication Union. (2007, May 17). *Global Cybersecurity Agenda (GCA).* Retrieved from International Telecommunication Union: www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law. (2020). In F. Delerue, *Part II - The Lawfulness of Cyber Operations* (pp. 204-2020). Cambridge: Cambridge University Press.

Ivezic, M. (2018). Stuxnet: the father of cyber-kinetic weapons. *CSO*.

Johnson, J. C. (2014, December 2019). *Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment.* Retrieved from Homeland Security: www.dhs.gov

Kasper, A., & Vernygora, V. A. (2020). Towards a ‘Cyber Maastricht’ : two steps forward, one step back. *University of Malta. Institute for European Studies*, 186-210.

Keefer, A., & Baiget, T. (2001). How it all began: a brief history of the Internet. *Vine*, 90.

Langner, R. (2011, September 22). From the man who discovered Stuxnet, dire warnings one year later. (M. Clayton, Interviewer)

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 365-404.

Lucas, K. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security (Int Secur)*, 7-40.

Nakashima, E. (2015). Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*.

Pepitone, J. (2015). China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper. *NBC news*.

Reus-Smit, C., & Snidal, D. (2008). *The Oxford Handbook of International Relations.* Oxford: Oxford University Press.

Satter, R., Donn, J., & Myers, J. (2017). Digital hit list shows Russian hacking went well beyond U.S. elections. *Chicago Tribune*.

Schjølberg, C. J. (2007). *Report of the Chairman of Hleg.* Retrieved from ITU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG): https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Siboni, G., & Siman-Tov, D. (2014). Cyberspace Extortion: North Korea versus the United States. *INSS Insight*.

The General Assembly of United Nations. (2010, March 17). *Resolution adopted by the General Assembly on 21 December 2009.* Retrieved from United Nations: www.un.org

The States Members of the United Nations. (2010). *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World.* Retrieved from https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

The World Data Bank. (n.d.). *Individuals using the Internet.* The World Data Bank.

The World Summit on the Information Society. (2003, December 10-12). *World Summit on the Information Society, First Phase.* Retrieved from The World Summit on the Information Society: https://www.itu.int/net/wsis/geneva/index.html

The World Summit on the Information Society. (2005, November 16-18). *Second Phase of the WSIS, Tunis.* Retrieved from The World Summit on the Information Society: https://www.itu.int/net/wsis/tunis/index.html

Theys, S. (2017). Introducing Constructivism in International Relations Theory. In S. McGlinchey, R. Walters, & C. Scheinpflug, *International Relations Theory* (pp. 36-41). Bristol: E-International Relations Publishing.

Trautman, L. J. (2015). Cybersecurity: What About U.S. Policy? *Journal of Law, Technology and Policy*, 40-45.

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*.

U.S. Government. (2021). *A Budget for America's Future.* Retrieved from Discover U.S. Government Information: https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf

UN. General Assembly. (2002). *Combating the criminal misuse of information technologies : resolution / adopted by the General Assembly.* Retrieved from United Nations Digital Library: https://digitallibrary.un.org/record/454952?ln=en

United Nations. (2010, April 12-19). *Twelfth United Nations Congress on Crime Prevention and Criminal Justice.* Retrieved from United Nations: https://undocs.org/A/CONF.213/L.2/Add.4

United Nations Office on Drugs and Crime. (2013, February). *Comprehensive Study on Cybercrime.* Retrieved from UNODC (United Nations Office on Drugs and Crime): www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Valeriano, B., & Maness, R. C. (2018). *International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain.* The Oxford Handbook.

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, 214-216.

Wintour, P. (2018). UK accuses Kremlin of ordering series of 'reckless' cyber-attacks. *The Guardian*.

Writers, S. (2008). NATO launches cyber defence centre in Estonia. *Space War*.

Wu, T. S. (1997). CYBERSPACE SOVEREIGNTY? – THE INTERNET AND THE INTERNATIONAL SYSTEM. *Harvard Journal of Law & Technology*, 648-666.

APPENDICES

Appendix 2. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[154]

I, Liia Svimonishvili

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis **CYBERSECURITY: ACQUIRING A DOMINANT POSITION IN CONTEMPORARY INTERNATIONAL RELATIONS?**

supervised by Lecturer Vlad Vernygora, LL.M., MA

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

13.05.2021 (date)

[54] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*