UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Anna Melenchuk

# IS UKRAINE CYBER RESILIENT?

MA thesis

Supervisor: Eamonn Butler, PhD

Supervisor: Eoin McNamara, MA

Tartu 2017

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

..... .....

*/ signature of author /*

The defence will take place on ..... */ date /* at ..... */ time /*

..... */ address /* in auditorium number ..... */ number /*

Opponent ..... */ name /* (..... */ academic degree /*),

..... */ position /*

# Abstract

Rapid development of technologies and fast digitalization of all spheres of life around the globe increased the importance of providing cyber security at all levels. For example, in 2016 Ukraine was a target for around 7000 cyber attacks targeted at the state's critical infrustructure, as well as a big number of cyber crimes, according to the government. (Poroshenko, 2017). The growing importance of tackling cyber crimes, events of cyber terrorism, cyber espionage and attacks makes countries and organizations develop new approaches to providing security. One of such approach is *cyber resilience,* which focuses among others on the inclusion of different actors into the process of confronting cyber threats in order to efficiently and quickly tackle and recover from those same cyber threats. This research contributes to the theoretical and conceptual understanding of cyber resilience as a new approach to addressing cyber threats. It also looks at the national strategy in cyber security of Ukraine with the aim to explain the process of its development and change and define the challenges it faces.



Key words: cyber security, cyber resilience, Ukraine, cyber attacks, cyber crimes

# Table of contents

## Introduction and methodology

During the NATO Warsaw summit on 8 July 2016 cyberspace was named as a fifth element of warfare along with air, space, sea and land. The growing importance of tackling cyber crimes, events of cyber terrorism, cyber espionage and attacks makes countries and organizations develop new approaches to providing security. 'The world of cyber-crime, cyber-terrorism, and cyber-warfare is truly a wild, unruly, and ungoverned place' (Tohn, 2009:17). Since threats connected to cyber dimension are mainly of international character and require global response, cyber security issues become more visible within the scope of the international security agenda. Furthermore, it is widely agreed by experts that security which presumes the absence of threats is impossible to achieve in cyber space (Tohn, 2009:17; Kaminski, 2010). Therefore, other approaches that look at preventing and combating cyber threats are being developed. One of such approaches is cyber resilience which is focusing among others on inclusion of different actors into the process of confronting cyber threats in order to efficiently and quickly tackle and recover from cyber threats. The cyber resilience concept, which was firstly developed in IT, and only after was borrowed by political scientists, seems to be most promising and widely used by experts, political figures and media. The concept, however, is relatively new and not studied and tested sufficiently. This research aims to test the abovementioned concept using a single case study method and focusing on a national policy in cyber sphere of Ukraine.

After the Euromaidan events and annexation of Crimea in 2014 Ukraine became a victim of a war with Russian Federation which has been taking place for already three years (Poroshenko, 2017). The conflict in Ukraine includes all means of cyber warfare such as Ddos attacks, digital propaganda, website defacements (Radchenko, 2017). Even though there were around 6000 cyber attacks targeted at Ukraine in 2014-2017 (Poroshenko, 2017) the national policy in cyber sphere is still being developed. Due to the absence on the law on cyber security and no control mechanisms of other state regulations there is little coordination in state efforts aimed at tackling cyber threats. However, from 2014 Ukraine experienced the rise of volunteerism and grass root movements which became

actively involved in providing cyber security of the country. Middle sized businesses and NGOs related to IT sphere provided their expertise and help to the state. These changes lead to the appearance of the new approach to cyber security of the country which has now more of bottom-up features focused on resilience rather than traditional cyber security. Cyber resilience concept is promising due to its flexibility and practical, realistic features. There is a need to provide a deep and thorough research of its application in different countries and on different levels. This research contributes to the study of cyber resilience as a new approach to addressing cyber threats. It also looks at the national strategy in cyber security of Ukraine with the aim to explain the process of its development and change and define the challenges it faces.

### a) Aim

To find out if the national policy of Ukraine in cyber sphere corresponds to the concept of cyber resilience and identify main challenges to providing cyber resilience in the country.

### b) Added value

From policy perspective, the attention to cyber security and cyber resilience is constantly growing within the recent years. However, both concepts are being used interchangeably and not consistently. Cyber security is often defined as 'the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.' (Oxford University Press, 2014). Cyber resilience at the same looks at the ways to ensure the quick and efficient recovery from cyber attacks and crimes be involving all possible tools and stakeholders'. Unlike cyber security, cyber resilience approach does not aim for achieving overall protection of cyber risks – it stresses that the risks are unavoidable and the efforts should be put into reducing their harm and quick recovery (Jegen, Merand, 2014). that Even though there are studies which look at cyber resilience and cyber security, the concepts are not researched to the full extent which leads to confusion and little understanding of their value. Therefore, both concepts require more in-depth academic research. Also, the Ukraine case study is specifically interesting and important due to the ongoing transformation which the country is going

through. Cyber domain reflected in the rapid development of ICT and e-democracy in the country is becoming increasingly important for Ukraine's cooperation with the European Union. At the same time, the conflict in the Eastern Ukraine and fragile process of reforms undermines its cyber security. The state is currently being exposed to a wide range of cyber risks the research of which can significantly contribute to the theoretical and conceptual understanding of cyber security and cyber resilience in general.

## c) Research questions:

***Does the new policy of security in cyber space of Ukraine matches the concept of cyber resilience?***

- What are the main challenges for cyber security policy in Ukraine?
- Can the policy on cyber security of Ukraine be explained through the concept of cyber resilience?

## d) Methodology and methods of data collection

I will use a qualitative method to conduct my research – process tracing case study. This method was first introduced in 1979 and then thoroughly developed by George and Bennett in *Case Studies and Theory Development in the Social Sciences* (2005). Process tracing is 'a case-based approach to causal inference which focuses on the use of clues within a case (causal-process observations, CPOs) to adjudicate between alternative possible explanations' (Mahoney, 2012: 9). The main aim of the process tracing case study is to look at 'establishing the causal mechanism, by examining the fit of a theory to the intervening causal steps. Theorists using process tracing ask' how does "X" produce a series of conditions that come together in some way (or do not) to produce "Y"?' (Wesleyan University, 2017).

There were a few attempts to develop a cyber resilience concept in political science (Cavelty, 2015; Pernik, 2015; Christou, 2016; Nicholas, 2016; Jagasia, 2017) and by

looking at a case study of Ukraine I will trace the process of the development of its national policy in cyber sphere and will conclude if it fits in the theory. By using a process tracing case study I will then be able to test of the concept of cyber resilience viability using one of the cases.

Process tracing focuses on a deep analysis of one case. Its form – theory testing case study is ‘an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident’ (Benbasat and Zmud, 1999; 33).

Thus, in order to use the process tracing case study as a research method the research design should correspond to the following principles:

a. Investigate a contemporary phenomenon
b. Exist in a real-life setting
c. be focused on organizational and managerial (rather than technical) issues

(Benbasat et al., 1987; Benbasat and Zmud, 1999)

In this research, I am analyzing the contemporary events which have happened in Ukraine in 2014-2016 in cyber security policy. They take place in a real-life setting. The research is not focused on specific issues but relates to national policies in cyber sphere (organizational and managerial ones).

Process tracing case study perfectly suits my research since I am looking at a single case (Ukraine) and test if the concept of cyber resilience can explain its cyber security policy and if not why. As philosopher A. Sayer pointed out: ‘within process tracing we would like a get knowledge of how the process works. Merely knowing that 'C' has generally been followed be 'E' is not enough; we want to understand the continuous process by which 'C' produced 'E,' if it did.’ (Sayer, 1992: 106-107).

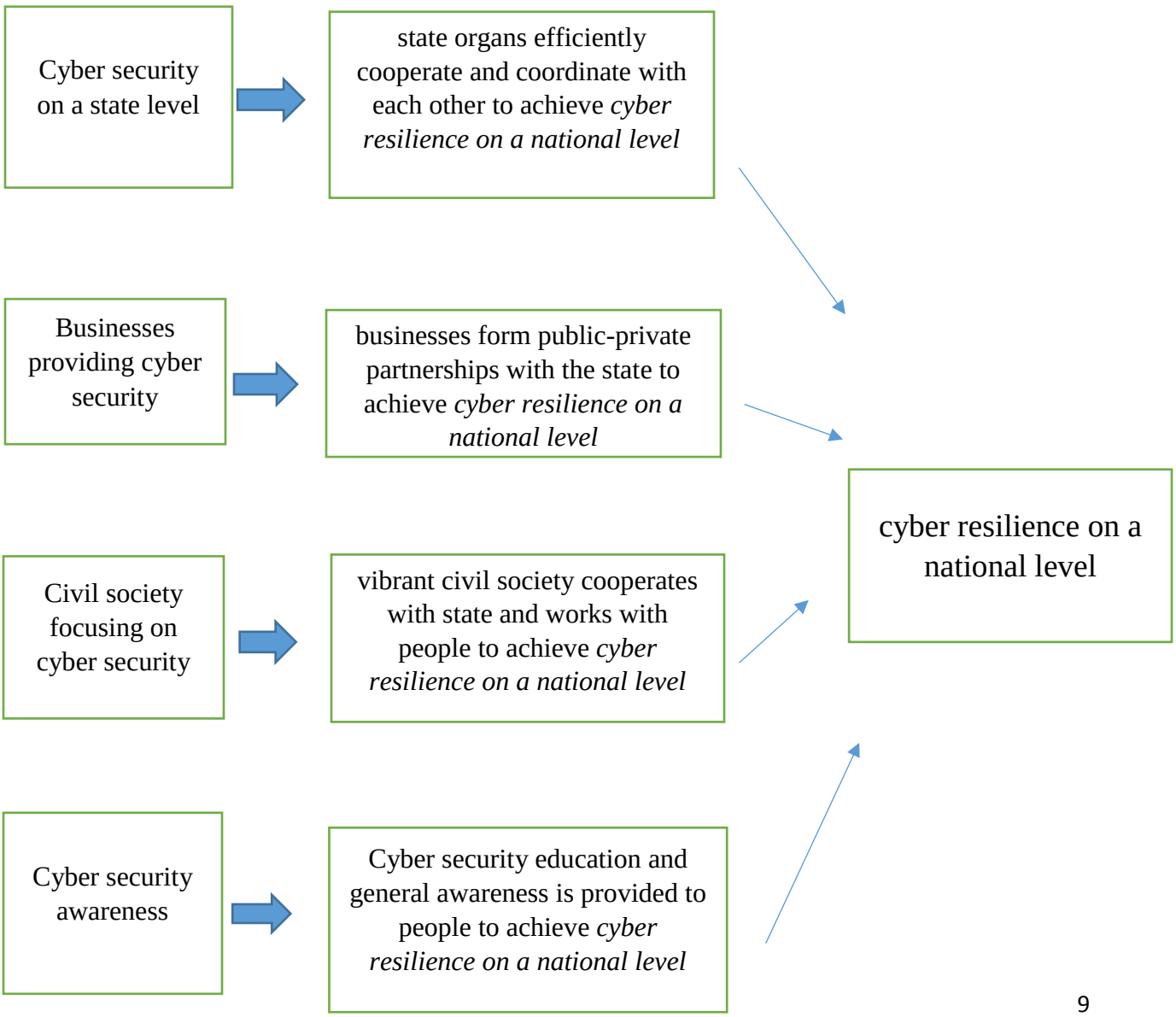
The process tracing is applied in four main steps within the scope of this research:

1. Developing causal mechanisms which are broken down in parts which will be empirically measured.

2. Operationalizing causal mechanisms during which evidence which will prove if a causal mechanism exists in the case study
3. Collecting evidence
4. The conclusions of a process tracing exercise

(Beach and Pedersen 2013)

The causal mechanisms of this research consist of four independent variables (also called criteria), four elements which are to be proved by their factors and the dependent variable:



Therefore, process tracing case study and its form – theory testing will help me to prove if national policy on cyber security in Ukraine can be explained though cyber resilience and if this concept is applicable in the case of Ukraine. Furthermore, though process tracing I will analyze the process of emerging and development of national policy in cyber security in Ukraine by looking at the process of development of national security policy as a whole. Therefore, the development of national policy in cyber security will act as a independent variable while cyber resilience on a national level is a dependent variable.

### e) The selection of a case study

According to George and Bennett "the primary criterion for the case selection should be relevance to the research objective of the study, whether it includes theory development, theory testing, or heuristic purposes" (George and Bennett, 2005). The research includes the theory testing component and looks at proving if cyber resilience concept which is claimed to by many authors a new modern approach to cyber security and governance (Pernik, 2015) fits one of the European country which only recently started to develop its cyber security policy due to the cyber war with Russia.

After the beginning of the war between Ukraine and Russia there was a rise of volunteering and grass root movements in Ukraine which aimed to support the government and people of Ukraine in providing cyber security. Small and medium sized businesses focusing on cyber security and IT became actively involved in providing expertise and help in cyber security as well. All these processes led to the appearance of the new approach to cyber security in Ukraine – cyber resilience. Cyber security as resilience has never been researched before in Ukraine. It is not used in official

documents on cyber security in Ukraine but its main features are presented in the country which makes Ukraine an interesting case to test the theory.

Therefore, my selection of the case study of Ukrainian national policy in cyber security is based on the four main arguments:

- There were only few attempts to analyze changes in cyber security policy in Ukraine. There has not been any comprehensive research on this topic so far.
- Growing interest to cyber resilience in political science and its possible application in Ukraine.
- Originality since cyber resilience is a relatively new approach to cyber security and governance in Ukraine and also worldwide.
- Availability of sources and knowledge of national and local languages in Ukraine.

Single case study rather than comparative one since it gives an opportunity to deeply research one case rather than focus on narrow comparisons. 'A single case study also makes the writer to have a deeper understanding of the exploring subject' (Gustafsson, 2017). Eisenhardt (1991) believes that the amount of a case studies depends upon how much new information the cases bring and how much is known. Since national policy in cyber security as resilience in Ukraine has been researched before this research brings a lot of new information itself. According to Gustafsson (2017) a single case study gives an opportunity to question different theoretical approaches related to the topic and test new ones which is the aim of this research.

### f) Availability of data:

Within the framework of the research both primary and secondary data are analyzed. As to primary sources, one of the most crucial parts of the research will be the analysis of original documents, laws and regulations on Ukrainian national policy in cyber sphere. As to secondary sources, publications and articles, monographs and books specialized in resilience, cyber resilience and security will be analyzed. The following laws and regulations are constituting the basis of the primary sources used in the research:

- ‘Cyber security strategy of Ukraine’ (2016),
- Draft law on ‘National cyber security’ (2016),
- Law ‘On information security’ (2009),
- ‘On National Security of Ukraine’ (2003),
- ‘On State Special Communications Service and Information Security of Ukraine’ (2006),
- ‘On Telecommunications’ (2003),
- ‘On protection of information in telecommunication systems’(2014),
- ‘On Access to Public information’(2011),’On Defense of Ukraine’(1991),
- ‘On the principles of domestic and foreign policy’(2010).

There are also Decrees of the President of Ukraine as well as decrees of Ukrainian government and National Security and Defense Council:

- ‘Doctrine on information security’ (2009),
- ‘Ukraine's National Security Strategy’ (2015)
- ‘Military Doctrine of Ukraine’ (2015)

Other documents and regulations released by organs which relate to cyber security issues such as: State service of special communication and information protection of Ukraine and its Department of cyber security together with CERT (Computer emergency response team); State Security Service; National Bank; Ministry of Defense; Ministry of foreign Defense.

The case study is draws upon eighteen semi-structured interviews that were carried out with representatives of Ukrainian government and specialized agencies in ICT and security; NGOs, thinks tanks, grass-root movements, businesses. The following criteria of selecting the organizations and businesses were applied:

- Number of projects, publications and other activities conducted
- Regional distribution
- Visibility in media
- Credibility (possibility to verify the provided information)

- Well-established, consolidated status of the organization in Ukraine

Interviews with international donors and organizations were also conducted since they play a crucial role in capacity building in cyber security in Ukraine as well as providing expertise to Ukrainian government. Such international organizations are interviewed: the NATO Cooperative Cyber Defense Centre of Excellence, Center of information and documentation of NATO in Ukraine, OSCE mission in Ukraine. Interviews with experts give the opportunity to look at opinion of civil society and businesses on Ukrainian policy in cyber security. Experts from the following NGOs, businesses and educational institutions are interviewed: the International Center for Defense and Security, ISACA (Information Systems Audit and Control Association), InfoSec Ukraine, Microsoft Ukraine, Berezha Security, Team4Ukraine, Atlantic Council, Cyber Shield NGO, Ukrainian Cyber forces, Cyber Warta NGO, Information security and informational technology association. Deputy Minister of Information of Ukraine and expert of National Institute of Strategic Studies are interviewed as representatives of government. 'The method of semi-structured interviews was chosen since it provides the interviewer flexibility by using open-ended questions and the possibility to ask for specifications or follow-up questions' (May 2001). Names of the interviewees as well the list of topics and questions discussed with them are the listed under Appendix 4 and Appendix 5 respectively.

The interviews' content was analyzed by textual analyses of the interview transcripts. Excel software tool is used for the purpose of conducting textual analysis. Highlighted topics and phrases discussed at the interview are uploaded to the Excel Sheet and grouped accordingly. When the themes were decided and the text grouped accordingly the write-up process which included a narrative with the quotes of interviewees began. The themes which have been discussed with the interviewees were related to their involvement in providing cyber security in Ukraine, main challenges they faced during their work, cooperation and coordination with other stakeholders and governments on cyber security and finally the prospects of cyber resilience for Ukraine. Official documents, laws and regulations as well as critical literature were analyzed with the help of online textual analyses.

## g) Limitations of the study

In general, 'Case study research and process tracing in particular face four main challenges: the reliance on pre-existing theories; the assumption that each case can be treated autonomously and that the cases are distinct from one another; the need for empirical data; and the pitfalls of cognitive biases' (Collier and Mahoney, 2006; Checkel, 2006: 367–9) As for the reliance on pre-existing theories arguments stresses on the fact that the empirical study often depends on an ill-fitted theory or the theory which is contested by academia to such extent that it should be rebuilt or reformulated. Some also argue that researches who use process tracing case study often select middle-range theories which consist of poorly formulated hypothesis rather than a working theory which has its set of guidelines to do a research.

The assumption that cases are usually very different from each other relates to the fact that political science problematics are very interconnected. World becomes more global and interdependent. It is hard to prove that one specific case the researcher is analyzing is autonomous enough to be researched as a single case. As for the empirical sources on which process tracing case studies are dependent they should have a 'sufficiently high level of accuracy, and reliability in order to work.' However, again the question is here how the reliability and sufficiency of empirical data be evaluated and measured remains a question (Checkel, 2006: 366–7).

Cognitive bias is the limitation which every social science`s research encounter. Very often researchers fail to notice negative evidences or the things which did not happen since they are harder to be analyzes than the existing events. Another example of the cognitive bias is the confirmation bias when the researcher tends to seek for specific information which confirms his or her believes rather than see the whole picture. This can affect all stages of the research – from collecting data to making conclusions. One more example of cognitive bias relates to theoretical bias (Venesson, 2012). The conclusions of the research may correspond to few theories or approaches and 'then becomes difficult to assess whether alternative explanations are complementary or if some are just spurious' (Njolstad 1990: 10).

The results of the research of one single case study contribute to the understanding of the trend comparatively little which is also a limitation of this research. The question here is where to place this research within the scope of debates on what cyber resilience stands for and what single case studies can show about the viability of this concept. This argument applies to 'arguably most prominent critique of single case study analysis is the issue of external validity or generalizability' (Willis, 2013: 16).

Another limitation is conceptual. Academics, experts, government officials as well as interviewees of this research have different understanding of the concepts used in the research. This relates to every concept related to cyber sphere – difference on cyber attack and cybercrime, the point when the number of cyber attacks can or cannot be considered a cyber war and eventually the understanding of resilience and its features. Finally, limitation of the research also lies in the objectivity of the interviews. Selection of interviewees is highly dependent on their availability.

### h) Structure of the thesis

The thesis will include an introduction to the problem, explanation of selected methodology, conceptualization and theoretical framework, empirical part, conclusion, bibliography and appendices.

## Synopsis

Having introduced the problem, defined the aim of the research and selected the methodology the research will start from the literature review and will be followed by the process tracing case study of Ukraine, conclusion, bibliography and appendices.

Within the literature review the biggest cyber security risks and threats are identified in order to better define the challenges to providing cyber resilience on the national level. After the cyber threats and risks are overviewed the concepts of cyber security and cyber resilience are compared and defined. The last chapter of the literature review looks at national cyber security policies to identify possible and the most efficient approaches to forming and conducting national cyber security policies which integrate the ideas of cyber resilience. Literature review is followed by the short background chapter which looks at the history of Ukrainian cyber security policy.

The process tracing begins within the empirical part of the research which aims to prove the four causal mechanisms developed in the methodology part. Each causal mechanism has one element which is analyzed by looking at different factors which confirms/ does not confirm it. When all the four causal mechanisms are traced and either proved or not the research finishes with the conclusion which summarizes not only the results of process tracing but also defines the conceptual contribution of the research. Bibliography and appendices are provided at the end of the research.

# Literature review

## 2. Overview of main cyber risks to a country

A resilience approach to security was developed through the merger of risk and crises management and critical security studies. The basic category of these theories is the understanding, preventing and tackling the consequences of risks. A *risk* according to ISO 31000 (standards of risk management formulated by International Organization of Standardization) is a 'basic negative and positive effects of uncertainty on objectives' (IOS; 2017). In majority of studies of cyber security the category of a risk is used interchangeably with a term threat and can be defined as 'possibility of malicious activities in which a digital system or network is exposed to a cyber attack or crime enabling the attackers to get unauthorized access to systems and data' (Center of cyber security, 2017). The main risks in cyber space of a country include cyber crimes, cyber attacks, cyber terrorism and cyber espionage. All of the threats are or may be present in a country to different extent depending on the level of its digitization, development and use of Information and communication technologies (ICT) both on a state level and among general public. Such threats are becoming more dangerous if country is a war, especially if the enemy is technologically well developed (Geers, 2017).

### a) Cyber crime

'The 2010 Resolution of the United Nations on cyber security defines cyber crimes as first main challenges to country's security in cyber space' (Ayofe, 2009 16). It is important to differentiate cyber crimes from computer based crimes which are often perceived as a broader term involving crimes which do not include a network intrusion. Cybercrime is a narrow term which is understood as an 'illegal behavior directed by

means of electronic operations that target the security of computer systems and the data processed by them' (Ayofe, 2009: 16).

The first cyber crimes took place right after the emerge of Information and communication technologies and first uses of them. However, the first cyber crimes were less sophisticated and could rather fit the concept of computer-based crimes rather than cyber crimes as mentioned above. The first cybercrime of such type was recorded in Canada in 1969. It was an attempt of a student to burn a computer in order to steal data. In 1970$^{th}$ computer based crimes became quite spread in the United States which led to the first attempts to adopt a bill on cybercrime prevention in this country. The speed of technology and internet development and its spread increased the level of sophistication of cyber crimes and therefore there was a necessity to adopt a new international agreement which would introduce regulations and common standards when addressing cyber crimes. Thus, the Budapest Convention on cybercrime was approved in 2001 and with few amendments later on still remains the main international bill on understanding, preventing and tackling cyber crimes. Cyber crimes are often conducted outside the victim country since the crime in a computer network can be conducted from any territory and the further that territory is (not only geographically but also legally) the easier it will be for a cybercriminal not to be caught. This makes cyber crimes specifically complicated and requires active involvement of all countries in catching cyber criminals.

### b) Cyber terrorism, cyber attacks and cyber sabotage

Cyber attacks, cyber terrorism and cyber sabotage are differentiated from cyber crimes because of the goals these two threats pursue. The means which are used to conduct both cyber crimes and cyber attacks are the same, however the aim of cyber criminals is usually to get economic or some other personal gains while the aims of cyber terrorists are often political. There is no agreement or common understanding in academia regarding the term cyberterrorism and cyber sabotage, however everyone agrees that cyberterrorism takes place if there is a motive of causing fear in the society. The term itself was coined by Barry Collin, a senior research fellow at the Institute for Security and

Intelligence in California in 1997. He explained the term as the use of terrorism in a new space – cyberspace (Abomhara, 2015). In 2008 the definition of cyberterrorism was given by NATO which is understood there as "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal" (Kurnava, 2016). Department of Homeland Security (DHS) of the United States defines cyber terrorism as '"a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies" (Kurnava, 2016).

As for cyber attacks, there are two types of them– the ones focused at attacking data and the ones focus at attacking control systems. The first type of cyber attacks is most widely spread and is more related to the concept of cyber espionage when the second one is more dangerous and can lead to the malfunction of factories, state infrastructure, services. (Abomhara, 2015). Potential targets which cyber terrorist are aiming at in this context are nation's critical infrastructure and e-government platforms that significantly depend on internet and communication technologies. The more the country is dependent on computer systems and technologies the bigger are the risks of cyber attacks (Abomhara, 2015). The ways the cyber attacks on a country are conducted are 'systems manipulation through secret entrance software, data deletion, Web sites damaging, viruses inserting' such Stuxnet, Blackenergy, Sandworm and others (Bogdanowski, 2013). Both cyber attacks against state websites and e-government platforms and critical infrastructure are dangerous depending on the significance of the object attacked. For example, a country which has a very well development e-government platforms which citizens are using in their everyday life in order to get some basic services from a state such as medical care, administrative certificates, allowances etc. in the event of a cyber attack can suffer significantly and thus prove its inability to provide basic services to citizens (Theohary, 2015). At the same time, an attack against a government web site which just contains information about some services and will not be as dangerous as in the first case. The termination of its work will entail negative image consequences for a country. Same logic applies to attacks against critical infrastructure which are usually referred to as *cyber sabotage*. Consequences of an attack against a nuclear power station will be way worse

than an attack against an electric grid the aim of which is to leave citizens without electricity for some period and trigger a panic (Bogdanowski, 2013).

Thus, cyber terrorism is dangerous because of the relative ease to conduct a cyber attack of a large scale. Conducting cyber attacks does not require many human resources and capitals (Bognanowski, 2013). As with cyber crimes, cyber terrorists can act being physically very far from their target and hard to be tracked. Yet, experts believe that the most damaging cyber attacks are those which combine a cyber attack with a physical terrorist attack.

### c) Cyberespionage

Cyberespionage can be defined as 'the strategy of breaking into computer systems and networks in order to extract sensitive governmental or corporate information' (Morag, 2014:12). Cyber espionage is also referred to as cyber spying by come authors. Cyberespionage is a very wide spread threat which may have or not have a political aim and therefore be considered as a part of cyber crime concept or cyber terrorism respectively and be dealt with on a different level of state security and defense bodies. Cyber espionage is usually conducted by the use of zero days exploits together with spear phishing and watering hole attacks in order to infiltrate the networks and get sensitive data (Morag, 2014). 'Gathered data can also be used for lateral movements within targeted systems in order to get information from other sources though the one the criminals managed to penetrate' (Paganini, 2015). In this context, it is of crucial importance for all actors to cooperate in preventing and countering cyberespionage. Government bodies can contain sensitive information about private companies and vise-versa therefore the good level of cyber protection is needed on both sides (Morag,2014).

### d) Cyber and hybrid warfare

A range of cyber attacks targeted at one country by other countries or non-state actors can be called a cyber warfare which is the part of a broader concept of a hybrid warfare (Pernik, 2015). Both terms are quite ambiguous and do not have one generally accepted definition. As in the case of cyber attacks, cyber terrorism, cyber espionage and cyber sabotage there is no international agreement or treaty which would shed light on common understanding of these terms as it was with the Budapest agreement on cyber crimes. Some scholars tend to call a cyber warfare only in the case that state actors are engaged in offensive and defensive efforts using cyber weapons (Hoffman, 2015; Conca, 2014). Others which are the majority consider cyber attacks conducted by non-state actors against country's critical infrastructure as an act of cyber warfare (Pernik, 2015; Geers; 2017; Malchenyuk 2017). Cyber warfare can be defined then as a 'cyber capacity of a sufficient scale, during a determined period in high speed, to reach certain objectives in or through cyberspace, these actions being considered as a menace for the targeted state.' (Belgium, 2014).

Nevertheless, there is a common agreement among researches that cyber warfare is a part of a broader concept of hybrid war. Firstly, the concept of hybrid warfare was used by William J. Nemeth with regards to the war in Chechnya in 2002 (Nemeth, 2002). It became frequently used also as of 2005 when looking at the strategy of Hezbollah during Lebanon war. After that, the concept became incorporated into political science to describe future and modern means of warfare including both conventional and unconventional weapons (Puyvelde, 2016). Hybrid warfare is used to combat Western predominance in conventional weapons by turning to 'conventional/unconventional, regular/irregular, overt/covert means' (Puyvelde, 2016). However, a number of scholars argue that hybrid warfare itself have not brought anything new in understanding of war. Asymmetries have always been used to target weaknesses of an enemy using conventional/unconventional, regular/irregular, overt/covert means (Bachman, 2014; Neag 2015). Therefore, the emergence of cyber warfare and other modern means of war which are often immediately included in the concept of hybrid war has not changed war`s nature but added another element of warfare along with air, space, sea and land (Hoffman, 2007). For the purpose of this thesis, hybrid warfare is then defined as

sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion (Hoffman, 2015).

### e) Conclusion

Thus, having defined and explained main cyber threats to national's cyber security and resilience as well as the notions of cyber and hybrid warfare this dissertation will look at national's policy in cyber security and resilience of Ukraine from the position of preventing and tackling these threats according to their nature and peculiarities. Cyber crimes are differentiated from the cyber attacks by the goals which these two threats pursue. Cyber attacks and cyber sabotage constitute a broader notion of cyber terrorism which is aimed at causing fear and chaos in the society. Cyber espionage is conducted for the purpose of collecting classified information from government and people. All of these threats if conducted repetitiously against one target usually a country may be called a cyber warfare. Cyber warfare can also be considered as one of the means of a broader concept of hybrid warfare if used for the purpose of influencing people's perceptions and international opinions.

## 3. Cyber security and cyber resilience. The conceptualization of cyber resilience

Achieving security in a cyber sphere has been viewed for a long time as an adequate and realistic goal. However, rapid development of IT has been accompanied with new challenges in cyber security. This lead to shift in ways of providing cyber security. Cyber security has no longer been sufficient and 'provided required protection' (Durbin, 2016). Thus, the need to develop a new approach was articulated first in IT sphere, then in business and on a state level. While resilience as an approach to tackle risks existed in political science for a while (Handmer and Dovers, 1996; Adey and Anderson, 2012; Anderson, 2010; Anderson and Adey, 2011; Aradau and van Munster, 2007; Rasmussen, 2007) it has not been researched and explained enough regarding cyber space on a state level. For the purpose of this research, cyberspace is defined as '…the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries' (Rasmussen, 2007:15).

### a) Cyber security related concepts

Such terms as cyber security, information security, information and communications security, computer security, internet security and cyber resilience in cyberspace are often used interchangeably not only in media but also by government, experts and researchers. It is important to draw the difference between those concepts even though there are ongoing debates in academia on their meaning. ICT security is a broader or umbrella

term which is used to indicate both software and hardware security however it does not relate to security of data in the web (Techtarget, 2009). Information security is used with regards to security of all data either online or printed. Computer security refers to hardware and computers security (Relia, 2016). Internet security has different meaning from technical and political point of views. In IT sphere internet security is usually understood as 'protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of internet services.' (Relia, 2016:231). However, in political science this concept is more related to internet safety, legal use of data, intellectual rights and issues related to censorship on the web (Hathaway; Klimburg, 2015). If we speak about the military side of cyber space, the events of cyber attacks or espionage the term cyber defence is used. Cyber defense according to NATO definition is 'the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace' (NATO website, 2017: 8).

### b) Cyber security concept

Cyber security as a concept became widely used after the year 2000 and the issue with the so-called millennium software bug. Majority of researchers agree that cyber security encompasses all the above mentioned terms and is an umbrella term that indicates 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.' (ITU, 2017;13) However, each country defines cyber security with regards to its peculiarities and needs. Thus, 'cyber security in Germany is the desired IT state in which the risks the country faces from cyber space are reduced to an acceptable and manageable level' (Federal Ministry of Interior of Germany, 2011).

Theoretically, there were few attempts to look at cyber security from a political science perspective. Cyber security tends to rely on either traditional theories of International Relations (realism, constructivism, liberalism) and, more precisely, the concept of cyber

power (Kramer et al. 2010; Nye, Jr 2010; Klimburg 2011a; Betz and Stevens 2011; Sliwinski 20141), or critical security studies which encompass securitization (Eriksson 2001; Bendrath et al. 2007; Dunn Cavelty 2007, 2008). However, there are also few researchers who look at cyber security though regulatory or governance approaches (Brown and Marsden 2007; Mueller 2010). Even though knowledge of all these approaches are useful for understanding cyber security this research will look at cyber security through the prism of cyber power since this approach is the most developed one.

Thus, most authors look at cyber security from the cyber power perspective which according J. Nye is 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power' (Nye, 2010: 4).

However, the authors who look at cyber security through the concept of cyber power differently see the role of non-state actors in its exerting. Thus, Nye believes that 'governments remain the strongest actors in resource terms, even though networks become more important as a tool of governance' (Christou, 2016). Another group of researchers including Betz and Stevens (2011) underline the 'the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace' (Betz and Stevens 2011, p.44). In line with cyber power concept Klimburg defines the following components as underlying to achieve cyber security: efficient coordination, cooperation and cohesion among governmental bodies; work with international organizations and adhering to common policies on cyber security; involvement of NGOs, civil society, businesses and other stakeholders to the process of achieving cyber security. However, Klimburg in his policy paper for the European Parliament argues that 'the most important dimension of cyber power is the ability to motivate and attract one's own citizens, an inward-focused soft-power approach that is fundamental for creating a "whole of nation" cyber capability' (2011, p.43). He claims that in order to achieve resilience (which he does not define) a government (in the paper - 'EU') has to involve civil society and volunteers and build efficient public-private partnerships and informal cooperation.

Nevertheless, while cyber power approach to cyber security stress on the necessity of efficient coordination and communication between actors, it does not do not explain how such partnerships should be built. Same applies to risk assessment which is believed to be important step in projecting cyber power but is not given enough attention to within beforementioned researches on cyber power and cyber security. Stuart Starr in this context argues that understanding of risks and threats is very little 'to employ neither in cyber assessments nor the relationships among those measures' (Starr, 2009). Furthermore, cyber security is rather focused on achieving overall protection in the cyber sphere rather than accepting the need to adapt to constantly changing environment of cyber space and very high probability of success of a cyber attack. And this is where the concept of resilience steps in to offer solutions.

### c) Resilience concept

Resilience is a notion borrowed from material sciences and describes the 'ability of a material to recover its shape after a deformation' (Dahlman, 2011:40). Stephen Cauffman defines resilience as 'the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions' (Caufmann, 2016:3). Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Within various policy fields, resilience is discussed as the answer to a 'world of rapid change, complexity and unexpected events' (Chandler, 2013a: 1).

Concept of resilience has been recently introduced into the political science by connecting this concept with global governance (Pfister and Suter, 1987), by explaining the role of NATO after the collapse of the Soviet Union (Barany and Rauchhaus 2011) and by introducing new approaches in international development and humanitarian spheres using some ideas borrowed from risk management theories (Goldstein 2011; Sendzimir, Reij, and Magnuszewski, 2011; Davies, 2012; Muggah and Savage, 2012). The concept of resilience is quite debatable among scholars and there is no single definition agreed by everyone. Majority of political science scholars who are applying

resilience concept believe that resilience is 'the process of patterned adjustments adopted by a society or an individual in the face of endogenous or exogenous shocks' (Bourbeau, 2015:375). Resilience looks at society as a system which exists in the constantly changing and unpredictable environment (Holling, 1973). However, on the contrary to risk analysis and traditional crisis management strategies resilience is aimed at 'preventing and preparing for a potentially disruptive future and is characterized by a temporality that combines the present with the future, but also actively deals with insecurities of the past' (Cavelty, Kristensen, Kaufmann, 2015). Resilience concept found its profound coverage within the critical security scholarship over the past few years. Majority of critical literature on resilience stems from Anglo-Saxon academia and empirical researches of Joseph, 2013; Chandler, 2012, 2013b; Duffield, 2012; Rogers, 2013b; Williams, 2013; (Handmer and Dovers, 1996; Adey and Anderson, 2012; Anderson, 2010; Anderson and Adey, 2011; Aradau and van Munster, 2007; Petersen, 2012; Rasmussen, 2007. In theory, critical scholarship on resilience looks at where resilience is placed within liberal security scholarship and what it brings to it. (Chandler, 2012, 2014; Duffield, 2012; Evans and Reid, 2013; Lentzos and Rose, 2009; O'Malley, 2010; Walker and Cooper, 2011; Zebrowski, 2013)

There were few attempts to categorize resilience by different scholars in order to systematize the understanding of it. Thus, Rogers (2013) suggests looking at three categorize of resilience – organizational, community and technological depending on where resilience takes place. Walkate (2013) at the same time identifies resilience within different society levels: human level, family, institutions, religions, nations and global level. Bourbeau (2013) uses different approach and suggests looking at categorizes of resilience from political perspective which appears as a result of a choice of political actors rather than exists as a 'self-emergent autopoietic processes of (complex) systems' (Handmer and Dovers, 1996). Resilience is studied by looking at two main topics – temporalities and subjects. As for temporalities resilience is seen as a preparedness to the event in the future which thus defines the present (O'Malley, 2010: 488). However, it also looks at past experiences which are useful to prepare for possible future threats (Evans and Reid, 2013: 91).

Subjects of resilience are mostly explained through a neo-liberal doctrine where they are claimed to a result of active self-organization in the events of crisis. However, resilient subjects may also be government backed but in fewer cases (Bulley, 2013; Rogers, 2013a). Resilience is aimed to change focuses and responsibilities for security. Resilient subjects exist due to the shift from 'government to municipalities, from national to local, from security authorities to the citizen – expecting and encouraging beneficial self-organization in the face of crisis by those units that are both knowledgeable of local contexts and directly affected by the adverse event' (Hagmann and Dunn Cavelty, 2012). Civil society which is self-organized plays a crucial role in achieving resilience and acts as a central subject of this concept. The role of private sector and cooperation with a state in the form of public-private partnerships is also emphasized. Public-private partnerhip is "a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance" (World Bank, 2017).

Resilience can also be seen as 'as a precursor to security—that is, as a process leading to and inducing security (Bourbeau, 2015:383). However, in case of applying 'security does not refer to the absence of danger but rather the ability of a system...to reorganise to rebound from a potentially catastrophic event.' (Cavelty, 2013: 23). Resilience approach is focused more on solutions rather than problems implying more defense spending (Jegen, Merand, 2014). In the field of crisis management and emergency response international organizations together with the United Nations, have introduced resilience as a 'new organizing principle, the development of which is perceived as critical to preventing unacceptable levels of human suffering and reducing the costs of international emergency response' (Bourbeau, 2015:377). The definition provided by the UN thus portrays resilience as a solution to reduce costs by involving all stakeholders to preventing and reducing the negative consequences of crises.

### d) Cyber resilience

Cyber resilience in its turn is was introduced as an answer to 'increasingly inadequate response to the modern cyber threat landscape' provided by the concept of cyber security (IT Governance, 2017). Cyber security according to IT scholarship claimed that computer system can be protected from any potential cyber risk. Cyber resilience on the contrary accepts that a 'cyber attack will inevitably succeed' (IT Governance, 2017). Cyber resilience thus is about identification and responding to cyber attack in order to achieve the survival of a computer system. Cyber resilience concept was built on the merge of traditional cyber security approach and business resilience. It consists of two main components:

- Ensuring cyber security without reducing some capabilities of computer systems.
- Having a business plan which would stipulate the way to secure critical information in case the cyber attack is successful.

Cyber resilience also stresses on changing the general perception of security in IT. It focuses on changing the culture and behavior when dealing with computer systems. Apart from setting a business plan and improving organizational leadership it talks about working with all employees who deal with computer systems. 'Investment in research, education, and identification of best practices needs to underpin this cultural aspect in the long-term' (Nicholas, 2016:23). Cyber resilience from the point of view of IT sphere thus can be defined as the 'preparations that an organization has made with regard to threats and vulnerabilities, the defences that have been developed, and the resources available for mitigating a security failure after it happens' (World Economic Forum papers, 2012).

Cyber resilience concept in political science was applied by George Christou in 2016 towards EU activities in cyber dimension. He fused the concepts of cyber governance and resilience in order to look at cyber security as resilience. By doing so he looked at resilience as proactive rather than reactive by 'accepting not resisting the inevitability of change and the creation of a system that is capable of adapting to new conditions and imperatives' (Christou,2016). At the same time traditional security governance approach

does not focus much attention on the complexity of meta-governance (Cavelty,2008) and relations between private and public sector. Therefore, the success of the cyber security as resilience concept lies in 'coalitions of different actors working together in partnership to construct new flexible and adaptive institutions and operating procedures, set the agenda and implement policies' (Christou, 2016). Such coalition should be supplemented by the decent level of IT education of citizens. Investment in research, education, and identification of best practices needs to underpin the 'cultural aspect' of cyber resilience in the long-term (Nicholas, 2016).

Among actors which have to be involved in providing cyber security are civil society which is a key element in building resilient communities and businesses. Private sector as mentioned can cooperate with a state on a basis of private-public partnership models. Usually critical infrastructure is owned at least by 50% by private companies which provide tools such as antiviruses, IT security trainings to ensure security of cyber component of their enterprise. However, if an attack takes or may take place and its source is hard to find a country has means 'collect foreign intelligence, collaborate with other international agencies, and gain access to critical information regarding potential threats' (Jagasia, 2017:2). There are many models upon which a business and a state can form a partnership and its selection depends on many factors ranging from interest of parties to cooperate, level of trust, available resources etc. One of the examples of efficient private-public partnership in cyber security was established in Netherlands between local businesses and a state. Both institutions responsible for decision making on national cyber security within a state – Cyber Security Panel and Government Regulatory Body are formed on the basis of private-public partnerships (picture 1) to increase trust between all partners, discuss mutual interests and prospects of cooperation.

In strategic view, cyber resilience can be understood as an element of 'deterrence by denial, or persuading the enemy not to attack by convincing him that his attack will be defeated – that is, that he will not be able to achieve his operational objectives.' Thus, in events of hybrid warfare and its component cyber warfare resilience is aimed to prepare

the nation to the extent that the attack will not make sense to be placed (Pernik, 2015). For this purpose the following goals are to be achieved:

1. Good societal competencies in understanding the nature of cyber warfare tools and ways to oppose them (Cavelty, 2015)
2. High level of trust between civil society and government provided through efficient government communication, political leadership and integrity of political system (Pernik, 2015; Rhinaud, Sundelius, 2014).
3. Strong sense of community between different groups of citizens, availability of local opportunities for citizens aimed at their empowerment, equity in economy that helps to reduce possible tensions between different groups in society and a state (Pernik, 2015; Rhinaud, Sundelius, 2014).
4. High level of development of volunteering culture in the country specifically with regard to security and defense; existence of grass root security organizations and initiatives aimed at strengthening national security (Pernik, 2015; Rhinaud, Sundelius, 2014).
5. High economic development as well as economic diversification and preparedness to reduce the possible damages of a cyber attack targeted at state`s economic activities.
6. Ability of critical infrastructure, as well as ICT systems to reduce the impact of cyber attacks, espionage or sabotage, adapt and continue working in the normal regime. (Rhinaud; Sundelius, 2014).
7. Efficient coordination of all actors involved in providing cyber resilience. 'A high degree of cooperation capacity translates into fewer transactions costs that impede both shared sense-making and collective action-taking' (Rhinaud; Sundelius, 2014).
8. Necessary amount of reserves such as financial resources, technical equipment and software which would allow to quickly renew damaged objects and avoid a possibility of an attack to have a broad negative impact on 'the nation's will to persevere' (Yost, 2003).

### e) Cyber resilience criteria

Thus, having analyzed the approaches to resilience from different perspectives the following criteria are identified as necessary to achieve cyber resilience at the national level:

*1. Efficient coordination and cooperation of all actors involved in providing cyber security of the country.*

Special role in this regard is played by state agencies and bodies, their transparency and readiness to share critical information with all stakeholders including foreign partners and due to often international nature of cyber attacks. Coordination is also needed to avoid duplication of a high number of actors involved in achieving cyber security. Leadership and high level of trust is required to act fast on both strategic and operational level in the event of a potential cyber attack or in case a cyber attack occurred to quickly regroup and reduce shortcomings (Yost, 2003).

*2. Private-public partnerships between businesses and government.*

Business can provide not only resources and tools regarding national cyber resilience but also unique expertise which by being formed in the business and competitive environment is considered to be more 'proactive and risk-managing oriented. Private-public partnerships may be established under different conditions in accordance with the agreement between a state and business.

*3. Social capital built on strong communities and volunteers are crucial for achieving resilience in any sphere including cyber.*

The resilience approach moves 'from government to municipalities, from national to local, from security authorities to the citizen – expecting and encouraging beneficial self-organization in the face of crisis by those units that are both knowledgeable of local contexts and directly affected by the adverse event' (Hagmann and Dunn Cavelty, 2012). Robert Deibert maned civil society as an "increasingly recognised and important

stakeholder in cyberspace governance" (Deibert, 2011). Grass root organizations and initiatives are able to respond quickly to potential or actual threats. High level of trust between governmental bodies and agencies and communities are crucial for the efficient work of such communities (Pernik, 2014).

*4. Good level of IT and cyber security education provided at school, Universities, educational institutions as well as general cyber security awareness at public and private organizations focusing on new threats and rapid growth of ICT should be provided at all levels.*

Experts agree that the majority of cyber crimes, breaches and attacks are caused by ordinary people who are not aware of simple 'cyber hygiene' (Pescatore; 2002). Since hackers and intruders are very well aware of this people's vulnerability they often take advantage of it and plan the attacks accordingly (Payne; 2003).

## f) Conclusion

Therefore, different concepts regarding security of ICT and computers were identified and compared. Focusing most at the theoretical framework of cyber security, resilience and cyber resilience and their interplay for the purpose of this research cyber security was analyzed through the cyber power approach developed by Nye (2010) and Klimburg (2009) While cyber security focuses on achieving overall protection in the cyber sphere rather than accepting the need to adapt to constantly changing environment of cyber space and does not equally recognize the growing role of non-state actors cyber resilience provides a new approach to national cyber security policies. Even though scholars looked at resilience from different perspectives within the theory of good governance or humanitarian response in political studies all of them agree that resilience's added value lies in explaining the advantages of active self-organization in the events of crisis and ways to reorganize to rebound from a potentially catastrophic event as well as shift from responsibilities for security to different stakeholders (NGOs, businesses). These

resilience's features are applied also towards cyber space where the level of unpredictability and constant change is very high. Cyber resilience, thus looks at such criteria as efficient coordination and cooperation of all actors and stakeholders, civil society, private-public partnerships and IT security awareness which are necessary to efficiently respond to the changing nature of cyber threats. Particularly these four criteria are defined above will be used to test Ukrainian policy on cyber security on its correspondence to the emerging concept of resilience.

## 4. Cyber security and cyber resilience on the national level

Having looked at cyber security and cyber resilience concepts, it is important to define how they are implemented on the policy level of the state. There are many approaches to understanding policy specifically public policy but for the purpose of this research, public policy is seen as a set of 'governmental decisions and the result of activities which the government undertakes in pursuance of certain goals and objectives' (Torjman, 2005:3). The main aim of the public policy is to provide solutions to existing and possible issues related to the public (Torjman, 2005).

### a) National security

There are many spheres in which the government applies public policy, one of which is national security. Understanding of national security differs according to each countries' priorities and needs. Furthermore, the concept is complex since it has to respond to threats which constantly evolve and change over time. While security as a concept concerns among others human or individual rights to stay safe and protected from threats national security concept encompasses those aspects of security for which a state can take

responsibility for. Therefore, national security is a political construct which looks at the spheres of security where the state is or may be involved. These spheres are economy, social and political life and among others cyber space. National security in cyber space is called *National Cyber Security* and is defined as 'the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security' (Klimburg, 2016:29).

### b) National Cyber Security policy

National Cyber Security policies are formed using different approaches according to a country's priorities. Some countries are more prone to cyber threats due to high level of development of ICT technologies (for example USA, Great Britain, Germany, Estonia). There are also countries which do not consider as necessary to have an integrated Cyber security policy. Provisions related to cyber security are incorporated into broader National Security doctrines though majority of countries have cyber component related to defence forces (Argentina, Philippines, majority of African countries) (Subrahmanian, Ovelgonne, Tudor, 2015). In general, introducing of Cyber Security policies is a relatively recent phenomenon which apart from USA became the most evident for majority of countries only in the 21 century. Around one hundred countries in the world own cyber capabilities and only fifty of them adopted specific policies usually in the forms of a strategy on cyber security. Cyber security strategy is thus a "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power' (US National Military Strategy, 2004). The main aim of a cyber security strategy according to ENISA (European network and information security agency) is 'to increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole.' (ENISA guide, 2012). This goal can be broken down into few concrete objectives which are tackling cyber crimes, raising awareness about cyber risks, securing government online systems, adopting efficient legislation on cyber security, strengthening infrastructure, supporting civil society initiatives in cyber security, clarifying foreign policy in cyber security. All

these efforts should contribute to the economic prosperity and increase of cyber resilience of the country.

NCS policies should have at least three functions:

- Provide a vision for government agencies and bodies on cyber security priorities in order for them to develop coherent policies.
- Facilitate the adoption of sub-strategies in other spheres that cyber security provisions are incorporated.
- Define spheres where resources are needed to achieve cyber security and resilience (Klimburg,2016:46).

Stakeholders of the NCS policy are government citizens, owners of critical infrastructure and businesses prone to cyber threats, government systems. However, depending on a country and its NCS policy stakeholders are defined differently with using different approaches to address them. Thus, 'historical, cultural, legal, organizational and political structure of a nation can lead to significant differences in working with stakeholders, ranging from a cooperative approach, public-private partnership, to mandatory legislation and regulation' (NATO Manual, 2016; 35).

Cyber security policy should define three main levels at which cyber security efforts are to be undertaken as well as their system and relation with each other – governmental, non-governmental and international (Klimburg,2016) It is important that NSC documents do not exist independently from other national security doctrines and are connected with them. As for the structure of a National Cyber Security policy there are three dimensions which are to be identified as mentioned above. On the governmental level, usually a large number of state agencies and bodies are involved in providing cyber security including ministries of defense, telecommunications, police, infrastructure, commerce. This is unavoidable due to the scope and depth of the issues related to cyber security. What is important here is to make sure that the coordination, communications and trust between all these bodies and agencies is ensured on the highest level. This one of the major challenge which National Cyber Security policies face which can be solved by a range of various approaches such as appointing an organ responsible for coordination of state

efforts in cyber security and resilience or/and improving the channels of communication between different bodies and agencies.

Another important dimension of every NCS policy is the inclusion of an effective mechanism which would facilitate the cooperation of the state and non-governmental actors in providing cyber resilience. Due to the rapid growth of a number of non-governmental actors in cyber sphere it is specifically important to give them voice and make sure that they are able to realize their potential. Some look at the third national dimension of NCS policies as at cooperation between state and private companies which own critical infrastructure. However, while such cooperation is crucial, the equal attention should be given to civil society capacities and small and medium business capabilities. According to the comprehensive approach to security or the whole nation approach a 'wide range of non-state actors (in particular private companies but also NGOs) should cooperate with the government on cyber security issues.' (CCDCE manual, 2016). Such cooperation can be ensured by applying different methods – through consultation meetings and easing legislation regarding the work of NGOs and small and medium businesses in cyber security sphere to the support of security of such enterprises and exchange of critical information.

Having defined the objectives, stakeholders and approaches to work with them as well the structure of NCS policies it is also important to focus on strategy development process. Thus, there are three approaches a country can take when developing a NCS policy – bottom-up, top-down and re-iterative approaches. The selection of the approach depends of the role which every category of stakeholders plays in implementing NCS policy. Some countries such as the United Kingdom and France have applied pure top-down approach taking control over developing of legislation, policies and strategic documents which form a NCS strategy. The advantage of such approach is 'an increased focus on the document and the development of policies is far more streamlined', however civil society and businesses may not agree on some provisions and negatively respond to the government (Klimburg, Healey, 2016:90).

In order to avoid criticism from the part of civil society and businesses some countries apply a mixed approach combining bottom-up and top-down features which is called re-

iterative approach. In 2003 when the National Strategy to Secure Cyberspace started to be developed US government used a bottom down approach by inviting experts, cyber security companies and other businesses in consultation meetings which ensured an overall acceptance of the strategy by citizens and businesses. However, in 5 years when cyber security threats became more dangerous to state system US government adopted another strategy – the Comprehensive National Cyber Security Initiative this time behind closed doors. Even though this document included some provisions elaborated within the first strategy its main part was worked out by the government and was made classified.

Some other countries such as Germany and Netherlands applied a pure bottom-up approach involving civil society and business in defining NCS agenda. It is also important to stress that bottom-up approach does not concern only the involvement of big private companies concerned with cyber security issues. It is main idea lies in involving all stakeholders in the process of NCS strategy development. For example, when developing its NCS strategy Netherlands established the Dutch National Cyber Security Council which serves as top level advisory organ on cyber security in the country. Eight out of 14 members of the Council are representatives of private sector and NGOs. The co-chair of the Council is also always a non-state actor.

### c) Conclusion

Thus, cyber security and cyber resilience is addressed within National cyber security policies of each country. NSC policies are a part of a broader concept of national security of each country which are designed to tackle challenges which exist in cyberspace. NCS policies are to serve as guidelines for a country on how to approach cyber risks and provide cyber security by addressing the needs and capabilities of all stakeholders in cyber sphere. It was proved that NSC policies should address three fundamental levels – governmental, non-governmental and international. Forms, objectives and content of all NCS policies differ according to the priorities and needs of every country. Three main approaches to developing a NSC policy were also identified: bottom-up, top-down and re-iterative ones depending on how much different stakeholders of cyber security are

involved in NSC policy. Some governments involve non-state actors into the process of development of NCS policies, others keep large of their parts classified.

# Ukrainian case study

## 5. Overview of Ukrainian policy on cyber security. History and current state

### a) Summary of cyber attacks in Ukraine

Ukraine has been a target of a large number of cyber attacks and cyber crimes throughout its history. The first cyber attack which took place in Ukraine was targeted against Ukrainian banking system and its state bank 'Ukraine' (Buryachok; 2016). An attack took place in 1995 and ended with the loss of 4 million of dollars from the state bank. The next biggest cyber attack took place in 2007 and was targeted at government websites. It was a massive DDos attack which lasted for 3 days but received very little reaction from government. DDos attacks is 'an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources' (Gu, 2007). In a statement late made by the state security service, it was mentioned that cyber attacks against government web sites were taking place quite often all around the world and there

are limited ways of resisting them (Buryachok, 2016). Other 'big' cyber attacks and cyber crimes, which were taking place before 2014 and should be mentioned are:

- 1997 – an attack against Global Ukraine internet provider which stopped its work for few hours
- 2000 – an attack against one of the biggest internet providers Ukr.net
- 2012 – a series of DDos attacks targeted at a state IP in the course of parliamentary elections

Most cyber attacks against Ukrainian critical infrastructure and state websites took place in 2015-2016, one year after the war with Russia started. Data on the biggest cyber attacks are provided in table 1. According to the statement made by Defence Minister of Ukraine Mr. Poltorak, 'there were at least 7000 cyber attacks against Ukrainian critical infrastructure and government websites since the war with Russia started in 2014' (Poltorak, 2017). Furthermore, according to Kaspersky Security Network statistics, Ukraine is the 9th country in the world according to the number of cyber attacks and crimes taking place. Around 33,7% of Ukrainians faced cyber threats for the last 3 years. (Kaspersky security network, 2017).

### b) Development of legislation in cyber security

Even though Ukraine has been a target of large cyber attacks throughout its history, there has been a lack of specific policy regarding the prevention and tackling of cyber attacks. Until 2014 cyber security issues were scarcely discussed on the governmental level. There were no laws and regulations which concern cyber attacks or cyber crimes. Issues related to security of cyber space were looked through the concepts of information and computer security. The concept of cyber security however, was incorporated in the doctrine of information security and was mentioned only as a part of this broader concept. Such approach was taken since in Ukrainian academic tradition the term cyber is used with regard to technical issues. The term information security in its turn has a broader scope and used to incorporate some issues regarding cyber security.

Thus, according to Article 17 of the Constitution of Ukraine, which was adopted on 28 June 1996, 'protection of sovereignty and territorial integrity of Ukraine, its economic and information security is one of the main functions of the state and all Ukrainians'. The

next fundamental document in the sphere of national security ‘On the basics of national security’ was adopted on 19 June 2003. Article 7 of the law defines the threats to national interests and security in information sphere:

- Restrictions on freedom of expression and access to information;
- Distributing violence and pornography in media
- Computer crime and computer terrorism;
- Disclosure of confidential information which is owned by the state to public
- Attempts to manipulate public opinion, especially by dissemination of false, incomplete or biased information.

The law also touches upon the need to protect information sovereignty of Ukraine, to develop national information infrastructure and innovations and confront the monopolizing of the information sphere of Ukraine. For the first time, the terms of computer crime and computer terrorism were used in Ukrainian policy towards information and cyber security. (Buryachok; 2016). However, both terms were not defined by law. The next strategic document which touches upon the issues of information and cyber security was adopted in 2012 and is called the Strategy of National Security. While the strategy among others defined the issues of information security in Ukraine due to the growing number of cyber crimes and attacks for the first time the intention to adopt a Strategy which would be focused specifically on cyber security issues was declared.

As for cyber crimes, for the first time the criminal responsibility for conducting *automating crimes* was incorporated into the Criminal Code of 1960, article 198-1 in 1994(). However, when the Criminal Code of independent Ukraine was adopted in 2001, issues related to cyber crimes took the whole chapter and three articles – 361 (unlawful usage of computers), 362 (stealing, acquisition and extortion of personal data), 363 (the distortion of usage of computers). The law № 908-IV adopted in 2003 amended the Criminal Code and Cyber crimes chapter by including the size of the fine for conducting cyber crimes. Finally, the Criminal Code was amended in 2004 by the Law № 2289-IV which incorporated few new provisions of the articles 361, 362, 363 mainly by specifying the types of cyber crimes.

Thus, together with the mentioned laws and regulations the following laws were regulating issues related to cyber security until 2014 and today:

- On information
- On National Security of Ukraine
- On State Special Communications Service and information security of Ukraine
- On Telecommunications,
- On protection of information in telecommunication systems
- On Access to Public information
- On Defense of Ukraine
- On the principles of domestic and foreign policy
- On state organs of increased risk

There are also Decrees of the President of Ukraine:

- Doctrine on information security
- Ukraine's National Security Strategy
- Military Doctrine of Ukraine

As well as decrees of Ukrainian government and National Security and Defence Council. As for international agreements Ukraine ratified the Council of Europe Budapest Convention on cyber crime in 2005.

### c) Recent changes of legislation in cyber security

If looking at recent developments in cyber security legislation in Ukraine we can define two main periods of development of Ukrainian policy in cyber security. The first one took place in 2010-2013 when the first discussions on the importance of cyber security resulted in the first policy papers being drafted and normative acts adopted by respective state agencies. The second period began in 2014 after the war with Russia started and Ukraine became a victim of a large number of cyber attacks which according to Ukrainian officials were conducted by Russia (Poroshenko; 2017, Turchynov; 2017; Poltorak; 2017; Zolotukhin; 2017).

During the first period of development of NCS policy, the development of the law on cyber security as well as the cyber security strategy has begun. The idea to adopt a law on cyber security was first introduced in 2011 by State Service of Special Communication and Information Protection (SSSCIP). However, representatives of other state agencies involved in cyber security during the first meeting on the draft law started to argue on which responsibilities will be assigned to each agency and were afraid to lose control over some areas of responsibility. Therefore, the process of development and adoption of the law took much time and still has not finished (Dubov; 2017). From the other hand, state agencies involved in cyber security managed to find a compromise around a document which does not have a binding force - cyber security strategy. The Strategy was approved in 2016 and identified main cyber security threats to the country, introduced a clear division of responsibilities between state actors involved in cyber security as well as mentioned the important role of non-state actors in achieving cyber security.

According to the Strategy, cyber security is viewed as a 'condition of protection of vital interests of citizens, society and state in cyberspace, which is achieved by a complex use of legal, organizational, informational measures and is based on the following principles: rule of law and respect for the rights and freedoms of citizens; Ukraine's national interests; openness, accessibility, stability and security of cyberspace; public-private partnerships, broad cooperation with civil society in the field of cyber security and cyber defense; proportionality and adequacy of the measures taken to tackle existing and potential cyber risks; prioritizing preventive measures; inevitability of punishment for committing cyber crime; priority of development and support of scientific, technological and industrial potential of the country; international cooperation aimed at strengthening mutual trust in the field of cyber security and the development of common approaches in combating cyber threats; consolidation of efforts in the investigation and prevention of cyber crime, preventing the use of cyberspace in illegal and military purposes; ensuring democratic civilian control by established military forces and law enforcement agencies operating in the field of cyber security according to the laws of Ukraine' (National Cyber Security Strategy of Ukraine, 2016). As for the role of non-state actors the Strategy used

a top-down approach according to which the development of legislation, policies and strategic documents which form a NCS strategy are done primarily by the government. The division of the responsibilities of the main state agencies involved in cyber security are highlighted in Chapter 5.

As for cyber crimes, there were no additional amendments taking place with regard to the Criminal Code, however the National Police was strengthened by a new division specifically focused on cyber crimes – Cyber Police. Cyber Police was introduced in 2015 as a part of the general reform of National Police in Ukraine in order to prevent, tackle and investigate cyber crimes.

### d) Conclusion

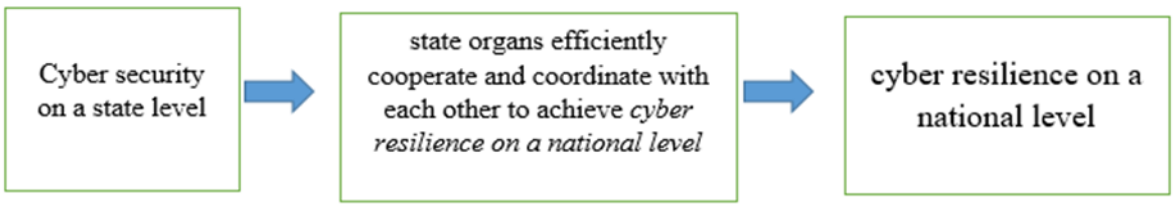
Ukraine has been a target of cyber attacks and cyber crimes since proclaiming its independence however, the biggest number cyber attacks and cyber crimes took place after the beginning of conflict in the Eastern part of the country. In order to efficiently respond to the growing number of cyber threats Ukrainian government amended and updated its legislation regarding cyber security which until 2015 looked at cyber security within the broader concept of information security. The legislation on cyber crimes from the other hand has been lastly amended in 2005 and remains actual till today. Starting from 2011, the ideas on adopting a Law and a Strategy on cyber security have been introduced. While the law has provoked discussions among the stakeholders and has not still been adopted, the compromise was found around the Strategy which in comparison to the law does not have a binding force. The Strategy was adopted in 2016 and introduced the definition of cyber security and cyber threats to the country, division of responsibilities among state bodies involved in cyber security as well as mentioned the important role of non-state actors in achieving cyber security.

## Process tracing of the causal mechanisms

### 6. Coordination and cooperation on a state level

#### a) Observation phase

Coordination and cooperation of state bodies involved in cyber security is a prerequisite to achieving cyber resilience on a national level therefore this chapter will look at how efficiently such cooperation and coordination is build and identify challenges. The causal mechanism consists from the independent variable – *cyber security at the state level*, the element which has to be proved by looking at its factors - *state organs efficiently cooperate and coordinate with each other to achieve cyber resilience on a national level* and the dependent variable – *cyber resilience on the national level.*




There is a big number of state bodies which are involved to different extent to providing cyber security and resilience in Ukraine. The main state bodies and the challenges to their

cooperation and coordination with each other will serve as factors which are used to prove the element of the causal mechanism.

### b) The analysis of the element's factors

According to the National Strategy on cyber security as of 27 January 2016 the main obligations on providing cyber security in Ukraine are assigned to such organs as:

- Presidency of Ukraine.
- National Security and Defense Council of Ukraine.
- The Cabinet of Ministers of Ukraine.
- The Security Service of Ukraine.
- The Ministry of Internal Affairs of Ukraine.
- State Service of Special Communication and Information Protection.
- The Ministry of Defense of Ukraine.
- The Ministry of Information Policy of Ukraine.
- The National Bank of Ukraine.
- Respective national intelligence agencies

According to the National Cyber Security Strategy, the State Service of Special Communication and Information Protection of Ukraine aims to improve the 'development and implementation of state policy in cyberspace; protection of state information resources; protection of critical infrastructure, state control in these areas; coordination of other bodies on cyber security in Ukraine; the implementation of organizational and technical measures to prevent, response to cyber attacks as well as elimination of their consequences, providing information on cyber threats and appropriate methods of protection against them; supporting the work of state cyber center; auditing security of critical infrastructure'(the National Cyber Security strategy, 2016). In fact, the State Service of Special Communication and Information Protection is a crucial organ for providing cyber security to the country. It provides secure working conditions for all state web services, provides cryptography security and makes sure that the complex system of

information protection is implemented by all state and semi-state organizations. Complex system of information protection (CSIP) consists of different organizational and technical measures on information security and was adopted a number of respective Laws and regulations on information security in 1994 and 1998 (Law on information protection, 1994; Decree on technical protection of information, 1998). The rapid development of digital security requires respective development of regulations and laws on a state level. CSIP is still regulated by the laws of regulations of 1990$^{th}$ and is outdated (Dubov, 2017). Furthermore, the process of adoption of CSIP for state organs is expensive and long. The starting price for implementing CSIP is 80 000 UAH which according to state budget allocated for administration of state organs (annual budget for Parliament's administration was 906,2 UAH in 2016) is very high. Furthermore, Ministry of finances became a victim of the cyber attack on 16 December 2016. The Ministry implemented CSIP on five of its servers however all of them were as easily broken as three other serves which did not use CSIP. Some state organs are not implementing CSIP since the penalty for not implementing it is around 3000 UAH or 3,5% of the price of the whole CSIP and it turns out cheaper to pay the fine in the end (Dubov, 2017). All these events prove the inefficiency of CSIP and the necessity for modification or a complete change by the State Service of Special Communication and Information Protection.

The second organ responsible to cyber security of the country is the State Security Service which deals with the prevention, detection and elimination of crimes against the peace and security within the cyberspace of Ukraine. Furthermore, it deals with the implementation of counterintelligence and operational measures on combating cyberterrorism and cyber espionage, as well as critical infrastructure preparedness for possible cyber attacks (the National Cyber security strategy, 2017). However, the work of the Department for counterintelligence protection which is responsible for cyber security within State Security Service is kept secretive. The majority of speeches and interviews on cyber security given by officials of State security service proves that the attention to this topic is relatively high (Dubov, 2017). The former head of the State Security Service stated that `according to statistical data, damage caused to a country by cyber crimes and attacks is much higher than from traditional forms of crime' (Kalinin, 2012). Due to the

rapid growth of technologies and wider use of internet and online services by citizens this number is increasing every year (State statics service, 2017).

According to the National strategy on cyber security both State Service of Special Communication and Information Protection and State Security Service are responsible for licensing of secure transportation protocols AS1, AS2 and AS3 which may result in duplication of their work. However, in fact both organs managed to divide their responsibilities. State Service of Special Communication and Information Protection is revising the technical parameters of transportation protocols while State Security Service is making sure that paper work and documentation are prepared in accordance with the requirements (Zhora, 2017).

The main role of fighting cyber crimes is played by the Ministry of internal affairs and national police. There is a special department on fight against cyber crimes within the Ministry, which is aimed at developing and implementing state policy on preventing and fighting with cyber crimes. The national police and its cyber police sector is responsible for prevention, detection, and fight with cyber crimes as well as raising public awareness about security in cyberspace (National Cyber security strategy, 2016).

Complications and duplications may, and are taking place, on the understanding of Articles 361, 362, 363 of Criminal Code of Ukraine which refer to crimes in information and computer sphere. Sometimes it is hard to distinct a cyber crime from a cyber attack due to absence of knowledge about their purposes (Geers, 2017). Some cyber crimes even though targeted at private organizations or individuals may be carried out with the purpose of violation of territorial integrity or other issues which fall under the mandate of State Security Service (Dubov, 2017).

Another governmental body responsible for cyber security in Ukraine is the Ministry of defense which is specialized at cyber defense of Ukrainian military forces. Its functions lie in taking measures on repelling military aggression in cyberspace; implementation of military cooperation with NATO, providing consistent protection against cyber threats (National Cyber Security strategy, 2017). There are two main departments responsible for cyber security within the Ministry of Defence – Administration of information technologies and Main administration on communication and information systems. The

functions of the departments include ‘organization of communication and automated command of troops in the Armed Forces of Ukraine; the operational management of telecommunication networks of Ukraine for the purpose of state defense; preparation of the communication system and automation of the control of troops of the Armed Forces of Ukraine and control over the preparation of telecommunication networks of Ukraine; participation in the implementation of state policy in the field of information security and counteraction to cyber threats in information and telecommunication systems of the Armed Forces of Ukraine; participation in military cooperation on issues related to the development of the system and communication facilities of the Armed Forces of Ukraine, information security and counteraction to cyber threats’ (Administration of information technologies, 2017). Even though the functions of the Ministry of defense listed in the Strategy and other regulations are quite wide their participation in coordination meetings on cyber issues organized by the Council of National Security and Defense is quite limited. Ministry of defense exerts its main duties within the war time (Dubov, 2017) however, there is no definition of cyber war in Ukrainian legislation and Ukraine has never proclaimed its involvement in cyber war in Russia on the official level.

The National bank acts as a regulator in protecting personal data. Furthermore, it is also tasked with ensuring cyber protection of critical bank infrastructure (Zhora, 2017). While the National Bank is focusing on ensuring that critical bank infrastructure is able to resist cyber crimes, it has fallen a victim of large cyber attacks at least twice within the researched period which resulted in a loss of 8 millions of UAH in the first cyber attack (Malchenyuk, 2017). These events show the lack of efficiency of the National bank in resisting cyber threats, which undermines its authority as regulator in the protection of critical infrastructure in banking sector.

An attempt to coordinate the bodies responsible for cyber security of the country was first made in 2014 when the National Security and Defense Council became a coordinating body on cyber security in Ukraine. Its main aim is to establish a platform for strategic coordination of 6 main state bodies which are looking at cyber security from different angles (Malchenyuk, 2017). They hold meetings which involve all state stakeholders on cyber security to discuss up-to-dated issues few times per year. On the operational level,

the National coordination center of cyber security has been established. The Center is responsible for conducting research of national cyber threats and suggesting ways to tackle them; coming up with indicators on cyber security condition; evaluating national resources including legislative and executive capacities to confront cyber threats; incorporating best international practices on cyber security; developing methods on protecting critical infrastructure; developing means effective means of communication and information exchange between organs involved in providing cyber security; monitoring the process of harmonization of national regulations to the legislation of the EU and NATO; controlling the implementation of decisions taken by the National Council of Security and Defence (National Cyber Security strategy). Even though the center has quite a wide range of tasks its work 'mainly is focused on collecting reports on the results of work of each organ involved in providing cyber security and creating one single report on how cyber security is provided on a state level' (Zhora, 2017). One of the tasks of the Center is to come up with indicators on state's cyber security. However, until June 2017 indicators were only partially agreed on in the State Service of Special Communication and Information Protection. As for general indicators, the Center still has not decided on methodology which should be used to develop them (Dubov, 2017). Such a slow pace of work and absence of indicators reveals that the coordination of state bodies in cyber security is not given enough attention, which is an important criterion for achieving cyber resilience.

Even though attempts to ensure both strategic and operational coordination were made in 2016 by adopting the National Strategy on cyber security, there was a lack of coordination between state organs and agencies which turn, perpetuates negative consequences through the tackling of cyber threats. The Council and the center were not fully carrying out the functions assigned to them. As of January 2016 until June 2017 there were only few strategic meeting of the National Council of Security and Defence and one of the latest decisions it took on banning Russian social media, Vkontakte, provoked many discussions within Ukraine and abroad.

The cooperation and coordination at state level on cyber security does exist according to Dubov, however 'it is based on interpersonal connections of heads of agencies and

specialized departments' (Dubov, 2017). Even though it is important that there is trust between state officials of respective state agencies in order to be able to respond fast to possible threats which is a prerequisite for resilience there must be a mechanism which would ensure regular meeting between all stakeholders in order to exchange information and develop common approaches (Geers, 2017).

Some of the organs involved in providing cyber security are duplicating each other. Furthermore, such duplication is approved on a legislative level. According to the functions of the organs and agencies mentioned above both State Service of Special Communication and Information Protection of Ukraine and State Security Service are responsible for preventing and tackling cyber threats related to the protection of critical infrastructure of Ukraine. Both State Security System and National police are responsible for dealing with the large-scale cyber attacks (Zhora, 2017). However, in fact national police takes responsibility for 'tackling large cyber crimes and attacks conducted by botnets while State Security Service is dealing only with attacks which may result in very negative consequences for Ukrainian economy and national security as well as classified information leaks' (Dubov, 2017).

Even though Ukraine adopted a strategy on national cyber security, there were no additional legislative acts and regulations adopted to provide a detailed mechanism of work for all the organs involved in cyber security as well responsibility for not complying with the norms declared there. Since Law has the strongest legislative power it has a potential to serve as an efficient coordination tool in cyber security. It may also contribute to achieving stronger cooperation among state organs due to clear clarification of their duties and responsibilities (Geers, 2017). A draft law which was suggested by a group of Members of Parliament in 2014 is still under consideration at the Verhovna Rada of Ukraine and is not planned to be approved in the nearest future due to a differing vision being held between different stakeholders (Zhora, 2017).

There are many provisions of the draft Law on cyber security which provoke discussions among key stakeholders and prevent it from being adopted. Firstly, the Law introduces the division between 'technical information' and 'content' (Draft Law on Cyber Security, 2017). Technical information regarding cyber security is thus can be checked by such

organs as State Security Service or State Service of Special Communication and Information Protection if there are some potential cyber risks. However, other state organs as well private sector fear that when checking the technical parameters of cyber protection these organs may also 'spy' or look at some sensitive or secret information of their interest not related to cyber security. Secondly, all state information resources according to the Law must be kept within one place according to the Law (Draft Law on Cyber Security, 2017). However, some of governmental web systems and data such as online state procurement tool Prozorro is kept on foreign servers which according to the new law will be considered illegal (Oleksiuk, 2017). Thirdly, the Ministry of Justice according to current Ukrainian legislation is keeping all state servers and has direct access to them. The new law suggests that these servers must be moved under the responsibility of SSSCIP which may result in losing or duplication of state information resources (Oleksiuk, 2017). There are also issues with security of state data center 'which in current conditions cannot be regarded as safe state data center and be referred to in the law' (Oleksiuk, 2017). Ukrainian data center is placed under the helicopter station in Parkovyi center which due to constant vibrations caused by helicopters is not safe to keep state data (Oleksiuk, 2017).

Ukraine has never conducted complex cyber security training such as the series of trainings called 'Cyberstorm' which are regularly held in the United States and in some countries of the EU (United Kingdom and Estonia). The aim of such training is to work together with all actors (mainly state ones) which are involved in providing cyber security on solving some potential cyber threats. The existence of such trainings show the attitude and importance of cyber security topic in the country and serve as a great opportunity to enhance coordination and cooperation of state organs which is a prerequisite for achieving cyber resilience (Homeland Security, 2017).

### c) Conclusion

Efficient cooperation and coordination at a state level is one of the four main criterion which contributes to achieving cyber resilience on a national level according to this research (Pernik, 2015; Rhinaud, Sundelius, 2014; Yost, 2003). Having looked at

political and governmental system involved in providing cyber security in Ukraine the following conclusions are made:

1. Even though Ukraine adopted a Strategy on cyber security in 2016 as a compromise between proponents and opponents of the Law it does not stipulate responsibility and law enforcement in case of violations of its provisions. Furthermore, it does not touch upon the necessity to update or change CSIP, does not clearly differentiates some of the agencies' functions; does not focus enough on regulating coordination between cyber security organs.
2. Some organs involved in cyber security are not duplicating each other or have the potential to duplicate their work. The responsibilities of State Security Service and National Police are not clearly divided towards dealing with botnets and large-scale cyber crimes. Same applies to functions of State Security Service and State Service of Special Communication and Information Protection towards licensing of secure transportation protocols AS1, AS2 and AS3. SSSCIP has a complex structure being both international and national organ at the same time. While being tasked by so many responsibilities IT specialists working there are paid very low salaries comparing to average IT salaries on the job market.
3. Complex system of information protection(CSIP) which is approved to set standards on information and cyber security within state organs and objects of critical infrastructure is outdated and often is regarded as a 'burden' for some of the state organs which opt to pay the fine for not implementing CSIP.
4. Ukraine has never held, nor is planning to hold, complex cyber security training which would involve all stakeholders of national cyber security (state, businesses, civil society) to enhance cooperation and coordination between them. Similar training proved their usefulness in the majority of countries which focus upon achieving cyber resilience (for example in the UK, Estonia, US).

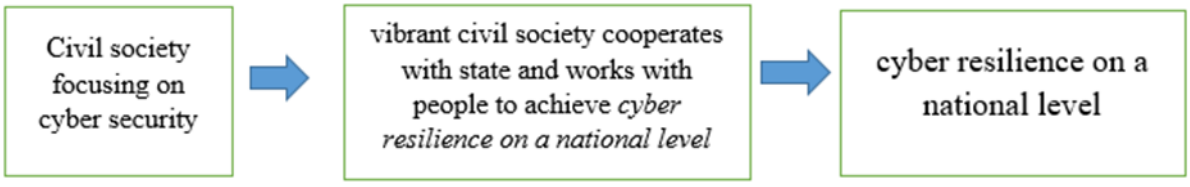
Therefore, the first causal mechanism, can be proven only partially since the efficiency of their interaction is impeded by the absence of legislation. Fundamentally, there is an absence of a law relating to cyber security which would offer the provision of law enforcement and responsibility in case of violation of the law. Efficiency is further

impended by the duplication of tasks between some organs of state, in this instance the State Security Service and National Police, State Security Service and SSSCIP; the fact that Complex System of Information Protection (CSIP) is outdated, thereby does not fulfil its functions; an absence of indicators on state's cyber security; inefficiency of work SSCIP caused by law salaries paid to IT specialists and complexity of SSCIP structure; and an absence of complex cyber security training involving all stakeholders.

## 7. Civil society and strong communities

### a) Observation phase

Although traditionally main responsibility for providing cyber security of the country is played by the state, such non-state actors as NGOs can not only assist state in providing valuable expertise but also by raising awareness of society about existing cyber threats and responsible use of internet. In order to trace the process of the work of civil society in cyber security which contributes to cyber resilience on a national level the following causal mechanism is developed:




Where *civil society focusing on cyber security* is independent variable; *vibrant civil society cooperates with state and works with people to achieve cyber resilience on a national level* is an element which has to proved by such factors as the work of civil

society organizations and the challenges they face. The independent variable of this causal mechanism is *cyber resilience on a national level.*

## b) The analyses of the element's factors

The work of non-governmental organizations, movements and associations is an indicator of the level of development of civil society (Tvedt, 2002). Civil society appeared in Ukraine only after proclaiming its independence in 1991 since within Soviet Union free and independent NGOs were either prohibited or worked under cover. It may take decades for a country in order to develop a vibrant and influential civil society therefore, Ukrainian civil society may considered to be young and not experienced comparing to some other European countries (Ghosh, 2014).

In order to explore the level of development of Ukrainian civil society three categories of NGOs, movements and associations as well as volunteer and grass-root movements will be researched:

1. NGOs and think-tanks supported by a state
2. Volunteer and grass-root movements or organizations
3. NGOs and projects supported by international partners

Even though there are many ways of categorizing NGOs, the categories of this research are divided in accordance with the funding and support these organizations receive or not receive which influences the scale of their involvement in cyber security issues in Ukraine. Civil society organizations are also categorized according to their area of work to think tanks (involved in analytical work), non-governmental organizations with a clear structure and state registration, volunteer and grass-root movements.

Even though there are 22,237 non-governmental organizations registered in Ukraine, only 88 of them are working on different aspects of security (Ukrstat, 2016; Informjust, 2017). The component of cyber security has been established in many organizations mainly starting from year 2014 when the biggest cyber attacks against Ukraine took place. There

is also a large number of non-registered grass-root movements and organizations. For the purpose of this research, only the biggest and most influential think tanks, NGOs and grass-root movements were interviewed in order to measure the role of civil society in providing cyber resilience according to the criteria stipulated within the chapter on methodology (p. 10).

*NGOs and think-tanks supported by a state*

There is a number of think tanks which have a status of a State science and research institution on a national level as well as on a level of specific government bodies. 'National institute of strategic studies' is an institution which works on a national level regarding different issues related to information and cyber security. Even though the institute is state funded, it often receives grants and funds for its research projects from other NGOs and foundations. Specifically, this NGO initiated the development of Cyber security strategy of Ukraine in 2005. Researchers of the institute developed its draft text which was later on agreed by all state stakeholders – state bodies, businesses, NGOs. Think-tanks supported by the state are often providing the draft texts of regulations, reports and statements on specific issues. National institute of strategic studies has been working on cyber security since early 2000 to fill the gap in national legislation towards this issue. Challenges related to the work such think tanks are often related to fewer opportunities to be independent and advocate its position with the help of media and other sources. At the same time, the access to government which such think-tanks have allows them to directly influence decision-making. Funding is also an important challenge since its main source comes from the budget which is usually small, however, institute fellows often get extra funding from different donors on specific projects.

The All-Ukrainian Association on information security and information technologies was created in 2010 as an initiative for experts who are dealing with information and cyber security in order to protect the social, economic and other common interests of people and organizations which strive for development of the level of information and cyber security in Ukraine. The main tasks of the organization include cooperation with the government and local administrations as well as other non-state organizations in order to

enhance coordination and partnership between them; contribution to the development of information security and cyber security policy of Ukraine and the popularization of Ukrainian cyber security tools and software. With these aims, the association regularly conducts research and produces publications on pressing issues on information and cyber security in Ukraine in order to influence decision-making at a state level and inform public on how to ensure personal cyber security. In order to enhance cooperation between all the stakeholders of cyber security, the association holds an international forum on the protection of personal data and electronic signature. The fora is visited annually by around 200 participants representing both state and non-state actors working on information and cyber security in Ukraine (Oleksiuk, 2017). Apart from preparing researches and policy papers, the aforementioned forum is the most important area of work of the association since they give space for networking between government and civil society (Oleksiuk, 2017).

When conducting their work, the head of the Association, Lilia Oleksiuk, identified several main challenges regarding the work of NGOs and other organizations which belong to the association (around 36 currently). One of the main challenges is the constant change of political power and legislation in the areas of information and cyber security as well as terms of work for non-governmental organizations. According to the recent change in law on non-governmental, voluntary organizations and associations only physical persons are able to be members of associations (Oleksiuk, 2017). Since some members of association belong are profit organizations or businesses they will have to terminate their membership in the association which will hinder its work (Oleksiuk, 2017). Another challenging issue of the work of Association is the desire of every member to take leadership and act as a coordinator rather than contribute to ongoing projects on information and cyber security which significantly affects productivity of the Association (Oleksiuk, 2017).

Cyber Warta is another organization which existed as an independent grass-root movement in Lviv for around 2 years until becoming one of Regional Administration's projects (Chayka;2017). The aim of the organization is to raise awareness of children on security in the internet. Members of the organizations were providing lectures and

trainings for children of different ages. Since the organization began to grow fast and many schools asked for such trainings the organizations decided to elaborate a booklet and established a non-mandatory lesson at schools. For this purpose, Cyber Warta turned to Regional Administration to receive the support (Chayka, 2017). While 'Lviv Regional Administration is quite flexible and open to volunteer initiatives, colleagues of Cyber Warta in other cities could not get access to regional administrations and receive support' (Chayka, 2017).

*Think tanks, volunteer and grass-root movements or organizations*

The specific of this category of civil society organizations lies in a higher level of independence and reliance on volunteers and independent contributors. Also, these organizations are often limited in terms of financial and human resources allocated for projects.

People, working in such organizations are passionate and active towards their initiatives but they can invest a limited time to their initiatives since this not their source of income. (Foweraker, 2001).

One of the most active NGOs which are specifically working within cyber security domain is Ukrainian Information Security Group. Members of this NGOs are working on advocating civil society's vision to the government through Civic Councils and annually organize the biggest Cyber Secure Conference in Ukraine – UISGCON (Ukrainian Information Security Conference). Due to the low level of trust to civil society and absence of will to cooperate members of the Council who are representing the state are constantly failing to show up to regular meetings. (Styran, 2017). This makes the work of the NGO in the area of advocacy inefficient.

Another organization which is an active member of Ukrainian civil society involved in cyber security is the Center for Army, Convertion and Disarmament studies. The center is mainly involved in analytical work. Therefore, it belongs in the category of think tanks. Even though the center focuses on different issues regarding security and defence of Ukraine, the cyber security area of research became one of the central since 2014. The main aim of the cyber security component within think tank is to build a bridge between

technical experts on cyber security and policy makers (Radkevych, 2017). This is also the biggest challenge of the think tank where experts of mainly technical background are working. The center also strongly advocates toward better informing of society about cyber risks and secure use of cyber space though press-briefings, public events and thematic conferences. Due to the limited resources allocated to the cyber component the responsibility for informing and training society on how to use internet in a secure manner should be put on a state and businesses for which the consequences of cyber crimes and attacks are the most serious (Radkevych, 2017).

There is also a number of think tanks in Ukraine focusing on issues in political science however majority of them are very small and range of questions they cover is too broad. This leads to relatively low quality of research they produce. Furthermore, their researches are in most cases not taken into account by decision makers which also proves that they did not manage to build bridges with governmental bodies or other stakeholders.

The biggest grass-root movement involved in providing cyber security in Ukraine is 'Ukrainian Cyber Forces'. Although the main goal of the organization is to actively fight with separatist forces in the east of Ukraine using offensive cyber measures, Ukrainian Cyber Forces dedicate a large part of their efforts towards cyber resilience of Ukrainian society. During Euromaidan, annexation of Crimea and after the beginning of conflict in the East there were dozens of volunteers contributing to the efforts of the organization. However, in 2016 only 3 members of the organization remained active. This trend relates to all volunteer and grass-root movements on cyber security in Ukraine, which reported the decrease of number of volunteers within their organizations (Dokunin, 2017; Interviewee 2; 2017). In three years of their work Ukrainian Cyber Forces blocked 19 millions of US dollars on 455 accounts of separatists, closed 147 separatists' websites, hacked separatist's 1,2 terabite of separatist's data from emails, social media accounts. (Dokunin, 2017). In the area of cyber security, Ukrainian Cyber Forces are working on raising awareness of society on cyber protection. For this purpose, a website Websecurity.com.ua as well as the Facebook page, Cyber Security Forces (3,648 followers) was established. The biggest challenge which Ukraine Cyber Forces are facing is improving cooperation with the government. There were a number of statements and

reports submitted to the State Security Service, CERT-UA, as well other state bodies the cyber security of which had to be improved (Dokunin; 2017). Furthermore, there were a number of state websites 'taken' or blocked by separatists or Russians as of 2014. According to Dokunin, only after 3 years and a number of appeals by Ukrainian Cyber Forces and other volunteer movements State Security Service began to block and investigate them. The cooperation between government and Cyber Forces is undermined by the low level of trust between them. Cyber Forces have never made an attempt to establish cooperation with government bodies while government bodies never took organization's recommendations seriously enough (Dokunin; 2017).

Another grass-root movement Cyber Shield is actively working within social media websites such as Facebook and, till May 2017, Vkontakte. Their Facebook pages – Cyber Shield of Ukraine, Cyber Ukrop, FalconsFlame, Trinity and Pyx8 belong to the Ukrainian Facebook pages with the biggest followers reach holding 29th and 30th place retrospectively (top 30; 2017). Among other goals such as combatting with Cyber Berkut and Russian trolls on social media, the movement is engaged in raising awareness of basic cyber security measures among Ukrainian citizens. Their information toolkit 'Recommendations on cyber security' has been published not only on social media among followers but also on wider Ukrainian media outlets such as 1plus1, Pravda.UA and Radio Free Europe. (Interviewee 2; 2017). In contrast to Ukrainian Cyber Forces which are trying to influence decision-making of Ukrainian government, Cyber Shield works anonymously using media to increase cyber resilience of Ukrainian society. The challenges which the organization is facing is the decrease in volunteerism among IT and cyber security specialists and a large number of Russian-backed and separatists' trolls on social media who are trying to undermine their work.

*NGOs, think tanks and projects supported by international partners*

There are quite a few influential NGOs which are funded primarily by donors and international organizations. Due to better funding, the structure and scope of work of these organizations are more clear and wider. The biggest donor of Ukrainian NGOs involved in cyber security in Ukraine are the United States, Great Britain, Italy. European countries which are interested in sharing their experience and provide assistance in

Ukraine are also Estonia and Czech Republic – countries which as Ukraine belong to post-soviet and post-communist spaces.

ISACA, Kyiv Chapter is the biggest international NGO on cyber security in Ukraine. Due to its wide international scope and well-established partnerships in 180 countries, ISACA is the most active NGO (Rybalchenko, 2017) which facilitates the exchange of experience between Ukrainian and international partners; provides certification of IT specialists of both state and commercial institutions; prepares policy papers and researches regarding cyber security issues in Ukraine; raises awareness on secure use of internet for citizens of Ukraine. Furthermore, ISACA is involved in enhancing the level of education on cyber security in Ukraine. Since the level of cyber security expertise in Ukrainian Universities is quite low (Malchenyuk, 2017) ISACA initiated the 'Academic Advocate Program' which boosts the knowledge of skills of Ukrainian professors and teachers. The main challenge the organization faces in Ukraine is related to cooperation with the Ukrainian government. Instead of reforming the management system of Ukrainian bodies responsible for cyber security government turn to 'fast decisions' related to mainly changing technical parameters of cyber protection when the attack occurs (Yankovskyi, 2017). There is also a low level of trust between the government and the organization. Hence, changing the governmental approach to cyber security, which is a key to cyber resilience, is ISACA's most important area of work (Rybalchenko;2017).

The ISC project of USAID in Ukraine is another initiative with foreign funding focusing on increasing Ukrainian cyber resilience, which focuses specifically on improving NGOs, media's and human rights activists' capabilities to counter cyber risks. The project was established in the end of 2013 after the government's efforts to steal private data and undermine the work of media and independent NGOs (Kostynyan; 2017). Since that time around 40 organizations received support from ISC project as well as thousands of people who were attending digital security trainings on the protection of social media, emails and other communication tools, technical protection, internet protection. The main goal of the organization is to make the beneficiaries more prone to cyber risks and sustainable in cyber security domain (Kostynyan; 2017). The project is of 'pure civil society character', which does not stipulate any cooperation with government or businesses

which makes it flexible and efficient. At the same time, the project is not being communicated well -there are only few mentioning about it in media and there is no application form though which any NGO which have cyber risks may apply. Furthermore, the majority of trainings are provided in the capital of the country which may lead to unequal geographical distribution.

### c) Conclusion

In order to achieve cyber resilience on a national level vibrant civil society working on cyber security should cooperate with state and works with people to achieve cyber resilience. Therefore, having looked at the biggest NGOs, think tanks and grass-root movements which form Ukrainian civil society working in the field of cyber security the following challenges were identified:

1. The number of non-governmental organizations on cyber security is very low. Comparing to NGOs working in other fields cyber security NGOs or NGOs which have a cyber security component in its work constitute less than 1% percent of overall number.
2. The efficiency of those civil society organizations working on cyber security is hindered by the scarcity of financial and human resources, especially in the case of voluntary and grass-roots movements, independent think tanks and state-backed research institutes which are mainly financed from the state budget;
3. A decrease of volunteerism in the country caused by ‘tiresome’ from active volunteering during Euromaidan and the war in the East of Ukraine.
4. A large number of cyber trolls sponsored by Russians and separatists which undermine the activities of Ukrainian hacktivists such as Ukrainian Cyber Forces and Cyber Shield.
5. Constant change within political power and legislation affecting the areas of information and cyber security as well as terms of work for non-governmental organizations.
6. Ambitions of members of NGOs to take leadership positions rather than contribute to ongoing projects within their status.
7. Absence of trust between the government and civil society.

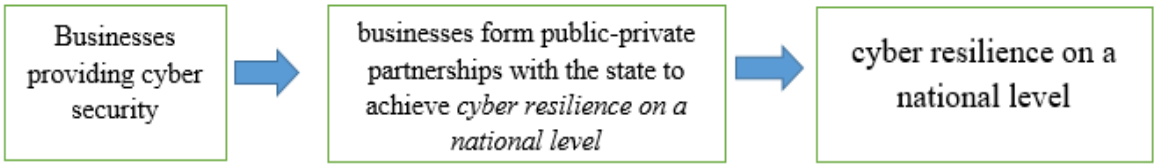
8. Inefficiency of the work of state bodies which result in slow decision-making and response to recommendations or appeals of civil society organizations.
9. The concentration of the work of civil society organization in the capital of the country which means that citizens on the local level may stay less aware on cyber security

Thus, due to the abovementioned challenges, the Ukrainian civil society working on cyber security cannot be called vibrant. Efficient cooperation with the state exists only between state-backed research institutes. Other NGOs, think tanks and movements have either failed to establish such cooperation or never tried to start it or are cooperating with state bodies. Organizations which adopt such a position experience an absence of trust between civil society and the state and slow reaction times to their proposals. Work with people aimed at raising awareness on what how to stay secure in cyber space is more vibrant. For this purpose, civil society is using such communication channels as traditional and social media as well organize lectures and trainings on cyber security for different age groups. However, the scope of their work is limited by the lack of resources both human and financial as well as often unequal geographical distribution when the majority of activities are being conducted in country's capital.

## 8. Public-public partnerships

### a) Observation phase

Another criterion of achieving cyber resilience on national level is related to active involvement of businesses into national cyber security in the form of private-public partnerships. In order to trace the process of public-private partnerships development in Ukraine the following causal mechanism is used:




Where *business providing cyber security* is an independent variable; *businesses form public-private partnerships with the state to achieve cyber resilience on a national level* is an element which has to be proved by looking at factors which either contribute to or challenge the existence of public-private partnerships in Ukraine. *Cyber resilience on a national level* serves as dependent variable as well.

## b) The analysis of the element's factors

*A Strategy on Cyber Security* mentions about the important role of cooperation with business sector in the sphere of cyber security. However, it does not go into details and explanations of possible forms of involvement of businesses, sharing of information and achieving mutual trust between the state and business. Since the Strategy does not mention the private-public partnership form of cooperation such instrument is not regulated even on the level of a legally non-binding document such as a strategy.

However, a draft law on *Cyber Security* adopted in the first reading by Verhovna Rada of Ukraine attempts to define such cooperation. The law is widely criticized by representatives of businesses for not being involved in the elaboration of the law (Zhora, 2017). Furthermore, the new law apart from the concept of *information* introduces the concept of technical information which relates only to system administration and other content related to cyber security. Technical information of a respective company thus is subject of control by a state in case of cyber risk or actual attack related to national security. However, some representatives of business claimed that such division is very disputable since government by claiming the need to check technical information may use also other data of a company in its own purposes (Dubov, 2017). Furthermore, according to the draft law, Cabinet of Ministers of Ukraine will have to adopt a decree which will provide the list of critical infrastructures of Ukraine. Majority of possible critical infrastructure objects which will be confirmed in the decree are owned by private sector at least on the 50-50 basis. Critical infrastructure objects according to the draft law will have to be CSIP licensed by State Service of Special Communication and Information. Incorporation of licensing on a mandatory basis is viewed by some business representatives as a possible way to put pressure on private sector and reduce their freedoms (Dubov;2017).

Therefore, on a policy level there are many issues which are hindering the facilitation of cooperation between state and businesses. Due to a number of disputes between state bodies and businesses regarding introduction of technical information concept, CSIP

licensing and poor communication and consultation processes the law which among others is aimed to introduce private-public partnerships in cyber security has not been adopted. Poor communication with businesses and other stakeholders is caused by reluctance to involve in consultations with large number of interested parties which may take additional time and resources (Dubov; 2017). This proves that the state is not ready to facilitate cooperation with businesses on a policy level.

From operational perspective, the state has a need to attract expertise and funding from private sector. For example, there is a necessity to establish additional CERTs in Ukraine to be able to protect critical infrastructure and state bodies from cyber attacks. Just to compare how limited Ukrainian potential is: Germany possess 33 CERTs, Poland – 26 in different areas both private and public. 'There will be no additional resources allocated to opening regional CERTs and CERTs of critical infrastructure' (Zolotukhin, 2017). Since majority of Ukrainian critical infrastructure belongs to business the state cannot be responsible for providing its cyber security – state's role can solely lie in monitoring of cyber security, sharing of information and best practices (Cys-CERT representative; 2017). There are many international experts involved in drafting the strategy of work of private CERTs in Ukraine as well as capacity building, however, Ukrainian private sector is expected to run such CERTs (Zolotukhin, 2017). Ministry of energy of Ukraine is currently looking for partners as well international ones to establish a CERT which would tackle cyber threats targeted at electric grids. There are also two CERTs being established by the Ministry of Defense and State Security Service, however, the funding still remains the issue and both bodies are holding negotiations with private companies to attract extra funds (Radkevych, 2017).

Another issue is related to CERT-UA capacities and funding. The main issue which influences the efficiency of work of CERT-UA is the low amount of salary paid to IT specialists working there. For example, the average salary of an IT specialist in Ukraine was 2,500 USD (Shymkiv, 2016) while the salary of a civil servant on the level of specialist was 3618 UAH (Cabinet of Minister's regulation 292, 2016). Good IT specialists can easily find a well-paid job in the private sector therefore, state service is chosen either by true patriots or low-qualified specialists. According to Radkevych,

students who are studying cyber security after or during graduation work for state bodies such as CERT-UA, however after one or two years take jobs in private sector. (Radkevych, 2017). Therefore, if looking at Ukraine's capabilities in preventing and fighting cyber threats the issue of human resources should be solved first of all because in the end these are cyber security specialists who are tackling cyber risks. For this purpose, the government is looking to additional funding or form of partnership with business to solve this issue.

Despite all the challenges, according to former officer of CERT-UA, this body managed to build trustworthy relations with internet providers both local and national which is crucial for fast and efficient reaction to cyber attacks (Cys-CERT, 2017). However, such relations were build according to personal connections and trust rather than private-public partnerships. Therefore, such cooperation exists de-facto according to the specific needs but is not systematic and institutionalized (Cys-CERT representative, 2017).

If looking at the issue from business point of view, the number of Ukrainian cyber security businesses working on Ukrainian market is not high comparing to other European states. Majority of cyber security companies are working with international clients mainly from Europe and the US. However, even though there is a need of the state to more fruitfully cooperate with business especially on the operational level as many experts mention (Dubov; 2017; Zhora;2017; Zolotukhin; 2017, Malchenyuk; 2017), the businesses which are working in Ukraine are not cooperating with the state to a large extent due to such reasons as: inefficient work of state bodies, low level of trust, fear of losing independence, reputation risks, and skepticism about state's role in cyber security, low or no funding a state can pay for their services.

As for inefficient work of state bodies, the head of Berezha Security company, Vlad Styran, mentions: "We are trying as much as we can to avoid cooperation with the state due to complicated procedures of establishing and conducting such cooperation" (Styran; 2017). In the event of a cyber crime or cyber attack the period of time needed to file a request and receive a feedback for example from Cyber Police may take up to a year (Styran; 2017). "When a cyber security company files a request to the state law-enforcement agencies about investigation the procedure is very tedious and long" (Cys-

CERT representative, 2017). Since cyber crimes are occurring rapidly, this leaves a state very little time to react and investigate the crime. However, this issue does not relate only to the work of Ukrainian state bodies – bureaucratic and complicated system of state procedures cannot efficiently cope with extremely rapid and sophisticated cyber crimes or attacks happening everywhere in the world (Geers, 2017).

This leads to another issue related to general skepticism of businesses about the role of the state in providing cyber security. A cyber security expert Serhiy Radkevych claims that 'the state should play primary role in providing cyber security of the country – its functions should only be regulatory and legislative ones' (Radkevych, 2017). When the state 'interferes with its recommendations it only worsens the situation' since it does not have good expertise and capacities in cyber security (Styran, 2017). Furthermore, it took 8 years for the country to adopt only the Strategy on cyber security and 'neither representative of businesses was consulted about the laws which are currently under consideration of Parliament' (Zhora, 2017). The fact that the state does not have good expertise on cyber security and is not willing to consult with businesses raises the question of its capacities to provide cyber security.

Another reason which prevents businesses to actively cooperate with the state in the form of private-public partnerships is the financial one. 'When announcing tenders or calling for partners the state is searching first of all for the cheapest service on the market, regardless of its quality' (Styran, 2017). This fact demonstrates how 'important' cyber security for the country is. 'State bodies operating in the field of cyber security do not have capabilities and expertise to provide quality control of the services provided so the only criteria when selecting a contractor is the low price' (Styran, 2017).

Businesses tend not to trust the state much in their work. 'This country is very corrupt and not predictable, issues related to cyber security are covered by secrecy and confidentiality' (Rybalchenko, 2017). If making a request to state bodies on any issue the answer you receive is usually either general and not even related to the request (Dubov, 2017). Such attitude to providing public information ruins the possibility to establish trust between businesses and state. As mentioned before in chapter 4, the intention of a state to introduce the concept 'technical information' which would allow State Security Service

to conduct перевірки of businesses as stipulated in the draft law On Cyber security makes businesses worried about confidentiality of its data and possibility of the state to spy on them (Dubov, 2017). Same applies to possible cyber crimes conducted against cyber security businesses' clients. Some cyber security companies choose to conduct investigations by themselves rather than turn to Cyber Police which may get access to their data which then can be used against them (Styran, 2017). Some companies are also hesitant to share information with the government (Jagasia, 2017). 'Since the government would not be able to provide all data regarding potential cyber crimes because some information may be classified or confidential, many companies feel that the information sharing would end up as a one-way relationship' (Jagasia, 2017: 3). Cys-CERT, one of the biggest cyber security companies in Ukraine is constantly informing state bodies and law-enforcement agencies about cyber risks. However, state agencies have never reacted to such 'good-will' actions of the company. Furthermore, in few cases 'law-enforcement agencies suspected cyber security companies in cyber crimes or attacks since they shared with them some 'suspicious' data' (Cys-CER, 2017).

Reputational risks are another reason for why not businesses are not willing to establish public-private partnerships. Over the last 3 years Ukraine has become a target of large scale cyber attacks, Failure to cope with cyber attacks in case of existence of public-private partnership between a state and businesses may have a negative influence on reputation of businesses (Deloitee, Risk Management, 2017) Therefore, some businesses decide not to risk its reputation which is critical for their purposes. Moreover, in some cases the involvement of the state bodies leads to escalation of the attack or crime which in Ukrainian case are often targeted at undermining the reputation of a state (Nesterenko, 2017).

Though there is large number of reasons which prevent businesses as well as a state to establish private-public partnerships there are few successful initiatives coming both from a state and business. One of the most successful examples of concrete cooperation between cyber security business and the state took place over tackling the consequences of a cyber attack targeted against an electric grid in Ivano-Frankivsk and Kyiv. Cyber

security company ESET provided its expertise and software tools immediately after the attack took place (Zolotukhin, 2017).

After the biggest cyber attack targeted at Ukraine in 2017 by notPetia virus Trade and Industry Chamber of Ukraine which is aimed at supporting Ukrainian and foreign business in Ukraine has established Anti crises Center of cyber protection which consists of both state bodies and businesses. The companies with one of the greatest expertise on the Ukrainian market – Privatbank, IT Laboratory, Axon Partners and other 27 companies and experts to support businesses affected by the virus with their expertise and software tools completely voluntarily. From the other hand, cyber security state bodies which belong to the Center – Cyber Police, SSCIP, State Security Service.

National Bank of Ukraine established a Cyber Protection Center (CSIRT-NBU) in order to immediately react to cyber threats and share information between banks and police. The aim of the Center is also to elaborate efficient plans on how to tackle cyber threats. The way National Bank cooperates with business is considered to be the most efficient if comparing to other state bodies by many experts. Due to immediate information sharing as well comparatively big investments in cyber security, banking sector is considered to be the most protected from cyber security point of view.

Neither of the mentioned cooperation projects were registered or established in the form of private-public partnerships. Thus, while there are sporadic initiatives of both businesses and the state in cyber security such relations have never aimed at long-lasting cooperation from both sides due to the reasons mentioned above.

### c) Conclusion

Cooperation between business and state remains on the low level in the sphere of cyber security. A private-public partnership form of relations between businesses and government in cyber sphere is not stipulated de-jure even though there were intentions to introduce a provision on private-public partnerships within the draft law on Cyber Security.

From the state's point of view there is the interest in developing cooperation with business on the operational level mainly when it comes to attracting additional financial resources due to limited budget allocated to cyber security. There are many examples when state bodies and agencies have called businesses with specific propositions of cooperation, which were seen by many companies as unequal or not relevant (Styran, 2017). On strategic level from the other hand, state bodies do not involve businesses in decision-making process, leaving majority of them behind policy elaborations. This may be explained by low trust of state to businesses; unwillingness to share power with other stakeholders; fear of protracted negotiations due to a large number of interested parties (Dubov, 2017). To sum up, such attitude of state towards private sector does not stimulate the establishment of fruitful cooperation among others in the form of private-public partnerships.

From business point of view there is little interest in establishing private-public partnerships with a state. The following reasons which are hindering business' involvement in cyber security on a national level were identified:

1. Inefficiency of work of state bodies caused by complicated and time-consuming procedures of information sharing and other services
2. Low budget allocated to cyber security which leads to the search for the cheapest services rather than the ones of the best quality.
3. Low trust of businesses to state bodies which have a reputation of being corrupt and not open. Fear that sharing of information with a state would end up in a one-way process.
4. General skepticism about the state's capacity to provide cyber security due to little investments in this sphere and lack of expertise
5. Possible reputational risks in the event of success of a cyber attack targeted at the state.

Thus, in order to achieve cyber resilience on a national level among others, there should be an efficient cooperation between businesses and the state in the form of private-public partnerships. Having interviewed representatives of the biggest cyber security businesses as well as former and current civil servants engaged in providing cyber security on the

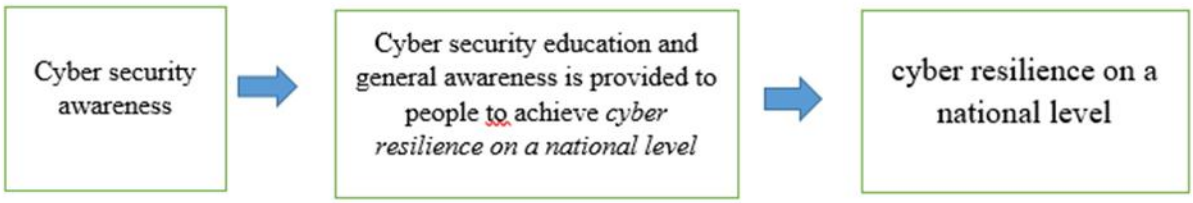
existence of such cooperation it has been proved that the sporadic events of private-public cooperation on cyber security cannot in fact be called private-public partnership. There are many reasons which prevent such cooperation and they do not seem to be solved in the nearest future.

# 9. Societal resilience

## a) Observation phase

The last criterion of achieving cyber resilience on a national level is ensuring quality information on cyber security education at schools, Universities and within society. In the end, it is a human who is responsible for security breaches (Radkevych, 2017). Therefore, 'comprehensive, effective end user awareness training and education is recognized as the single most effective component in the prevention of data loss or a security breach' (Lohrmann, 2012:7).

In order to trace the process of achieving societal resilience the following causal mechanism is developed:




Where *cyber security awareness* is an independent variable; *cyber security education and general awareness is provided to people to achieve cyber resilience on a national level* is an element which will be proved by looking at the factors such as IT and cyber security education in public and private schools, higher education in cyber security and general cyber security awareness. The dependent variable is *cyber resilience on a national level.*

## b) The analysis of the element's factors

*IT and cyber security education in public and private schools*

Very little attention is given to information and cyber security in Ukrainian public schools. Such issues as personal data protection, security of passwords and cyber bullying are important to be addressed from the early age (Brady, 2010). According to the latest educational program adopted by the Ministry of Education, only one class of the subject, 'Internet Security' should be provided to pupils of the primary school. Furthermore, this class is not mandatory and should be held within the scope of extracurricular activities. Usually, Internet security class is held at International Day of Secure Internet which is celebrated every year on February 6. 'Since children start using internet in the very early age it is crucial to provide enough training on how to stay secure in cyber space: one hour of the internet security class is definitely not enough' (Zolotukhin, 2017). There is a clear generation gap between civil servants who work in the Ministry of education who started using internet in their middle age and children who are born in the internet era which results in 'almost no education on information security at primary schools' (Oleksiuk, 2017). After being pushed by civil society, the Ministry of education has suggested to work on introducing 8 hours of internet security classes at schools, however, according to experts this is not enough (Oleksiuk 2017; Zolotukhin, 2017). Another problem concerns the absence of internet in some regional schools in Ukraine where consequently the

classes on internet security are ignored due to the absence of the problem (Oleksiuk, 2017).

As for secondary school, pupils start learning information security within the *Informatics* class. However, even though this class runs from fifth till ninth grade information security is taught only during the last year (Ministry of education, 2017). Furthermore, the educational program does not include any notion of cyber security and its basics. In order to fill this gap a private school Computer Academy suggested a new program on Informatics which would include more hours on information and cyber security to the Ministry of education on a voluntary basis. However, 'the Ministry considered this initiative as PR project of the Computer Academy and refused to collaborate' (Oleksiuk, 2017). According to Oleksiuk, this happened in the absence of understanding by the Ukrainian government of the public-private partnership concept (Oleksiuk, 2017).

Apart from public schools, cyber security is taught at few private schools and training centers -InformSecurity, Domina Security, Academy IT, Network Academy Lanit, Computer Academy. The first two schools are considered to be leading ones since they focus specifically on cyber security issues. Another three schools are teaching cyber security among other IT programs. The audience of the private schools are usually graduate students, recent graduates or adults wishing to retrain to change their current job or get at new one. Computer Academy among others is teaching IT to a younger audience, usually pupils who want to learn this sphere more deeply. Private schools which teach cyber security are comparatively expensive, therefore, not everyone wishing to work in this field can afford them and the number of members of such schools is comparatively low (Potii, Oliynykov, 2016).

The negative consequences of the little attention given to information and cyber security in public schools and little interest to private schools are not only poor skills and knowledge in cyber security but also low interest in pursuing education and career in this field.

*Higher education on cyber security*

Even though there are degree studies in Ukrainian Universities on Information security taught at 7 Universities all over Ukraine there is a lack of cyber security experts in Ukraine who received specific education in cyber security (Potii; Oliynykov, 2016). Every year around 500 students graduate from Universities with a BA degree in information security which constitutes less than 1% of the total number of students who enter Ukrainian Universities each year (Table 3; Potii; Oliynykov, 2017). Thus, the majority of cyber security experts in Ukraine are IT specialists who have learned cyber security themselves (Malchenyuk, 2017). The reason for low popularity of information and cyber security, according to many experts lies in the rapid development of cyber threats and ways to protect from them which educational institutions can barely follow (Styran; 2017, Kostynyan; 2017, Rybalchenko 2017; Geers, 2017; Christensen, 2016). 'There is no need to have a BA degree program in Cyber Security which lasts normally 4 years – Universities will not cope with the approving of special literature which is constantly changing' (Styran, 2017). However, the same argument may be applied towards other IT degrees which are also developing very fast today but nevertheless exist in Universities. Low number of information security graduates may also be explained as mentioned above by little attention paid to this field in schools which means that pupils do not have a chance to look at the issues related to information and cyber security and consider pursuing career and education in this sector.

Up to 2017 there were no degree programs in Cyber Security in Ukraine. Cyber security courses are taught within Information Security degree programs. The idea of adding Cyber security degree programs in addition to Information Security degree programs is contested by many experts within Ukraine due to different understanding of the terms *information security* and *cyber security* which are often used interchangeably. On one hand, Information Security covers broad issues related to 'information and the protection of information whether be it physical or computerized' (Kissel, 2013). From the other hand, cyber security is focusing more specifically on 'protection of cyberspace and use of it against any sort of crime (related/not related to information)' such as, for example cyber terrorism and cyber sabotage (Kissel, 2013). Having in mind the ongoing war with the Russian Federation and the large number of cyber threats to the country, the Ministry of Education introduced a Cyber Security BA degree program which will be taught

separately from Information Security. 'Given the Russian aggression, we are in desperate need of cyber security professionals. The approval of the new standard will allow us to train high-level specialists ready to apply their knowledge in practice and respond to the current challenges' (Kovtunets, 2017). This decision was widely criticized by cyber security experts in Ukraine due to lack of understanding about who will be developing teaching plans and teaching this degree program in Universities. (Dubov, 2017; Styran, 2017; Malchenyuk, 2017; Oleksiuk, 2017). Furthermore, as mentioned above, the efficiency of the program is impeded by the fast development of cyber threats.

Some interviewees claimed that Cyber Security should be taught within Master's degree programs since they are more specific and last for only one or maximum two years (Malchenyuk, 2017; Dubov, 2017). Thus, former Microsoft cyber security expert Igor Malchenyuk initiated establishing a Master's degree program in cyber security at the Ukrainian Catholic University which is considered to be one of the most prestigious Universities in Ukraine (Malchenyuk, 2017). However, due to bureaucratic complications and the absence of official educational specialty in cyber security the program has still not been established (Malchenyuk, 2017).

Currently, there is one Master's program in cyber security which is funded by the European Commission and organized together with European Universities. The program is called *Educating the Next generation experts in Cyber Security: the new EU-recognized Master's program* (ENGENSEC) and includes among others 7 Ukrainian Universities (Lviv Politechnik University website, 2017). The program lasts 2 years and is targeted at knowledge exchange between European countries on cyber security. Due to the fact that the program is run on an international basis within Erasmus+ agreement with Ukraine there were no complications with setting up this program in Ukraine. According to Rybalchenko, this degree program on cyber security has been the most efficient in Ukraine so far, however, the number of students who were involved in it (around 30) was quite low due to the program structure and funding (Rybalchenko, 2017).

There are a few initiatives of NGOs which support Ukrainian higher education in cyber and information security. ISACA – one of the biggest international NGOs in Ukraine introduced an *ISACA Academic Advocate Program* which provides assistance to

professors who want to increase their knowledge and skills in teaching cyber and information security. (ISACA website, 2017). The program provides access to ISACA's e-library as well as methodology and research of ISACA worldwide. Members of the program receive a free subscription to ISACA Journal and participate in meetings and webinars of more than 10 000 ISACA members worldwide. Six out of eight Universities which teach information security are already a part of the ISACA program (Rybalchenko, 2017).

*General cyber security awareness*

Educating citizens to the dangers they face when conducting business online is an effective first line of defense when it comes to cyber security (Pernik, 2016). Cyber security awareness projects are extremely important in Ukraine due to the poor education on information and cyber security which people receive in primary and secondary schools. There is an expectation that such projects will fill the gap of knowledge and skills on information and cyber security of Ukrainian citizens.

There are two main ways of raising awareness of cyber security among the population and thus strengthening societal resilience – through advertisements and banners in the media and on the streets and by holding training, courses and events targeted at specific groups of the population (Radkevych, 2017). The majority of interviewed experts agree on the fact that 'the state should not be responsible for increasing societal resilience. The most important role here should be played by business and civil society organizations. The state in this context has regulatory and controlling functions.

There are only a few projects in Ukraine which are educating people though the media and advertisements on cyber and information security. Those projects mainly belong to banks which aim to raise awareness of how not to be become a victim of cyber crimes. Apart from banks, some NGOs and businesses invest in advertisements on social media about cyber security. Among them – Microsoft with the large project *Onliandia*, the aim of which is to raise awareness among children about secure use of the internet. The project is supported by a wide range of NGOs on children's rights and education all over

Ukraine (Malchenyuk, 2017). The project teaches the basic ways to protect yourself on the internet through their website, social media accounts and social billboards. Another large project is run by the NGO *Cyber Warta* and Lviv State Administration. Apart from organizing classes and trainings for children on internet security Cyber Warta advocated for social billboards on internet security for children in Lviv and Kyiv. (Chayka, 2017). The main challenge of raising awareness programs through advertisements on the streets and social media campaigns is relatively high cost which small businesses or NGOs cannot afford.

If talking about achieving societal cyber resilience through trainings and courses for targeted groups there are many initiatives of this kind held by businesses, NGOs and the state. 'Even a simple training on cyber security which may last a day or two can give enough knowledge on how not to become a victim of cyber hackers' (Radkevych, 2017). While there is a general agreement in society that such training is useful, the way they are conducted is contested by many experts. Some believe that the audience of such trainings should be divided by age and profession, while others may divide targeted audiences by their level of IT education and skills (Radkevych, 2017). Interestingly, the training which targets specific age groups or professions is usually organized by small businesses or NGOs which have an interest in training specific groups, for example, their staff. When training is targeted at people with different level of IT skills and for everyone interested in improving their knowledge of cyber security, they are organized by either large businesses such as Microsoft, Zillya, Bererzha Security or large NGOs which aim to achieve societal resilience among others (USAID, ISACA). According to experts, the state has to conduct trainings for civil servants since they usually 'possess much more sensitive data than others and they are more likely to become a victim of hackers' (Radkevych, 2017). After the recent cyber attacks in June and July 2017 the government is planning to invest more resources into cyber security trainings of civil servants. (Turchynov, 2017).

The form in which cyber security training is provided also differs and depends on many factors. The most common form of cyber security trainings is webinar. Such a form is usually cheaper, more convenient for participants and if communicated well has a

potential to reach large audiences. The disadvantages of such a form of training is the fact that people tend to be less committed to an online form of learning and are more likely to give up webinars. Therefore, the classic form of trainings when participants stay in one place for a specific period of time, communicate and work together with a trainer still exists and is actively used by ISC project of USAID, ISACA, Zillya and others.

While raising awareness on cyber security is important for increasing societal resilience to cyber threats it is complicated to evaluate their impact. Even though it is possible to calculate the number of people taking part in trainings or courses the number of people who have seen the billboards on the streets or posts on social media can be calculated only approximately. Furthermore, 'it is difficult to measure with precision what affect an awareness raising activity has on an individual' which often prevents donors from investing into such programs. (McElfroy, 2013).

### c) Conclusion

Thus, societal cyber security awareness is equally important among other criteria in order to achieve cyber resilience on a national level since human error is very often the reason for cyber crimes and cyber attacks. After looking at education on information and cyber security in schools, Universities and general awareness programs the following challenges which prevent the country from achieving societal cyber resilience were identified:

1. Not enough classes on internet security in primary schools which result in poor understanding of personal data protection, prevention of cyber bullying, viruses and fishing threats and others.
2. Little attention is given to information security within Informatics class in secondary schools which results in little interest in pursuing careers in information and cyber security
3. Absence of confidence of the government in private sector and private public partnerships

4. Low interest in private schools on cyber security which are not affordable for a significant amount of population
5. Absence of cyber security specialty within the Ukrainian higher education system on both BA and MA levels which leads to the lack of experts in cyber security in Ukraine
6. Relatively high cost of projects aimed at raising the general awareness of the population about cyber security through advertising on the streets and social media which prevents small businesses and NGOs from conducting them.
7. Difficulty in measuring the impact of raising awareness campaigns which results in low interest of donors to invest in them.

Thus, the societal resilience to cyber security threats does not exist in Ukraine which limits the cyber resilience on the national level in general. Primary and secondary education on cyber and information security does not equip people with the necessary skills and knowledge which would help them to protect themselves from cyber threats. At the same time, there are only a few projects which contribute to general awareness on cyber and information security run by businesses and NGOs, the majority of which are concentrated in few big cities. However, after the biggest cyber attacks in 2014-2017, the Ukrainian government and other stakeholders have committed to invest more resources into societal awareness on cyber security (Poroshenko, 2017; Turchynov, 2017).

# Conclusion

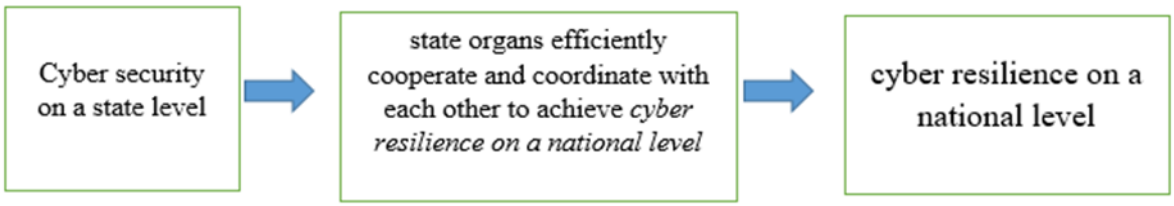
## a) The results of process tracing case study

The concept of resilience which is developed at the crossroads of physics, political science and economics has been used within the scope of this thesis to analyze the national policy of Ukraine in cyber security and identify whether Ukraine is a cyber resilient country and if not, what prevents it from becoming cyber resilient. Even though in political science scholars looked at resilience from different perspectives such as within the theory of good governance or humanitarian response all of them agree that

resilience's added value lies in explaining the advantages of active self-organization in the events of crisis and ways to reorganize to rebound from a potentially catastrophic event as well as shift from responsibilities for security to different stakeholders (NGOs, businesses). These resilience features are applied also towards cyber space where the level of unpredictability and constant change is very high (Holling, 1973). Having this in mind, cyber resilience according to this research contains such criteria (independent variables) as efficient coordination and cooperation of all actors and stakeholders (Christou, 2016; Cavelty, 2008; Hagmann and Dunn Cavelty, 2012), vibrant civil society (Wagner, 2016; Bourbeau, 2013), private-public partnerships (World Bank, 2017) and cyber security education (Nickolas, 2016) which are necessary to efficiently respond to the changing nature of cyber threats. Particularly these four criteria are the basis of the causal mechanisms which were developed within the process tracing case study of Ukraine in order to test Ukrainian policy on cyber security on its correspondence to the emerging concept of resilience and identify the main challenges to providing cyber resilience in the country.

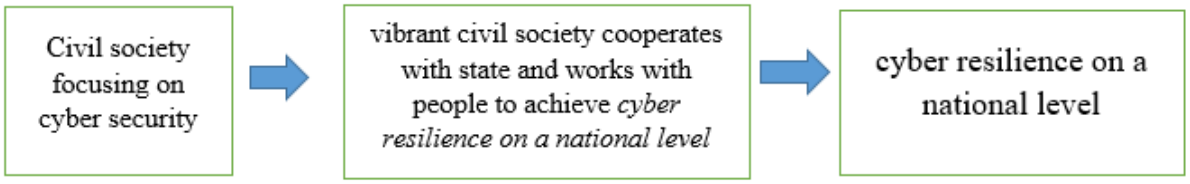
Due to the conflict in Eastern Ukraine and the ongoing process of reforming and transforming of Ukraine after Euromaidan the issues related to the national cyber security of the country are challenged by a large number of cyber threats, including cyber attacks, cyber crimes, cyberespionage and sabotage. In such conditions, the cyber resilience of the country should be set as a priority of all stakeholders which are involved in cyber security. These stakeholders are the government, private sector and civil society. According to this process tracing case study, cyber resilience exists on the national level if the four causal mechanisms which involve the above mentioned stakeholders are fully proven. The challenges and issues which prevent the existence of cyber resilience on a national level are identified in case the causal mechanisms do not exist or exist only partially.

The first causal mechanism is related to the government and reads as follows:




Due to the number of challenges to the element's factors identified in the sixth chapter such as the absence of legislation, specifically a law of cyber security which would provide law enforcement and responsibility in case of violation of the law; the events of duplication of work between some of the organs (State Security Service and National Police, State Security Service and SSSCIP); the fact that Complex System of Information Protection (CSIP) is outdated and does not fulfil its functions; the absence of indicators on state's cyber security; the inefficiency of work SSCIP caused by low salaries paid to IT specialists and complexity of SSCIP structure; the absence of complex cyber security training which involves all stakeholders the causal mechanism of this process tracing case study has been proved only partially. Another reason which impedes the efficient cooperation and coordination on the state level in the sphere of cyber security and which relates not only to Ukraine, lies in the sensitivity of this sphere and the high volume of classified information which belongs to specific agencies such as State Security Service in Ukraine (Nojeim, 2010; Radkevych, 2017).

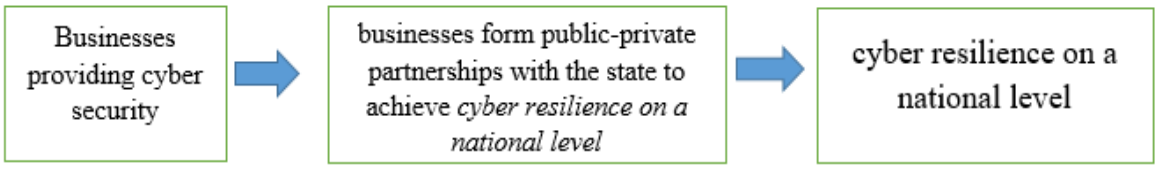
The second causal mechanism is related to civil society and reads as follows:




The analysis of the element's factors proved that due to challenges such as the low number of cyber security NGOS; the scarcity of financial and human resources, - especially in the case of voluntary and grass-roots movements, independent think tanks and state-backed research institutes; decrease of volunteerism in the country caused by 'tiresome' active volunteering during Euromaidan and the war in the East of Ukraine; a

large number of cyber trolls sponsored by Russians and separatists which undermine the activities of Ukrainian hacktivists such as Ukrainian Cyber Forces and Cyber Shield; constant change of political power and legislation in the areas of information and cyber security as well as the terms of work for non-governmental organizations; the ambitions of members of NGOs to take leadership positions rather than contribute to ongoing projects within their status; the absence of trust between the government and civil society; inefficiency of the work of state bodies which result in slow decision-making and response to recommendations or appeals of civil society organizations; and concentration of the work of civil society organization in the capital of the country, the element of the causal mechanism does not exist to the full extent.. Ukrainian civil society working on cyber security cannot be called vibrant. Efficient cooperation with the state exists only between state-backed research institutes. Other NGOs, think tanks and movements either failed to establish such cooperation or never tried to start it or are cooperating with state bodies however, experience the absence of trust to civil society and slow reaction to their proposals. Work with people aimed at raising awareness on cyber security issue seem to be fruitful, however the scope of their work is limited by the lack of resources both human and financial and other challenges mentioned above. Therefore, the causal mechanism can only be proved partially regarding some cooperation with the state and more active work with people.

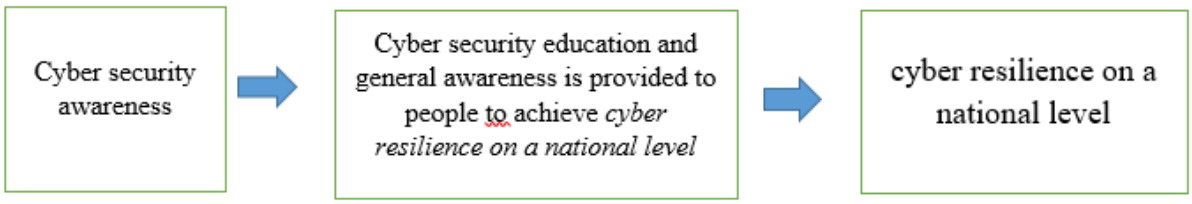
The third causal mechanism is related to businesses and reads as follows:




The analysis of the element's factors proved that cooperation between the state and businesses in the form of public-private partnerships does not exist in the cyber security sector in Ukraine on the official level. The cooperation between the state and businesses exists at the primitive level. From the state's point of view there is interest in developing cooperation with business on the operational level mainly when it comes to attracting

additional financial resources due to the limited budget allocated to cyber security. On the strategic level on the other hand, state bodies do not involve businesses in decision-making process, leaving the majority of them behind policy elaborations. From a business point of view there is little interest in establishing private-public partnerships with the state due to the inefficiency of work of state bodies caused by complicated and time-consuming procedures of information sharing and other services; a low budget allocated to cyber security which leads to the search for the cheapest services rather than the ones of the best quality; low trust of businesses to state bodies which have a reputation of being corrupt and not open; fear that sharing of information with a state would end up in a one-way process; general skepticism about the state's capacity to provide cyber security due to little investments in this sphere and lack of expertise; possible reputational risks in the event of success of a cyber attack targeted at the state. Thus, the sporadic events of cooperation between the state and businesses which in a few cases resembles the logic of private-public partnerships cannot prove the causal mechanism.

The fourth causal mechanism is not related to all the stakeholders and touches upon the issue of societal resilience:




The analysis of such element's factors as cyber security education and awareness proved the absence of societal resilience in Ukraine which limits the resilience on the national level in general. Primary and secondary education on cyber and information security does not equip people with the necessary skills and knowledge which would help them to protect themselves from cyber threats. At the same time, there are only a few projects which contribute to general awareness of cyber and information security run by businesses and NGOs, the majority of which are concentrated in few big cities. The reasons for that lies in not enough classes on internet security in primary schools; little

attention given to information security within Informatics class in the secondary schools; the absence of confidence of the government in private sector and private public partnerships; low interest in private schools on cyber security which are not affordable for a significant amount of population; an absence of cyber security specialty within Ukrainian higher education system on both BA and MA levels; relatively high costs of projects aimed at raising general awareness of the population about cyber security through advertising on the streets and social media; and difficulty in measuring the impact of raising awareness campaigns in general.

Therefore, the fact that the causal mechanisms of this process tracing case study were not proven implies that cyber resilience on a national level in Ukraine does not exist. The country thus remains prone to cyber threats at all levels due to the war in its Eastern part as well as the challenging process of reforms. The absence of efficient coordination of state bodies impedes smart decision-making on the state level regarding adopting relevant legislation and regulations, preventing and reacting to cyber threats. Little involvement of businesses in cooperation with the state leads to the lack of information sharing and expertise on both sides. Insufficient levels of development of civil society and lack of societal resilience in cyber security imply inability to protect, prevent and tackle the negative consequences of cyber crimes and attacks.

### b) Conceptual contribution of the research

Since the concept of cyber resilience is very new and not sufficiently researched there is a great potential to find out its features and test its application in many cases starting from the government and ending with the human level. Ukraine's experience with providing cyber security and resilience research within this process tracing case study also contributes to the wider conceptual understanding of cyber resilience. While the majority of researchers who look at cyber resilience stress the importance of engaging all stakeholders in preventing and tackling cyber risks (Christou, 2016; Cavelty; 2008); strengthening societal resilience and civil society (Nicholas, 2016; Hagmann and Dunn Cavelty, 2012) and achieving efficient cooperation and coordination of the state level regarding cyber security (Handmer and Dovers, 1996; Bourbeau; 2013; Pernik, 2015; Rhinaud, Sundelius, 2014), the empirical findings of the Ukrainian case proves that there

is a number of limitations to achieving all the above mentioned criteria. While some of those limitations may be considered specifically Ukrainian given its high level of corruption and lack of transparency of the government (Transparency International, 2017),the predominance of large businesses owned by oligarchs which impedes the existence of small and medium-sized businesses (Zaslavskiy, 2016), and young and comparatively weak civil society (Pekar, 2017), the following limitations are considered to be a general concern:

Firstly, the sensitivity of the cyber security sphere and the high volume of classified information which belongs to specific agencies such as State Security Service in Ukraine impedes the efficient coordination and cooperation on the state level of many countries. Security Services either prohibit or unwilling to share some sensitive data with other agencies due to possible data leaks which may threaten the overall security of the country (Nojeim, 2010; Radkevych, 2017).

Secondly, while the role of non-governmental organizations in providing cyber resilience is stressed within the majority of studies, limitations such as the lack of human and financial resources which has been proved in the case of Ukraine, is typical in other countries. Since the cyber security sphere is traditionally regarded to be the responsibility of the government, there is not much attention of experts and donors to NGOs working in this sphere. Another factor which impedes the role of civil society in providing cyber security lies in the lack of cyber security volunteers. In order to volunteer for cyber security a person has to have good IT knowledge and skills, which prevents many people who are willing to dedicate their time to providing cyber resilience from becoming cyber security volunteers. Furthermore, volunteering culture in IT and cyber security is not developed well – there are quite few opportunities even for those IT specialists who are ready to volunteer in this sphere. It is proved that people tend to volunteer more in areas such as charities, religion, medical service (Bussel; Forbes, 2002). However, at the same time the rise of volunteerism can be expected in the event of the massive cyber attack or a conflict which within cyber space which affects a large part of the society. In Ukraine, the rise of volunteerism occurred after the country became involved in the war in the East. From the other hand, if the conflict is protracted or frozen there is a risk that

volunteerism activity may go down especially if no support is given to volunteers from the government or other donors.

Thirdly, the existence of private public partnerships and overall more intense cooperation between the government and businesses is prevented by a number of reasons which relate not only to Ukrainian case. Governments are traditionally considered to be less flexible and more bureaucratic which results in complicated and time-consuming procedures of information sharing and other services. The private sector therefore, usually opts to avoid such bureaucratic state procedures. There is also quite low trust of governments by businesses and fear that sharing of information with a state would end up as a one-way process. The majority of interviewees on this research as well as some researchers (Styran, 2017; Zhora, 2017; Cys-CERT Representative, 2017; Carr, 2017; Germano, 2014; Rogers, 2016) expressed general skepticism about the state's capacity to provide cyber security due to the lack of expertise. When deciding on cooperation with the government private sector also cares about the possible reputational risks in the event of a successful cyber attack targeted at the state.

Fourthly, the fact that there is an ongoing discussion on how much society should be aware of cyber security limits the development societal resilience which has to be underlined as an integral factor needed to achieve cyber resilience on the national level (Pernik, 2016; Christou, 2016; Rhinaud, Sundelius, 2014). Even though all stakeholders to some extent are involved in educating or raising awareness on cyber security within society, their activity in this area is not prioritized in majority of cases. the interest of the stakeholders in this sphere is also relatively little also due to the difficulty in measuring the impact of raising awareness campaigns as well as education.

# Bibliography


1. Ackerman, R. (2010) Network Situational Awareness Looms Large in Cyberspace, and What to Do About It, New York, Harper Collins Publishers.
2. Abomhara, M. (2016) Security and privacy in the Internet of Things: Current status and open issues. [online] Available at: http://ieeexplore.ieee.org/abstract/document/6970594/?reload=true, [Accessed 25 Feb. 2017].
3. Anon, (2017). Cyber terrorism – global security threat. [online] Available at: https://www.researchgate.net/publication/252195165_CYBER_TERRORISM-_GLOBAL_SECURITY_THREAT [Accessed 01 Feb. 2017].
4. Apostrophe. (2017). Масштабна кібератака в Україні: хто винен і як захиститися. [online] Available at: https://apostrophe.ua/ua/article/society/2017-06-27/masshtabnaya-kiberataka-v-ukraine-kto-vinovat-i-kak-zaschititsya/13149 [Accessed 22 Aug. 2017].
5. Bachmann, S. and Gunneriusson, H. (2017). Hybrid Wars: 21st Centurys New Threats to Global Peace and Security.
6. Baker, S. and Waterman, J. (2009) In the Crossfire – Critical Infrastructure in the Age of Cyber War, A global report on the threats facing key industries, McAfee Inc., Santa Clara.
7. Belgian Defence Strategy Department (2014) Cyber Security Strategy For Defence. [online] Available at: https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf [Accessed 08 Jun. 2017].
8. Betterevaluation.org. (2017). Process Tracing. Better Evaluation. [online] Available at: http://www.betterevaluation.org/en/evaluation-options/processtracing [Accessed 22 Aug. 2017].
9. Betzt, D. and Stevens, T. (2011) Chapter One: Power and Cyberspace. Adelphi Series 51: 35–54.
10. Borchert, H. and Juhl, F. (2011) Securing Cyberspace – Building Blocks for a Public Private Cooperation Agenda, Lucerne, Sandfire AG.

11. Bourbeau, P. (2015) Resilience and International Politics: Premises, Debates, Agenda, available at: http://onlinelibrary.wiley.com/doi/10.1111/misr.12226/full

12. Bowden, M. (2011) Worm – The First Digital World War, London, Grove Press UK.

13. Brady, C. (2010) Security Awareness for Children [online]. Available at: https://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-05.pdf [Accessed 22 May. 2017].

14. Bussell, H. and Forbes, D. (2002) Understanding the volunteer market: The what, where, who and why of volunteering. International Journal of Nonprofit and Voluntary Sector Marketing, 7 (3), pp.244-257.

15. Buzan, B. and Waever, O. (1998) Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner.

16. Buryachok, V. (2016) Technological and anthropogenic impact on security of some countries. [online] Available at: file:///C:/Users/Anna%20Melenchuk/Downloads/szi_2015_4_6%20(1).pdf , [Accessed 22 May. 2017].

17. Cabinet of Minister's regulation 292 (2016) Деякі питання оплати праці державних службовців у 2016. Government currier press.

18. Carr, J. (2009), Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media.

19. Caufmann, S. NIST Community resilience program. [online] Available at: http://peer.berkeley.edu/events/annual_meeting/2016AM/wp-content/uploads/2016/02/Cauffman_PEER-Presentation_Cauffman.pdf

20. Chaikin, D. (2006) Network Investigations of cyber attacks: the limits of digital evidence. Crime, Law and Social Change, Vol. 46, No. 4-5.

21. Chang, F. (2009) Is Your Computer Secure? Science 325, 550

22. Christensen, K., Liebetrau T. (2016) Security Meets Cyberspace: The Politics of Cyber of the 21st century, McMurray, The Technolytics Institute.

23. Clarke R. and Knake R. (2010) Cyber War – The Next Threat to National Security of the United Kingdom: Threats and Responses, A Chatham House Report, The Royal Institute.

24. Clarke, R. and Knake, R. (2010) Cyber War – The Next Threat to National Security and What to Do About It, New York, Harper Collins Publishers.

25. Coleman, K. (2008) Cyber Warfare Doctrine – Addressing the most significant threat, [online] Available at: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

26. Coloradotech.edu. (2017). [online] Available at: http://www.coloradotech.edu/~/media/CTU/Files/ThoughtLeadership/cybercrime-white-paper.ashx [Accessed 21 Aug. 2017].

27. Comninos, A. (2013) A cyber security agenda for civil society: what is at stake? [online] Available at: https://www.apc.org/sites/default/files/PRINT_ISSUE_Cyberseguridad_EN_2.pdf [Accessed 01 May. 2017].

28. Cornish, P. Hughes, R. and Livingstone D. (2009) Cyberspace and the National Security. Institute of International Affairs.

29. Council of Europe (2001) Convention of Cybercrime. [online] Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed 29 Feb. 2017].

Cyberterrorism, New York, Citadel Press.

30. Dahlman O. (2011) Security and Resilience, Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, Volume 2, Vienna

31. Deloitte. (2017). Чем чреваты кибератаки | Управление рисками. [online] Available at: https://www2.deloitte.com/ru/ru/pages/risk/articles/beneath-the-surface-of-a-cyberattack.html [Accessed 22 Aug. 2017].

32. Dudgeon, I. (2009) Targeting Information Infrastructures," Chapter 4 in Australia and Cyber-warfare, Canberra Papers on Strategy and Defence No. 168, Australia National

33. Dunn-Cavelty, M (2013) A Resilient Europe for an Open, Safe and Secure Cyberspace. Occasional Papers, No.23, The Swedish Institute of International Affairs.

34. Dunnigan, J. (2002) The Next War Zone: Confronting the Global Threat of

35. Durbin, S. (2017). As Cybercrime Increases, Cyber Security Itself is No Longer Sufficient. [online] Available at: https://www.cso.com.au/blog/cso-bloggers/2016/07/13/as-cybercrime-increases-cyber-security-itself-is-no-longer-sufficient/ [Accessed 22 Aug. 2017].

36. E-International Relations, (2017). The Advantages and Limitations of Single Case Study Analysis. [online] Available at: http://www.e-ir.info/2014/07/05/the-advantages-and-limitations-of-single-case-study-analysis/ [Accessed 22 Aug. 2017].

37. ENISA guide. (2012) National Cyber Security Strategies. [online] Available at: file:///C:/Users/Anna%20Melenchuk/Downloads/ENISA%20Guidebook%20on%20National%20Cyber%20Security%20Strategies_Final%20(1).pdf [Accessed 01 Mar. 2017].

38. Eriksson, J. (2001) Cyberplagues, IT, and Security: Threat Politics in the Information Age. Journal of Contingencies and Crisis Management 9: 200–210

39. Espresso, (2017) 250 млн на кібербезпеку. РНБО створила контур для захисту від нових кібератак. [online] Espreso.tv. Available at: http://espreso.tv/news/2017/07/10/250_mln_na_kiberbezpeku_rnbo_stvoryla_kontur_zakhystu_vid_kiberatak [Accessed 10 Apr. 2017].

40. Federal Ministry of Interior (2011) Cyber Security Strategy for Germany. Available at: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, [Accessed 11 Apr. 2017].

41. Goldsmith J. and Wu T. (2006) Who Controls the Internet? Illusions of a Borderless World (Oxford: Oxford UP).

42. Grant, R. (2008) Rise of Cyber War, A Mitchell Institute Special Report, Air Force Association.

43. Guitton, C. (2011) An Analysis of the Cyber-Strategies of the US, China and Russia, Geneva, Geneva School of Diplomacy & International Relations, University Institute.

44. Gu Q. (2007) Denial of Service Attacks. Available at: https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-June-07.pdf [Accessed 09 May. 2017].

45. Habiger, E. (2010) Cyberwarfare and Cyberterrorism, White Paper, The Cyber Secure

46. Hoffman, F (2007) Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies. https://minorthesis.files.wordpress.com/2012/12/vennesson-case-study-methods.pdf [Accessed 07 May. 2017].

47. Iancu, N. and Fortuna, A (2015) Countering Hybrid Threats: Lessons Learned from Ukraine [online]. Available at: https://books.google.ee/books?id=Uwy3DAAAQBAJ&pg=PA148&lpg=PA148&dq=european+union+cyber+ukraine&source=bl&ots=5c4x_fklMK&sig=rXejyh3fqU9pqZn_2GeMhAasUac&hl=uk&sa=X&ved=0ahUKEwi5rpixtqjQAhWF1RQKHUviBpQQ6AEIMjAD#v=onepage&q=european%20union%20cyber%20ukraine&f=false [Accessed 27 May. 2017].

48. INSA, (2009) Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models, Arlington.

49. Jagasia, A. (2017) A look into public private partnerships for cyber security, [online]. Available at: https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for/for-students/blog/news.php, [Accessed 04 May. 2017].

50. Kaminski T. (2010) Escaping the Cyber State of Nature: Cyber deterrence and International Institutions, available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Kaminski%20-%20Escaping%20the%20Cyber%20State%20of%20Nature%20Cyber%20deterrence%20and%20International%20Institutions.pdf

51. Kaspersky Security Network (2017) Kaspersky Security Network statistics. Available at: https://support.kaspersky.ru/7269#block2

52. Kissel, R. (2016) Glossary of Key Information Security Terms. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [Accessed 02 Aug. 2017].

53. Klimburg, A. (2012) National Cyber Security Framework Manual. [online] Available at: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [Accessed 08 Jun. 2017].

54. Klimburg, A. and Tirmaa-Klaar, H. (2011) Cyber war and Cyber security: challenges faced by the EU and its Member States', DG for External Policies, Policy Department, European Parliament.

55. Kramer, D., Starr, S. and Larry K.Wentz, (eds) (2010) Cyber Power and National Security. Washington D.C.: National Defence UP.

56. Kurnava, M. (2017). Cyber-crime v Cyber-terrorism: What is the difference? [online] available at: https://www.linkedin.com/pulse/cyber-crime-v-cyber-terrorism-what-difference-matthew-kurnava [Accessed 12 Jan. 2017].

57. Lessig L. (1999) Code and Other Laws of Cyberspace (New York: Basic Books).

58. Liga. Business. (2017). В Украине заработал антикризисный центр киберзащиты бизнеса. [online] Available at: http://biz.liga.net/ekonomika/all/novosti/3703083-v-ukraine-zarabotal-antikrizisnyy-tsentr-kiberzashchity-biznesa.htm [Accessed 22 Aug. 2017].

59. Lillemose, J. (2015) The (Re)invention of Cyberspace. Kunstkritikk. Available at: http://www.kunstkritikk.dk/kommentar/the-reinvention-ofcyberspace/?do_not_cache=1. (Accessed 02 Apr, 2017).

60. Lohrmann, D. (2013) Cyber Training 3.0: New Solutions Addressing Escalating Security Risks. Available at: https://www.nascio.org/portals/0/awards/nominations2013/2013/2013MI10-NASCIO%20Security%20Award%202013%20Final.pdf [Accessed 01 Aug. 2017].

61. Lp.edu.ua. (2017) Магістерська навчальна програма нового покоління експертів із інформаційної безпеки, визнана ЄС (ENGENSEC). [online] Available at: http://lp.edu.ua/node/7052 [Accessed 22 May. 2017].

62. Marcem, M. (2016) A new typology of war – the hybrid war, Available at: http://www.armyacademy.ro/reviste/rev1_2016/NEAG.pdf [Accessed 06 Apr. 2017]

63. McElfroy, L. (2013) Measuring the Effectiveness of Security Awareness Programs. Available at: https://net.educause.edu/ir/library/pdf/ERB1310.pdf [Accessed 02 Aug. 2017].

64. Ministry of Foreign Affairs of the People's Republic of China. (2017). International Strategy of Cooperation on Cyberspace. [online] Available at:

https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/ [Accessed 22 Aug. 2017].

65. National Research Council, (1991) Computers at Risk: Safe Computing in the Information Age, Washington, D.C.: National Academies Press.

66. NATO (2016) NATO's support to Ukraine. [online] Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-nato-ukraine-support-ukr.pdf [Accessed 01 May. 2017].

67. Nemeth, W. (2002) Future war and Chechnya : a case for hybrid warfare, [online] Available at: http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf [Accessed 01 Apr. 2017]

68. Newmediary Inc. (2002) Stopping Attacks: The Importance of Denial of Service (DoS) Security Appliances [online]. Available at: http://www.techguide.com/html/netsec.pdf [Accessed 27 May. 2017].

69. Newmediary Inc. (2010) Security for Today's Enterprise, [online]. Available at: http://www.techguide.com/html/security.pdf [Accessed 27 May. 2017].

70. Nicholas, P. (2017). Cybersecurity and cyber-resilience – Equally important but different. [online] Microsoft Secure Blog. Available at: https://blogs.microsoft.com/microsoftsecure/2016/11/03/cybersecurity-and-cyber-resilience-equally-important-but-different/ [Accessed 22 Aug. 2017].

71. Nojeim, G. (2010) Cybersecurity and Freedom on the Internet. [online] Available at: http://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf [Accessed 16 Aug. 2017].

72. Payne, S. (2003) Developing cybersecurity and awareness programs. [online] Available at: https://www.educause.edu/ir/library/pdf/eqm0347.pdf [Accessed 09 Jan. 2017].

73. Penn, F. Wharton, D. Public Policy Initiative. (2017). A Look into Public Private Partnerships for Cybersecurity. [online] Available at: https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for/for-students/blog/news.php [Accessed 22 Aug. 2017].

74. Pernik, P. and Jermalavicius R. (2016) Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense. [online] Available at:

http://transatlanticrelations.org/wp-content/uploads/2016/12/Resilience-forward-book-pernik-jermalacivius-final.pdf [Accessed 12 Mar. 2017].

75. Pescatore, J. (2002) High-Profile Thefts Show Insiders Do the Most Damage. [online] Available at: https://www.gartner.com/doc/379171/highprofile-thefts-insiders-damage [Accessed 01 Jan. 2017].

76. Pfister U., Suter C. (1987) International Financial Relations As Part of the World-System, available at: https://www.jstor.org/stable/2600667?seq=1#page_scan_tab_contents

77. Pekar V. (2017). Civil society in Ukraine: A sled dog, not a watchdog. [online] Neweasterneurope.eu. Available at: http://neweasterneurope.eu/articles-and-commentary/2283-civil-society-in-ukraine-a-sled-dog-not-a-watchdog [Accessed 22 Aug. 2017].

78. Poroshenko P. (2016) Cyber security strategy has been adopted. Available at: http://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856 [Accessed 09 Aug. 2017].

79. Poltorak S. (2017) Ministry of defence has defined 5 main priorities of the reform. Available at: http://www.mil.gov.ua/news/2017/07/12/ministr-oboroni-ukraini-general-armii-ukraini-stepan-poltorak-viznachiv-pyat-prioritetnih-napryamiv-oboronnoi-reformi/ [Accessed 22 Aug. 2017].

80. Potii, O. and Oliynykov, R. (2016) Ukrainian educational system in the field of cybersecurity. Available at: https://procon.bg/system/files/3501_cybesecurity_education_ukraine.pdf [Accessed 16 Aug. 2017].

81. Rauchhaus R., Barany Z. (2011) Explaining NATO's Resilience: Is International Relations Theory Useful? Available at: http://dx.doi.org/10.1080/13523260.2011.590355

82. Review, N. (2017). Hybrid war – does it even exist? NATO Review. [online] Available at: http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ [Accessed 22 Aug. 2017].

83. Robinson, N., (2014) EU cyber-defence: a work in progress, European Union Institute for Security Studies.

84. Rogers, J. (2016) Private-public partnerships: a tool for enhancing cybersecurity. [online] Available at: https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/40245/ROGERS-THESIS-2016.pdf?sequence=1&isAllowed=y [Accessed 01 May. 2017].

85. RSA Security Inc. (2001) Implementing a Secure Virtual Private Network [online]. Available at: http://www.rsasecurity.com/solutions/vpn/whitepapers/ISVPN_WP_0501.pdf [Accessed 27 May. 2017].

86. Sanchawa Dh., Public policy. [online] Available at: https://www.slideshare.net/denissanchawa/public-policy-an-introduction-48206769 [Accessed 27 May. 2017].

87. Sanjev, R. (2017). Cyber Warfare. [online] Available at: http://bit.ly/2wijf08 [Accessed 22 Aug. 2017].

88. Seymour, H. (2010) The Online Threat, The New Yorker.

89. Toffler A. and Toffler H. (1995) The Politics of the Third Wave, (Kansas City, Andrews and McMeel).

90. TSN.ua. (2017). Шимків розповів про високі зарплати IT-спеціалістів. [online] Available at: https://tsn.ua/groshi/shimkiv-rozpoviv-pro-visoki-zarplati-it-specialistiv-708972.html [Accessed 22 Aug. 2017].

91. Turchynov O. (2016) Cyber Security Coordination Center must enhance country's cyber resilience. [online] Available at: http://www.rnbo.gov.ua/news/2528.html [Accessed 14 May 2017].

92. US Government Accountability Office (2010) Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. Signal Magazine

93. Vennesson, P. Case studies and process tracing: theories and practices. Available at: http://cadmus.eui.eu/handle/1814/9592, [Accessed 14 May 2017].

94. Ventre, D. (2011) Cyberwar and Information Warfare, London & Hoboken, NJ, Security. Available at: http://dpsa.dk/papers/Security%20Meets%20Cyberspace%20-%20The%20Politics%20of%20Cyber%20Security%20DRAFT.pdf [Accessed 02 Aug. 2017].

95. Veracode, H. (2017). The Rise in Global Cyberattacks Highlights the Dangers of Cyberespionage. [online] Available at: https://www.veracode.com/blog/2015/07/rise-global-cyberattacks-highlights-dangers-cyberespionage-sw [Accessed 01 Apr. 2017].

96. Wagner W. (2016) Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising? available at: http://www.tandfonline.com/doi/full/10.1080/13523260.2016.1228034

97. Walt, S. (1991) The Renaissance of Security Studies. International Studies. Quarterly 35:211–239.

98. Wiemann, G. (2006) Cyberterrorism: How Real Is the Threat. Washington DC, United States Institute of Peace.

99. World Economic Forum papers (2012) Partnering for Cyber Resilience, available at: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

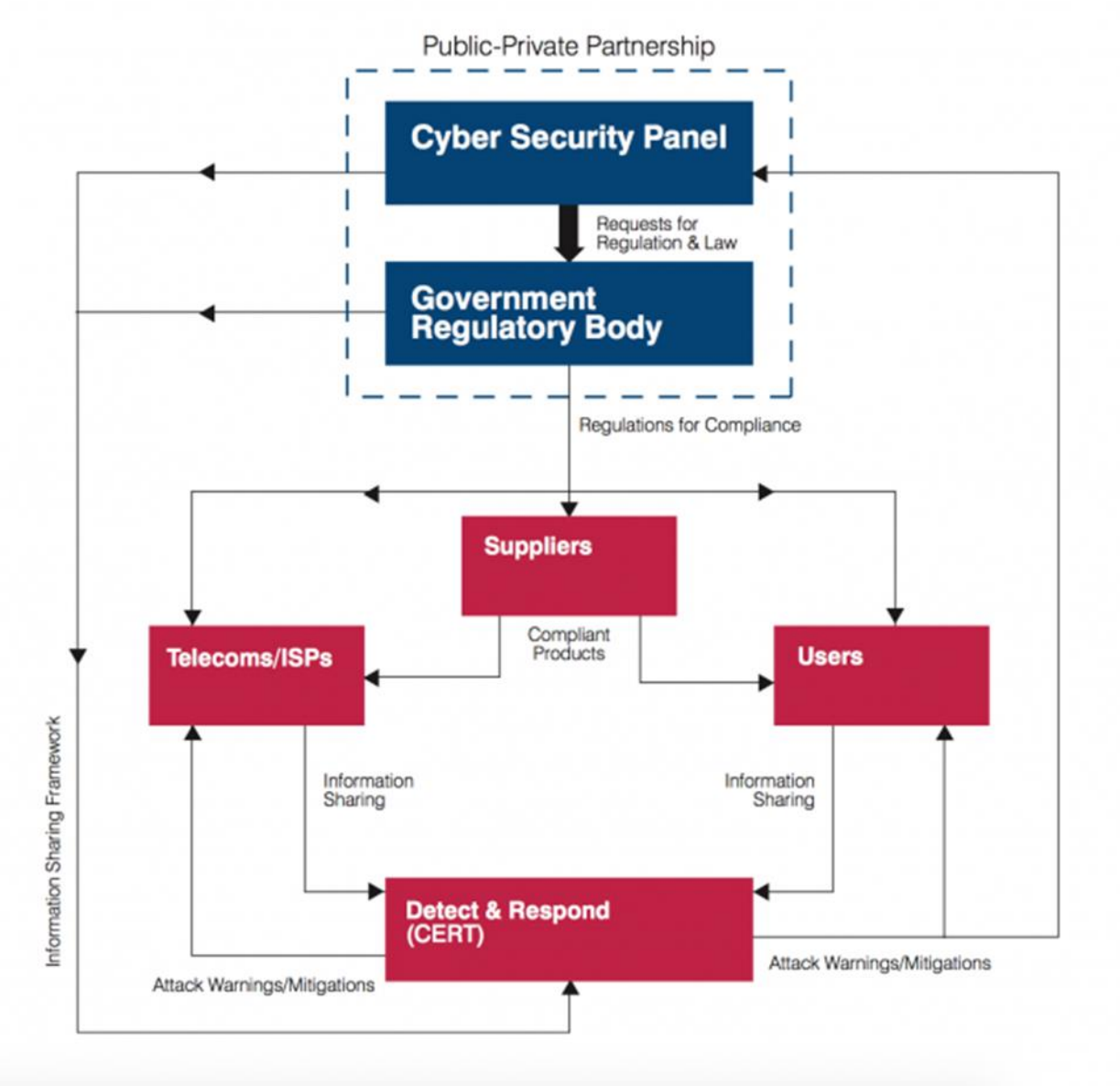
100. Yost, (2017). Nato Review. [online] Available at: http://www.nato.int/docu/review/2003/issue4/english/art4.html [Accessed 22 Aug. 2017].

101. Zaslavskiy, I. (2016) The Tsar and His Business Serfs. [online] Available at: https://www.martenscentre.eu/sites/default/files/publication-files/russia-elections-russian-oligarchs.pdf [Accessed 27 May. 2017].

102. Znaj.ua. (2017). Вірус "Петя" добряче підмочив репутацію українським компаніям. [online] Available at: https://znaj.ua/society/virus-petya-dobryache-pidmochyv-reputaciyu-ukrayinskym-kompaniyam [Accessed 22 Aug. 2017].

# Appendices

Graph 1




Source: ISANA (2017)

Table 1

| Date | Author | Target | Description | Attack | Links |
|---|---|---|---|---|---|
| 1/2/2015 | Anonymous | Ukrainian Law Enforcement and Justice Agencies | Anonymos claimed to have successfulду penetrated few Ukrainian Law Enforcement and Justice Agencies | Targeted Attack | |
| 7/16/2015 | Not known | http://unicredit.ua | Cyphort Labs discovered a malware infection at the Ukrainian website of UniCredit bank: unicredit.ua. | frame Injection | http://www.cyphort.com/unicredit-compromised/ |
| 7/30/2015 | | Ukraine | ESET reveals that the Win32/Potao malware family has been used for the past five years in covert targeted attacks against the Ukrainian government, served up by a trojanized | Targeted Attack | http://www.infosecurity-magazine.com/news/potao-trojan-served-up-by-russian/ |

| | | | | | |
|---|---|---|---|---|---|
| | | | Russian version of encryption software TrueCrypt. | | |
| 8/18/2015 | CyberBerkut | Unso.in.ua<br><br>Dontsov-nic.org.ua<br><br>Pse3zub.org<br><br>Ps-shop.com.ua<br><br>Bilozerska.info<br><br>Banderivec.ho.ua | The Pro-Russia collective CyberBerkut takes down several Ukrainian sites | DDoS | http://m.tyzhden.ua/news/115639 |
| 12/24/2015 | Russia according to Ukraine State Security Service(SSS, 2017) | Ukrainian Utilities | The Ukrainian government blames power outages in the Western Ukraine on "hacker attacks by Russian special services". According to the Security Service of Ukraine (SBU), malware has been found in the networks of some utilities. Moreover, these malware intrusions coincided | Targeted Attack | http://www.theregister.co.uk/2015/12/29/kiev_power_outages_blamed_on_russian_hackers/ |

| | | | | | |
|---|---|---|---|---|---|
| | | | with a “non-stop telephone flood at utility plants’ technical support departments”, according to local reports.The attack was performed by using Black energy program which brought Killdisc malware to the information system of the grid. It was reported that a number of documents, visual ad video materials were destroyed as a result of an attack thus giving the ground to claim that the attack on Prykarpattia power grid was also an act of cyber espionage. Furthermore, the attack on Prykarpattia power grid seem to represent the ‘first time since Stuxnet degraded Iran’s | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | uranium processing capability in 2010 that a cyber attack has been used to cause a physical outcome'(Vijagan, 2016).<br>The Ukrainian government blames power outages in the Western Ukraine on "hacker attacks by Russian special services". According to the Security Service of Ukraine (SBU), malware has been found in the networks of some utilities. Moreover, these malware intrusions coincided with a "non-stop telephone flood at utility plants' technical support departments", according to local reports. | | |
| 1/5/2016 | root AKA @ciadotgov | allwomenstalk.com | Root AKA @ciadotgov hacks | Unknown | http://siph0n.net/exploits.php?id= |

| | | | | | |
|---|---|---|---|---|---|
| | | | allwomenstalk.com and dumps 136,938 usernames and passwords. | | 4358 |
| 1/6/2016 | Russia according to Ukraine State Security Service(SSS, 2017) | Ministry of Finance | On December 6, 2016 a cyber attack against Ministry of Finances took place with the aim to terminate budget process in Ukraine. Because of the attack payments and money transfers for million of UAH were terminated and slowed down. In order to fight with the consequences of the attack and prevent similar attacks in future Ukrainian government allocated 40 mln of UAH to buy new computer and information systems. According to Ihor Malchenyuk, cyber security specialist from Microsoft Ukraine such actions will not | Targeted Attack | https://economics.unian.ua/other/1666452-minfin-povidomiv-pro-problemi-z-platejami-derjkaznacheystva-pislya-hakerskoji-ataki.html |

| | | | | | |
|---|---|---|---|---|---|
| | | | prevent future cyber attacks. 'Resources should rather be allocated into trainings of civil servants and IT specialist of new types of cyber threats as well strengthening exciting information systems with effective cyber security measures which would make an attack against government and country's critical infrastructure costly and complicated.' (Malchenyk, 2017) | | |
| 1/16/2016 | Russia according to Ukraine State Security Service (SSS, 2017) | Kyiv Airport | Ukrainian authorities announce to review the defences of government computer systems, after detecting a cyber attack on Kiev's main airport launched from a server in RussiaOn January 16, 2016 there was a cyber attack against | Targeted Attack | http://uk.reuters.com/article/uk-ukraine-cybersecurity-malware-idUKKCN0UW0S7 |

| | | | | | |
|---|---|---|---|---|---|
| | | | Ukrainian airport Boryspil. Blackenergy program was found on one of departments of the airport. However, due to the fact that the program was found before starting to spread to the whole information system of the airport no damage was done. The information security system of the airport was reviewed and is expected to be changed in order to be ready to cyber attacks. Similarly to other cyber attacks against Ukrainian critical infrastructure Russia is suspected to be an originator of the attacks, however the evidences are still need to be provided in order to prove it. | | |

| | | | | | |
|---|---|---|---|---|---|
| 1/20/2016 | Russia according to Ukraine State Security Service (SSS, 2017) | Ukrainian Utilities | ESET reveals a new wave of cyber attacks against the Ukrainian electric power industry. | Targeted Attack | http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/ |
| 5/18/2016 | Not known | Anti Ukraine Government Separatists | Researchers from ESET unveil the details of another cyberespionage operation in Ukraine: Operation Groundbait targeting anti-governative separatists. | Targeted Attack | http://www.welivesecurity.com/2016/05/18/groundbait/ |
| 6/25/2016 | Not known | Unnamed Ukrainian Bank | Another hacks carried on via the SWIFT messaging system: this time hackers have stolen $10 million from an unnamed Ukrainian bank, according to an ISACA report. | Targeted Attack | https://www.kyivpost.com/article/content/ukraine-politics/hackers-steal-10-million-from-a-ukrainian-bank-through-swift-loophole-417202.html |
| 9/3/2016 | Myrotvorets | Ukrainian alleged pro-Russian Journalists | Myrotvorets, a group of Ukrainian nationalist hackers, leaks the personal details of local | Account Hijacking | http://news.softpedia.com/news/pro-ukraine-hackers-leak-personal-details- |

| | | | | | |
|---|---|---|---|---|---|
| | | | journalists they consider pro-Russian for the second time in four months. | | of-ukrainian-and-foreign-journalists-507926.shtml |
| 12/6/2016 | Not known | State Treasury Service of Ukraine (treasury.gov.ua) and Ministry of Finance | The Website of the State Treasury Service of Ukraine redirects the users to www.whoismrrobot.com. Also, the website of the Ministry of Finance of Ukraine experiences a service disruption. | DNS Hijacking | http://uaposition.com/latest-news/ukraine-state-treasurys-website-hacked/ |
| 12/13/2016 | Not known | Ukraine's defence ministry | Ukraine's defence ministry says that its website is down due to cyber attacks that appeared aimed at disrupting it giving updates on the pro-Russian separatist conflict in eastern regions. | DDoS | http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN1421YT |
| 12/15/2016 | BlackEnergy | Ukrainian Banks | ESET reports that BlackEnergy, the same group who targeted Ukrainian utilities last December has been | Targeted Attack | http://www.theregister.co.uk/2016/12/15/ukraine_banks_apt/ |

| | | | | | |
|---|---|---|---|---|---|
| | | | using the TeleBots malware against Ukrainian banks in the last month. | | |
| 12/20/2016 | Not known | Kiev's Power Grid | Ukraine investigates a suspected cyber attack on Kiev's power grid at the weekend, the latest in a series of strikes on its energy and financial infrastructure | Targeted Attack | http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF |
| 12/23/2016 | Fancy Bear (APT28) | Ukrainian Artillery Units | Fancy Bear, the hacker group previously linked to the Russian Military Intelligence (GRU), is believed to have deployed malware on Android devices to track and target Ukrainian artillery units over the past two years. | Targeted Attack | http://www.ibtimes.co.uk/russian-hackers-deployed-android-malware-track-target-ukrainian-artillery-units-1597834 |

Source: Anna Melenchuk and Piret Pernik (2017)

**Table 3 Entrance campaign to Ukrainian Universities; Information security specialty in 2014.**

| | Eastern region | | | Central region | | | Western region | Sum |
|---|---|---|---|---|---|---|---|---|
| | KhNU | KhAI | KhNURE | NTUU "KPI" | NAU | SUT | Lviv Poly-technic | |
| SICS | 28 | 22 | 40 | 54 | 74 | 23 | 24 | 265 |
| STIS | - | - | 30 | 32 | 32 | 27 | 33 | 153 |
| ISM | - | - | 2 | - | 46 | 16 | 30 | 94 |
| | | | | | | | **Total:** | **512** |

Source (Ministry of education, 2017)

**Appendix 4**

Interviewees:

*Government*

1. Zolotukhin Dmytro, Deputy Minister of information of Ukraine

2. Dmytro Dubov, Expert of National Institute of Strategic Studies, was involved in drafting Cyber Security Strategy of Ukraine

3. Former representative of SSSCIP (State Service of Special Communication and Information Protection), anonymous.

*Business*

1. Viktor Zhora, director 'Infosafe Ukraine'

2. Ihor Malchenyuk, Microsoft Ukraine

3. Vladyslav Styran, director 'Berezha Security'

*Civil society*

1. Lilia Oleksiuk, Head of the Association of Ukrainian NGOs 'Information security and information technologies'

2. Kateryna Chaika, founder of 'Cyber Warta' NGO

3. Mykola Konstynian, Civil society cyber security trainer

4. Andrey Rybalchenko, International NGO 'ASACA' member

5. Eugene Dokunin, founder of Ukrainian Cyber Forces

6. 'Cyber Shield' NGO representative (anonymous)

*International organizations*

1. Nadia Khvan, OSCE Programme Officer

2. OSCE cyber security officer, anonymous

*Experts, think tanks*

1. Kenneth Geers, Atlantic Council Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence Ambassador

2. Henry Roigas, Project Manager at NATO Cooperative Cyber Defence Centre of Excellence

3. Piret Pernik, Research Fellow of International center of security and defence in Estonia

4. Serhiy Radkevych, Expert at Center for Research of Army, Conversion and Disarmament

## Appendix 5

Topics and questions discussed with interviewees:

- Introduction to resilience concept in international relations. In your opinion does Ukrainian efforts in cyber security correspond to this concept's criteria?
- Which issues related to cyber resilience Ukraine faced in 2014-2016? Which of such issues your organization/institution is addressing or can address?
- Which projects are targeted at cyber resilience in your respective organization?
- How would you evaluate the role of civil society and businesses in providing cyber security in Ukraine? Is community-based approach to security used? Are Ukrainian citizens cyber resilient?

**Non-exclusive licence to reproduce thesis and make thesis public**

I, Anna Melenchuk

(personal identification code 2489824m)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright, Is Ukraine Cyber Resilient?

supervised by Eoin Micheál McNamara and Dr. Eamonn Butler,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu 25.08.2017 (date)

(signature)