Kyiv National University of Trade and Economics

The World Economy Department

FINAL QUALIFYING PAPER (PROJECT)

on the topic:

"NATIONAL CYBER SECURITY IN GLOBAL COMPETITION"

(based on the Ministry for Development of Economy, Trade and Agriculture of Ukraine)

Student of the 2nd year, 2nd group,
specialty 051 "Economics",
specialization "International economics" _____ Daria Sharan

Scientific adviser
Candidate of Science (Economics),
Associate Professor _____ O. O. Shnyrkov

Manager of the educational program
Candidate of Science (Economics),
Associate Professor _____ K. P. Kravets

Kyiv, 2020

TABLE OF CONTENT

INTRODUCTION……5

PART 1. ANALYSIS OF THE CURRENT STATE OF CYBER SECURITY IN THE WORLD IN THE CONDITIONS OF GLOBAL COMPETITION……8

1.1. An overview of current problems of cybercrime and trends in cyberspace……8

1.2. The main trends of cyber security in the world……16

Conclusions to part 1……23

PART 2. ANALYSIS OF THE LEVEL OF NATIONAL CYBER SECURITY IN THE CONDITIONS OF GLOBAL COMPETITION……24

2.1. Features of national cyber security in conditions of global competition……24

2.2. Cyber security assessment of Ukraine and its issues……31

Conclusions to part 2……38

PART 3. DIRECTIONS OF IMPROVING THE LEVEL OF NATIONAL CYBER SECURITY IN THE CONDITIONS OF GLOBAL COMPETITION……39

3.1. International cooperation as a direction of cyber security of Ukraine……39

3.2. Forecast assessment of the effectiveness of the proposed measures to increase national cybersecurity……45

Conclusions to part 3……53

CONCLUSIONS……54

REFERENCES……57

ANNEXES……64

LIST OF SYMBOLS

CERT – Computer Emergency Response Team

CERT-UA – Computer Emergency Response Team of Ukraine

CIIP – Critical Information Infrastructure Protection

CoE – The Council of Europe

CPS – Cyber-Physical Systems

CSIRT – Computer Security Incident Response Team

CSIRT – Cyber-Security Incident Response Team

DoD – Department of Defense

ENISA – European Union Agency for Network and Information Security

GCA – the Global Cybersecurity Agenda

GCA – Global Cybersecurity Agenda

GCI – Global Cybersecurity Index

GRPS – Global Risk Position System

IoT – Internet of Things

GSI – Global Cybersecurity Index

HLEG – High-Level Experts Group

ICT – Information and Communication Technology

IDI – ICT Development Index

ISACA – Information Systems Audit and Control Association

ISP – Internet Service Provider

IT – Information technology

ITU – International Telecommunication Union

MLAT – Mutual Legal Assistance Treaties

MoD - Ministry of Defence

NATO – North Atlantic Treaty Organization

NCS (NCSS) – National Cybersecurity Strategy

NCSC – The National Cyber Security Centre

OT – Operational Technology

PAC – Pierre Audoin Consultants

R&D – Research and Development

SME – Small and medium-sized enterprises

UN – the United Nations

INTRODUCTION

In the Era of Digitalization, the importance of involvement in the Internet network of all aspects of commerce, government institutions, private sector organization and just ordinary citizens is significant. The Internet-based technologies have offered increasing opportunities for economic and social development worldwide. These technologies have brought, or will bring, significant competitive advantage into everyday life so cyber security is being a hot topic for whole modern world, especially this issue is considered by all developed countries. The probability of the potential macro-economic consequences of cyber-attacks raised many disputes between experts of cyber security. Cyber criminals are seeking to compromise countries systems and data. Cyber activity knows no international boundaries. That is why over the last several years many countries have published national cyber security strategies with the aim to improve or achieve their nation security in cyberspace. International research centers and organizations have published some recommendations on issues to include in these strategies. Avoiding the danger of cyber-attacks or preventing them on time shows the strength of the government system, legislations and is becoming a significant advantage over other nations.

The relevancy of the final qualifying paper (project) reflects the increasing importance of cyber security. It is connected with the fact that despite knowledge of importance of the national cyber security, many countries is still far away of real security in cyberspace. Not considering of having the national cyber security strategy, many states even don`t have a proper legislation. So It is an urgent question to provide countries with more comprehensive practical and technical recommendations about the covering the key public policy issues of legal frameworks, educational programs, and political coordination about cyber security.

The development of the topic is supported with continuous studies not only by foreign and Ukrainian scholars and practitioners but also by governments, international

organizations and agencies. In order to prevent and minimize cyber-attacks governments all over the world are developing the national cyber security strategies.

Hence, the theoretical and practical aspects of cybercrime and the areas of counteraction are best investigated by national cybercrime bodies and outlined in national strategies and doctrines: Cybersecurity Doctrine of the Republic of Poland' (National Security Bureau, 2009), Cyber Security Strategy for Germany (Federal Ministry of the Interior, 2011) etc.

The studies about strategic controls are very scarce and they usually belong to regional or international bodies like the European Union Agency for Network and Information Security (ENISA), International Telecommunication Union (ITU), High-Level Experts Group (HLEG,) North Atlantic Treaty Organization (NATO).

Among the scholars who are investigating the current state and directions of combating cybercrime in Ukraine, it is worth highlighting O.S. Bondarenko, M. Kravtsova L., Kovtun, O.V. Kosarevska, O.I. Novitsky, D. Dubov, V. Petrov and others.

The purpose of this research is to identify the gaps in Ukrainian cyber security system and to provide the recommendations of establishing the thorough policy of cyber security and strategic control in order to make a cyber-security a competitive advantage of Ukraine in international arena.

Object of the final qualification work is the process of improving the international competitiveness of Ukrainian cyber security in the environment of international economic and technological activity.

Subject of the research is the theoretical and practical aspects of functioning of external and internal factors that affect the national and global level of cyber security and infrastructure.

The following **research methods** are used in this work: empirical (experiment, observation, description), the method of structural and logical generalization (construction of structural-logical models), theoretical (analysis, generalization,

induction, deduction, explanation, classification), economic-statistical analysis, analysis of frames and reports constructed by relevant political actors, cybersecurity sector experts, international agencies and organizations, scientists and ethical hacktivists is the main research method.

Achieving this goal led to the following **main objectives**:

- detailed analysis of the current problems of cybercrime and trends in cyberspace;
- diagnostics of the main trends of cybersecurity in the world;
- determination the features of national cybersecurity in conditions of global competition;
- the assessment of Ukrainian cybersecurity and its issues;
- proposed development of international cooperation as a direction of cyber security of Ukraine ;
- forecast assessment of the effectiveness of the proposed activities measures to increase national cybersecurity.

The scientific and practical novelty of the obtained results lies in the set of methods, approaches, procedures and recommendations of increase Ukrainian cooperation with International organization. Practical significance consists in the future development of cyber security approaches of Ukraine and raise awareness and relevance of the topic.

Approbation and utilization of research result. The results of this research were represented in a collection of scientific articles `International economics`, KNUTE, Kyiv, 2020 by the students of full-time education program – i.e. Master of Science in Economics.

PART 1. ANALYSIS OF THE CURRENT STATE OF CYBER SECURITY IN THE WORLD IN THE CONDITIONS OF GLOBAL COMPETITION

1.1. An overview of current problems of cybercrime and trends in cyberspace

The development of computer and Internet technologies is an absolute achievement and a preference for modern society: business opportunities are expanding, trade has become global, payments are made through international payment systems, the world has become open and free for communication between people. At the same time, the Internet has caused the emergence of new types of crime, which before this date did not exist, and made possible the transformation and growth of existing types of crime. The various fraudulent criminal schemes, which are based on fraudulent money takeover of Internet users, are especially actively developed and improved (Myskiv, Irshak, 2019, pp. 365-376).

Computer network became a key element in individual's life, in successful business operating and expanding, in whole industries functioning and even on country level security. Computer networks currently have joined water, food, transportation, and energy as the critical resource for the function of the national economy. Application of Cyber-Physical Systems (CPSs) can be seen in many forms of industries. The common sector is oil and gas, the power grid manufacturing, defense and public infrastructures are fully relying on the advancement of CPS. Therefore, cyber-physical systems security has become a matter for societal, infrastructures and economic to every country in the world due to the tremendous number of electronic devices that are interconnected via networks communication (Wang and Z. Lu, 2013, pp. 1344–1371). Latest reports have shown that cyber-attacks are aimed to destroy nation`s systems that used for country development. CPS starts with by not simply disrupt a single enterprise or damage an isolated machine, but a target to damage infrastructures via modern dynamics threats (Ali, 2016, p. 303). Those types of attacks are able to provide destruction to critical infrastructures system, which used in sectors such as defense, finance, health, and the public (Al-Mhiqani, Ahmad, Abdulkareem, Ali, 2017, pp.

6557-6567). Increased security risk awareness and appropriately security relevant information management provide an equally important role in the trusted infrastructure maintenance.

To understand the all tremendous threats that might cause the CPSs, firstly such terms as `*cyber space*`, `*cybercrime*` and `*cyber terrorism*` are needed to be considered.

One of the many national strategic objectives is ***cyber-space protection*** in order to protect critical infrastructure and decreasing possibility of intrusion and cyber-attacks but also reducing damage consequence caused by cyber-attacks (Ackoski, Dojcinovski, 2012). The US Department of Defense (DoD) defines ***cyberspace*** as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (Wills, David, and Bunn, Sarah, 2006).

There are a various directions of cyber threats which causes millions of losses for economies around the world. The Figure 1.1 demonstrates the comparison of the distribution of the most widespread types of cyber threats: cybercrime, cyber espionage, hacktivism and cyber warfare.

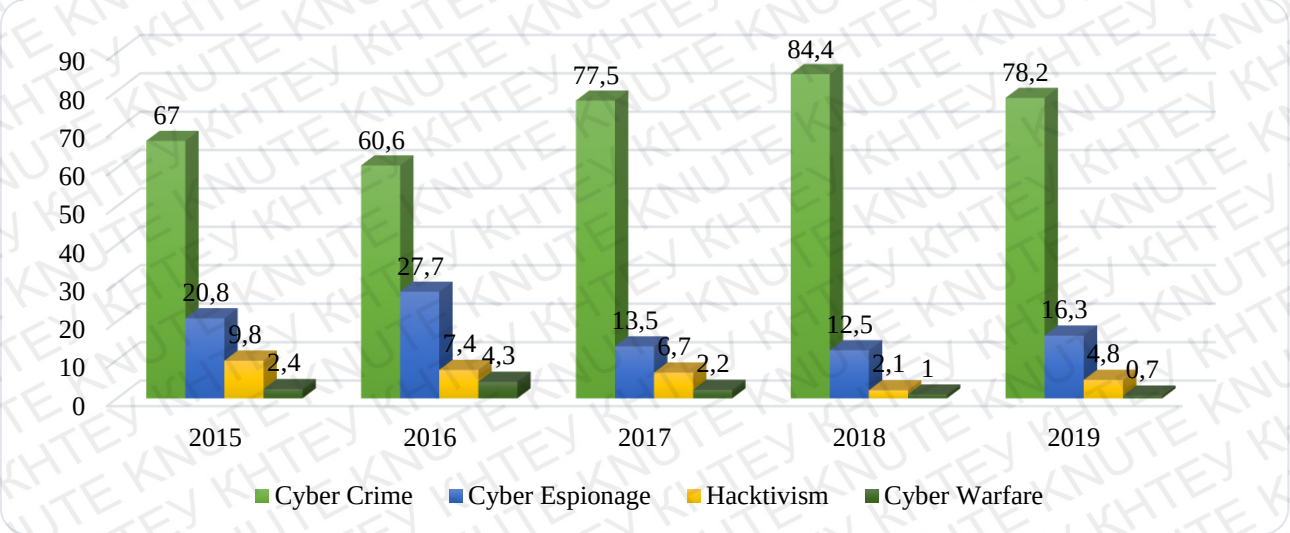

Figure 1.1. Motivation of cyber threats in 2015-2019 in %

Source: composed by the author based on Hackmageddon, 2020 data

Discussions are under way to the term „**cybercrime**". Most reports, guides or publications on cybercrime begin by defining the terms "computer crime" and "cybercrime". In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms.

During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop (Kumar, 2019, p.29).

Cybercrime in *a narrow sense* (computer crime) covers any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in *a broader sense* (computer-related crimes) covers any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network (Elsevier Science, 2005, pp.149-164).

In 2001 The Council of Europe (CoE), adopted its Convention on Cybercrime Treaty, known as Budapest Convention which identifies several *activities to be cybercrime offences* (CoE, 2001):

• Intentional access without right to the whole part of any computer system.

• Intentional interception, without right, of non-public transmissions of data.

• Intentional damage, deletions, deterioration, alteration, or suppression of computer data without right.

• Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering, or suppressing computer data.

• The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent of committing any of the above crimes.

One more important definition which should be considered is `***cyber terrorism***`.

According to US law, the state secretary has obligation to get the report on Congress each year, which is put into the Annual report. Terrorism is defined in a follow way: "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents". According to Federal Bureau of Investigation (FBI), new phenomenon recognized as *a cyber-terrorism* is defined by follow: "previously planned, politically motivated attack against information, computer systems, computer programs and data that result with violence against targets that are not military (civilian) by the sub - national groups or secret agents" .

Another definition according to the US Commission for Protecting Critical Infrastructure is that *terrorist attacks* are created in order to cause physical violence or extreme financial damage. The cyber terrorist will seek to accomplish their mission by techniques not mitigated by classic security mechanisms (Petrović R. S., 1999).

There are cases that have been described as cyberterrorism. For example, in 2000, an Australian man hacked into a municipal waste-management system and dumped "millions of liters of raw sewage" into parks, rivers and businesses.

In 1997 a Massachusetts hacker shut down all communications to a Federal Aviation Administration control tower at an airport for six hours.

On the Table 1.1, the cost of cyber terrorism is illustrated compared to GDP.

Table 1.1

Regional Distribution of Cybercrime in 2018

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	$75.8	$445 to $608	0.59 to 0.80%

Source: CSIS, McAfee, 2018

Cybercrime costs businesses close to $600 billion, or 0.8 percent of global GDP, which is up from a 2014 study that put global losses at about $445 billion, according to a report by McAfee, in partnership with the Center for Strategic and International Studies (CSIS).

The number of cybercrimes is increasing significantly from year to year. The impact of cyber activity on society is reflected in the numbers. In August of 2016, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined. The cybercrime prediction stands, and over the past two-plus years it has been corroborated by hundreds of major media outlets, academia, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally (Steve Morgan, 2019).

The Center for Strategic & International Studies (CSIS) tracks “cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.” Over the past decade, they’ve tracked 490 significant cyber incidents.

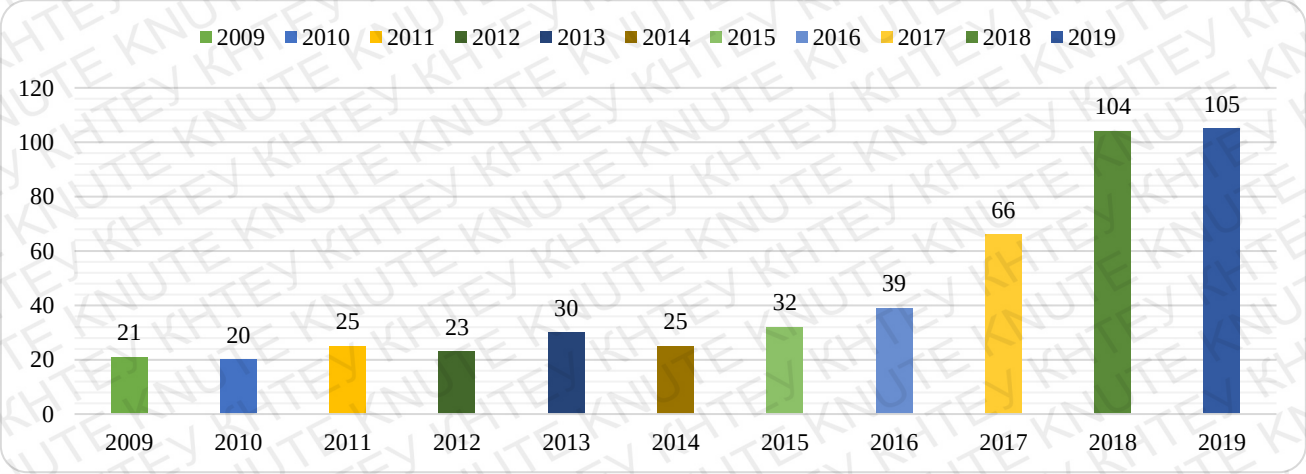

Figure 1.2. Cyber-attacks incidents with +1 million dollars in Reported Losses

Source: CSIS, 2020

Cyber-attacks are considered to be a great risk by a lot of countries. This topic is under discussion by major international structure and summits. For example, In the World Economic Forum Global in Davos, cyber security is a justified as one of the biggest risks during the several past years. Technology continues to play a profound role in shaping the global risks landscape for individuals, governments and businesses. In the GRPS, "massive data fraud and theft" was ranked the number four global risk by likelihood over a 10-year horizon, with "cyberattacks" at number five. This sustains a pattern recorded last year, with cyber-risks consolidating their position alongside environmental risks in the high-impact, high-likelihood quadrant of the Global Risks Landscape. Annexes A - B illustrates the position of cyber security in the landscape of risks in 2019. Around two-thirds of respondents expect the risks associated with fake news and identity theft to increase in 2019, while three-fifths said the same about loss of privacy to companies and governments.

Companies and governments are increasingly investing in improving their cybersecurity protocols as the frequency of attacks rises. Figure 1.3 illustrates the lost prepared countries against cyberattacks. (World Economic Forum, 2019, p.12-16).

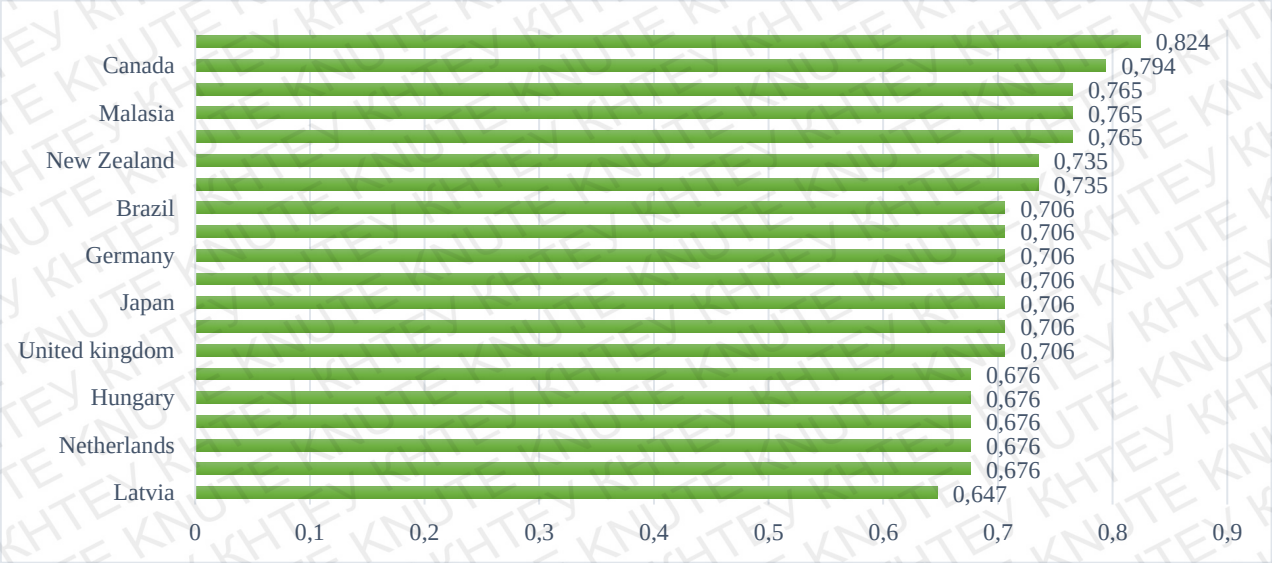

Figure 1.3. Percentage of businesses expecting short-term risks increasing in 2019

Source: World Economic Forum, 2019

Countries (means government systems, industries, community structures) are potential victims gathering corporate or government information illegally in order to subvert competitive advantage or national security. There are a lot of examples when the whole government structures were attacked by cyber criminals with huge damages accordingly.

It is not a challenging threat only for government but also for the whole economy of each particular country. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

There are some *range of industries that are more likely to be hacked*, for instance such industries as pharmacy, finance industry, energy and technological companies.

Energy companies and need to be aware of the various cyber threats that face them, and accept that their strategic role in society places them in the firing line of some particularly skilled and motivated attackers, including state actors. Energy sector organizations are becoming increasingly concerned about cyber-attacks affecting their operations and many are still trying to keep up with the pace of the evolving sophistication of attacks that are becoming increasingly more frequent, impacting our critical national infrastructure.

Banks and other financial firms clearly need their security teams to monitor their IT infrastructures for weaknesses, not stand in front of the safe. Virtual and electronic security are arguably more important than physical security. A single hacker can make off with the information of hundreds of thousands of customers, stealing more money from more people than a single old-fashioned bank robber could make off with in a number of heists our critical national infrastructure.

Industry and technology companies are one of the most popular targets for cyber criminals. The scale and variety of cyber threats to these industries have grown considerably in the recent years. Industrial Control Systems (ICS), Internet of Things (IoT) and Operational Technology (OT) have been at the center of many recent high-profile breaches.

Pharmacies tend to be highly exposed in terms of the threats cape as they combine retail (payment systems and data) with health. That these are two of the hottest spots on the cyber-criminal radar right now makes the pharmacy a prime target (Statista, 2020).

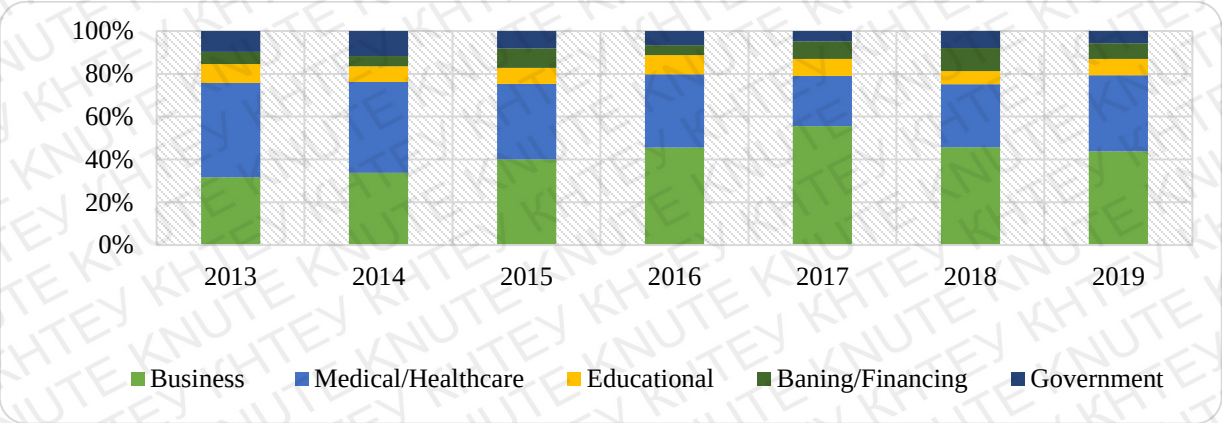

Figure 1.4. Number of data breaches in the US from 2013 to 2019, by industry

Source: Statista, 2020

The Figure 1.4 shows the number of data breaches in the United States from 2013 to 2019, by industry. In the last measured period, the majority of the 1,473 annual data breaches affected business and medical or healthcare organizations, with 644 and 525 data breaches respectively.

According to Statista as of 2020, the average cost of a data breach in the healthcare sector amounted to 7.13 million U.S. dollars. The global average cost of a data breach in the measured period was 3.86 million U.S. dollars. Data breaches in the public sector ranked last, costing an average of 1.08 million U.S. dollars during the measured period. In Annex C – D, expenditures by industry are illustrated.

1.2 The main trends of cyber security in the world

The primary duty of the government is to defend the country from attacks by other states, to protect citizens and the economy from harm, and to set the domestic and international framework to protect interests, safeguard fundamental rights, and bring criminals to justice. Authorities need to be aware of all markets of cyber security to provide measures. Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cybersecurity addresses cybercrime as one major challenge underlines this.

Countries all over the world are making alliances and collaborations, to prevent such losses for their economies and countries securities. For example, the ITU Secretary-General launched ***the Global Cybersecurity Agenda (GCA)*** (ITU, 2015) on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions. The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the GCA complements existing ITU work programs by facilitating the implementation of the three ITU Sectors' cybersecurity activities, within a framework of international cooperation. The Global Cybersecurity Agenda has seven main strategic goals, built on *five work areas*: 1) Legal measures;

2) Technical and procedural measures;

3) Organizational structures;

4) Capacity building; and

5) International cooperation.

This is a reason why cyber security plays such a big role in the modern government policies. Countries try to find effective tools, which will help to prevent cyber-attacks or at least will help to decrease the number and the influence of damages.

In order to elaborate preventing actions against cybercrime, firstly, it is important to know the directions of struggle. States around the world explore the potential market of cybercrime. According to report by Pierre Audoin Consultants (PAC), the market for cyber security is a varied one, and the market structure and supply chain depend on the nature of the business being protected and the extent of exposure to potential threats. There are identified four separate and distinct submarkets which require the cyber security measures.

The four submarkets are:

• *Defense and intelligence:* this submarket is focused on securing the nation's secrets, and involves the security and intelligence agencies as well as the MoD. It incorporates the most advanced (and most secret) cyber security technologies available. It is, however, a niche market and is relatively constrained in size.

• *Government, other than Defense & Intelligence:* this submarket incorporates all the other government funded cyber security tasks out with its defense and intelligence obligations. It includes security of health and education data, crime and criminal justice information, as well as more run of the mill (but essential) government operations. Although the requirements of this segment are varied and not as sophisticated as defense and intelligence, the segment is substantially larger in volume and spend.

• *Enterprises:* the bulk of the cyber security market is orientated around large commercial enterprises securing their day-to-day business. This would include banks, telecommunications companies, utility and energy firms, manufacturers etc. Some of these firms may play a huge role in the nation`s critical national infrastructure, but the nature of the threat is considerably less than that for intelligence and defense organizations.

• *SME and consumers:* most small and medium-sized businesses have cyber security needs, but these are substantially less in sophistication and scale to those experienced by larger organizations in government and business. Similarly, consumers do have cyber security requirements but again these are at the low end of the sophistication spectrum. We have aggregated the submarket for SMEs and consumers because the supply chains serving their needs are similar (Pierre Audoin, 2013).

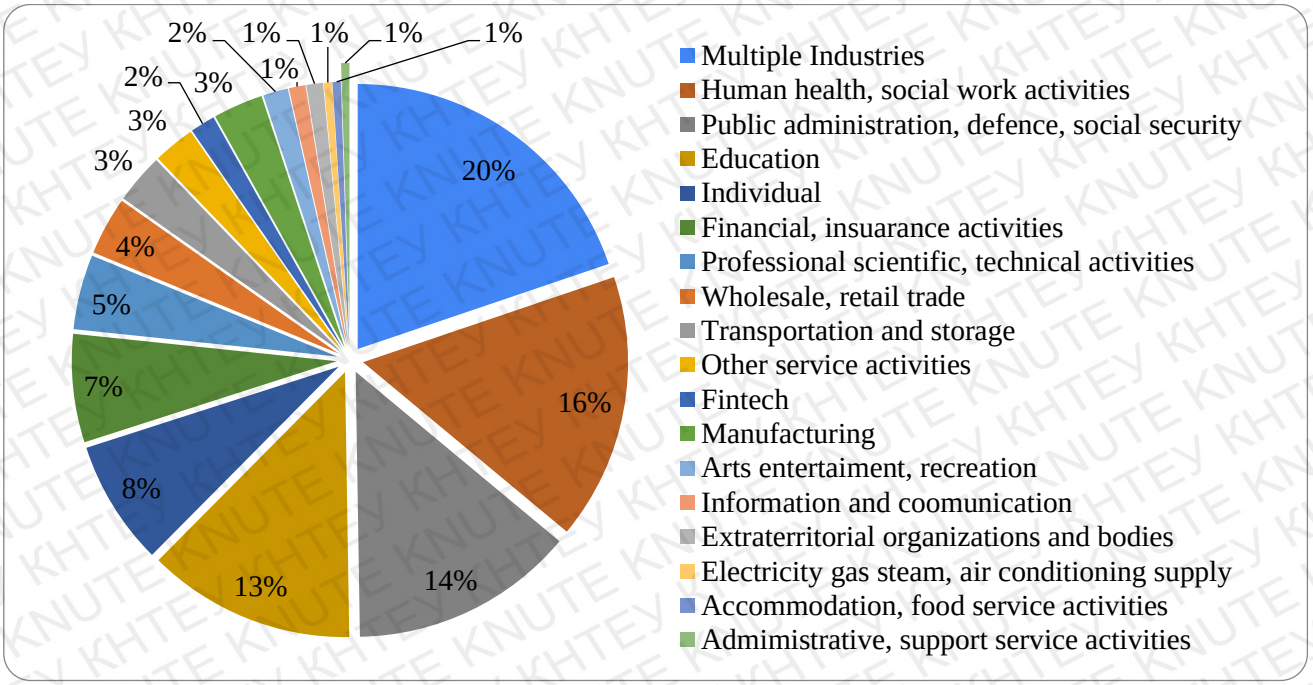

Figure 1.5. Target Distribution of cyber-attacks in September, 2020

Source: composed by the author based on Hackmageddon, 2020

In the Figure 1.5 the latest statistics of cyber-attacks is demonstrated. Similarly to August, attacks against multiple targets lead the Distribution of Targets chart with 20% (down from 23.9% in August). Healthcare targets rank at number two with 16% (12.2% in August), ahead of government targets 14% (12.4%).

Such sorting system helps countries to divide the volume of pending issues about the national security. National structures will be responsible for macro level: developing legislation, developing common cyber security strategy, implementation and regulation of proposed actions etc. Considering micro level, companies, which

provide cyber security services, will help to develop strong technical systems with other security measures.

Taking into consideration the cyber security, it is a competitive advantage of a country, currently. It shows that the security of citizen data is taken seriously. There is still a visible gap between many countries in terms of knowledge for the implementation of cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programs in the field of cybersecurity. Sustainable development in this area should ensure the resilient and adequate use of ICTs as well as economic growth.

So modern approach of evaluating cyber security of a country is making a full analysis of each aspect of cyber field, which is illustrated in an index. One of such indexes is called The Global Cybersecurity Index. ***The Global Cybersecurity Index (GCI)*** is a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of countries with regard to the five pillars of the Global Cybersecurity Agenda (GCA). These pillars form the five sub-indices of GCI. The main objectives of GCI are to measure:

• the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;

• progress in cybersecurity commitment of all countries from a global perspective;

• progress in cybersecurity commitment from a regional perspective;

• the cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives) (ITU Publications, 2018).

Some pillars are easier to achieve, some are hard to obtain, but many states still don`t have even proper legislation or even a concern of importance cyber security.

The colors in the Figure 1.6 indicate differences in the level of commitment with high, medium, and low scores in a range of colors from light blue (peak commitment) to dark blue (low commitment).

Figure 1.6. Heat map showing geographical commitment around the world

Source: Global Cybersecurity Index (GCI) ITU Publications, 2019

Countries are classified according to their level of commitment: high, medium, and low.

1. Countries that demonstrate high commitment in all five pillars of the index.
2. Countries that have developed complex commitments and engage in cybersecurity programs and initiatives.
3. Countries that have started to initiate commitments in cybersecurity.

The level of commitment tables upper list the countries that have maintained high, medium, and low GCI scores. Scores were obtained using the 99 percentile: High countries within this range (1.000- 0.670) are ranked (1-51), total 54 countries, medium country scores (0.669-0.340), range in rank from 52-99 totaling to 53 countries. Low country scores (0.339-0.000) range in rank from 100-175, with a total of 87 countries (Shafqat, Masood, 2016).

Geographically, Mexico reclaimed the top spot for the most organizations experiencing a successful attack (93, 9%). Down the list, China (83, 3%), the US (82, 6%), the UK (82, 3%), and France (81, 1%) were a bit above average. Compromised less often than most were Germany (79, 2 %), Brazil (77, 4), and Japan (76, 7%).

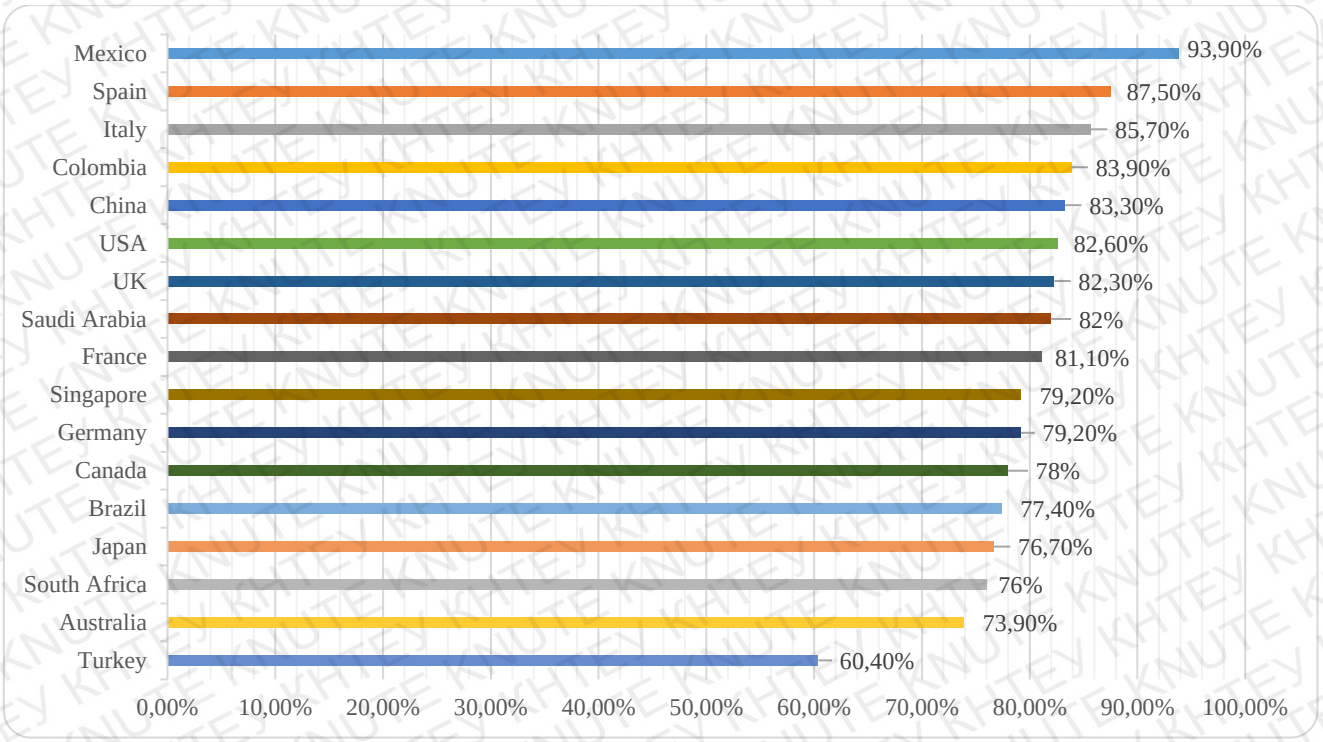

Figure 1.7. Percentage of compromised businesses by at least one successful attack in path 12 month, by country

Source: composed by the author based on CyberEdge Group, 2020

The goal of the GCI is to help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the collected information, GCI aims to illustrate the practices of others so that countries can implement selected aspects suitable to their national environment, with the added benefit of helping to harmonize practices, and foster a global culture of cybersecurity.

Another approach of developing cyber security is raising the awareness of all market players. In order to have a clear vision of fighting with cybersecurity, a lot of countries around the world annually publish their ***cyber security strategies*****.** The cyber security strategies exist in various forms and length varying from nine pages (Netherlands Cyber Security strategy of 2011) to ninety pages (Saudi Arabia's Cyber Security strategy of 2013). Most of the countries under study have developed separate

strategies for national defense and cyber security, whereas few have added a portion of "cyber security" in the national security strategy or the defense strategy.

The timeline infers that majority of the countries published their cyber security strategy in 2011. The United States of America, on the other hand, published the first strategy draft in 2003, when cyber-attacks were not very common.

National Cybersecurity Strategy (NSC) basically defines the vision of any country for addressing the cyber security challenges at the national level. Since all strategies are directed towards the ultimate goal of safeguarding the national cyberspace, they share many common themes and concerns. Except for Germany, which lists down some priority areas as the objectives, all other countries clearly states their strategic objectives in the document. The common objectives found in almost all NCS are:

- to maintain a safe and resilient cyberspace;
- to secure critical national cyber assets and infrastructures;
- to define a cyber-security regulatory, legislative and assurance framework;
- to raise cyber awareness amongst citizens, government officials;
- to develop cyber security incident detection and response capabilities e.g. Cyber-Security Incident Response Team (CSIRT) etc.,
- to develop indigenous cyber-security technology,
- to promote public-private co-operation for enhancing the cyberspace security,
- to stimulate international co-operation with neighboring and regional countries.

Beside the common ones, few strategies have also proposed objectives that are only specific to their country. For instance, France desires to become a world leader in cyber security domain in near future. Also, Japan desires for agile adaptation of evolving cyber threats and introduction of global outreach programs for cyber security.

The thorough study of the selected strategies also brings forward the fact, that with the passage of time, the scope of cyber security strategies is shifting from merely

securing citizens or governments against cyber-attacks to securing the whole information society in general (Luiijf, Besseling, Spoelstra, Graaf, Ten. 2013).

Conclusions to part 1

Cybersecurity has a field of application that cuts across all industries, all sectors, both vertically and horizontally. In order to increase the development of national capabilities, efforts have to be made by political, economic and social forces. This can be done by law enforcement, justice departments, educational institutions, ministries, private sector operators, developers of technology, public private partnerships, and intra-state cooperation considering the long-term aim to increase efforts in the adoption and integration of cybersecurity on a global scale.

Cyber threats are names as one or the biggest challenge for nearest period all over the world. It doesn`t concerns and individual citizen, the enterprises, governments and the whole country can be affected. It is names also one of the biggest challenge for economy because even industries are becoming a potential victims. There are some *range of industries that are more likely to be hacked*, for instance such industries as pharmacy, finance industry, energy and technological companies.

Authorities around the world have already understood the importance of upcoming problem and in order to prevent the potential financial and intellectual losses in long-term period, governments are collaborating and formatting different alliance. ITU, ENISA, NATO, ISACA are leading organization in fighting with cyber criminals. Moreover, countries establish National Cybersecurity Strategies, which usually are published annually in order to have a clear vision of future preventing actions.

Also, the assessment of cyber security is performed in a form of The Global Cybersecurity Index (GCI), which help to identify the leading countries in this sphere and deficiencies in national cyber systems.

PART 2. ANALYSIS OF THE LEVEL OF NATIONAL CYBER SECURITY IN THE CONDITIONS OF GLOBAL COMPETITION

2.1. Features of national cyber security in conditions of global competition

Cybersecurity is becoming a priority issue in the context of national security among both transitional and developed countries in modern digitized world. This is particularly relevant and is an urgent topic for Ukraine, which are struggling during the last years repetitively with high-profile malicious activity in cyberspace, the so-called "cyberattacks".

The dynamics of the cybercrime level in Ukraine since 2009 has been growing, although in some years there has been a reduction.

Table 2.1

Number of cybercrimes in Ukraine from 2009 to 2018

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Number of crimes	217	190	131	138	595	443	598	865	2573	1885

Source: composed by the author based on Kravtsova M., 2018

The number of detected cyber-security crimes in Ukraine increases on the average by 2.5 thousand annually. Therefore, a new unit was created in the structure of the National Police of Ukraine - the Cyber Police Department, which deals with cybercrime, develops a methodology and acquires knowledge from foreign partners.

In 2018, the Department of Cyber police of the National Police of Ukraine found about 6 thousand of crimes committed in the area of high-tech information technology, including:

- 2398 in the field of payment systems;
- 1 325 - crimes committed in the field of cybersecurity;
- 1598 in the field of e-commerce;
- 680 - in the field of illegal content (The National Police, 2018).

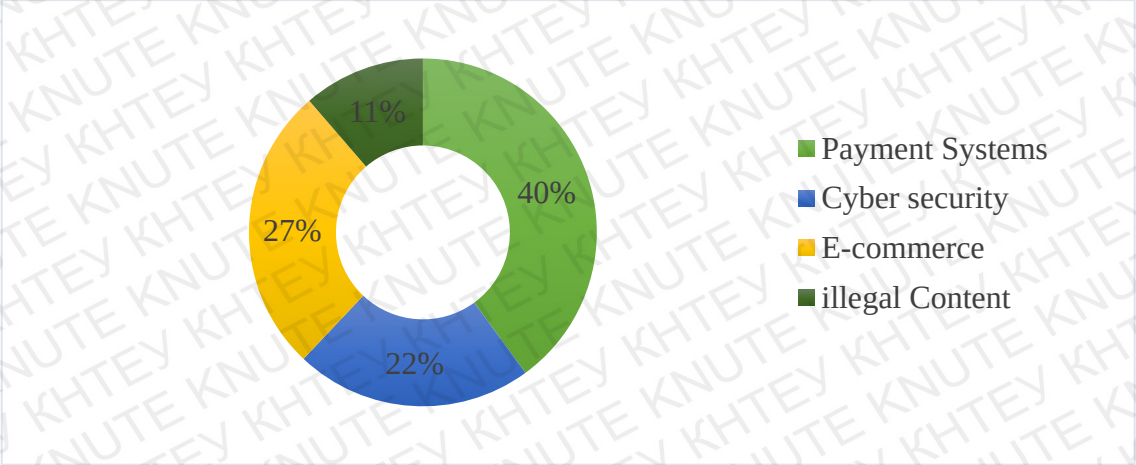

Figure 2.1. The percentage of fields of cyber security in Ukraine in 2018

Source: composed by the author based on The National Police data, 2018

Another example is when on June 27, 2017, several Ukrainian banks were attacked by hackers State Savings Bank limited some of the functions of customer service through a hacker attack to Ukrainian banks. A large-scale hacking attack using a version of `Petya` also caused the violation works of Ukrainian state-owned enterprises, agencies, banks, media, etc. Due to the attack, the activities of such enterprises have been blocked, as Kyivenergo, Boryspil Airport, Chernobyl stations, Ukrtelecom, UkrPoshta, Oschadbank, Ukrzaliznytsia, and other large enterprises.

The virus also attacked the Cabinet of Ministers of Ukraine, Inter TV channel, media holding of TRC Lux, which includes Channel 24, Radio Luxury FM, Radio Maximum, various Internet editions, as well as sites of Lviv City Council, Kyiv City state administration, cyber police, and special communications service of Ukraine. June 28, 2017, Cabinet Ministers of Ukraine reported that the attack on corporate and government networks has been stopped.

During 2018 the Cyberpolice of Ukraine was prevented from spreading 4 massive cyberattacks in the territory of the state and suspended activities of more than 40 unauthorized websites. Within the framework of international cooperation, 8 transnational hacker groups were exposed and more than 30 international operations took place (The National Police, 2018).

Very crucial field, which is considered by most of countries as one of the most important, is legal aspect. On the country level, proper legislation is an important issue. Ukraine has made some steps towards it which will be described below.

The first mention was in the principal provision of ***the Constitution of Ukraine*** (Law, 28.06.1996 № 254к/ 96-ВР). Article 17 states: "The protection of the sovereignty and territorial integrity of Ukraine, provision of its economic and information security are the most important functions of the state, a matter of the whole Ukrainian nation".1 There is no mention of cybersecurity per se; however judging by the spheres of protection that are seen as most important, it is safe to assume that cybersecurity falls into the area of information security.

A much more useful source of normative provision is the ***Law "On the Fundamentals of National Security of Ukraine"*** (Law, 19.06.2003№964-IV) Article 7 defines nine main areas of threats to national interests and national security of Ukraine. They are the spheres of external politics, state security, military and border security, internal politics, economy, social and humanitarian, science and technology, civil defense, information. The threats connected to the sphere of information security that are listed in the act are: limitations of the freedom of speech and access to public info; dissemination of the cults of violence, cruelty and pornography by media; manipulation of the public conscience (e.g., by spreading false, incomplete or biased info); disclosure of state secrets or other restricted info that is essential for the protection of national interests; *"computer crime" and "computer terrorism".*

Based on this understanding of types of information, another legal act - the Law of Ukraine "On Basic Principles of Information Society Development in Ukraine for 2007-2015" of 2007 is the only normative act that contains the following definition of ***information security***: "it is a state of protection of vital interests a person, society and the state, in order to prevent damage caused by incomplete, untimely and unreliable information used; negative information impact; negative consequences of the use of information technologies; unauthorized dissemination, use, breach of integrity,

confidentiality and accessibility of information ”(Law of Ukraine on Basic Principles of Information Society Development in Ukraine for 2007-2015, 2007).

Following the decision of the National Security and Defense Council of Ukraine on the National Security Strategy of Ukraine of 6 May 2015, adopted by Presidential Decree No. 287/2015 of 28 May 2015, ensuring Ukraine's entry into the EU and establishing the conditions for NATO membership are the key priorities of modern defense policy. One of the main challenges to national cyber security is the insecurity of Ukraine's vital infrastructure and public information systems.

Consequently, the National Cyber Security and Cyber Risk Response Center was established in Ukraine on 1 July 2015 to support the Computer Emergency Response Team of Ukraine (CERT-UA). The Center shall serve as the Technical Coordinator of State governments, local self-government entities, military agencies, businesses, organizations and organizations, regardless of the mode of ownership for the prevention, identification and elimination of cyber incidents. (Shypovskyi, Cherneha, Marchenkov, 2020).

It is emphasized that cyberspace is gradually being transformed into *a separate*, along with the traditional “Earth”, “Air”, “Sea” and “Space”, a sphere of warfare, in which the relevant units of the leading powers of the world are increasingly active. Given the widespread use of modern information technologies in the security and defense sector, the creation of a unified automated control system of the Armed Forces of Ukraine makes our country's defense more vulnerable to cyber threats (Cherep, Nurlikhina, Saenko, 2020).

For the introduction of this terminology and determination of priority directions of activity in this sphere it was suggested to renew the development of the Cyber Security Strategy of Ukraine Project (2015-2018). This project defines basic terms and definitions, threats in the sphere of cyber security, main principles of cyber security of Ukraine, main directions of resistance to threats in the sphere of cyber security, system of cyber security of Ukraine, stages of Strategy realization.

After that, on March 16, 2016, the President approved the Cyber Security Strategy of Ukraine approved by the National Security and Defense Council, and on February 25, 2017, the Doctrine of Information Security of Ukraine approved by the National Security and Defense Council. The new Cyber security strategy for the period starting from 2021 is developing.

Having provided an overview of threats to Ukrainian cybersecurity and reflected on the question of their classification, it is possible to move on to establishing ***the main actors*** in this area of national security and their roles in its provision. Unfortunately, today the legal basis of the system of said actors as a whole is provided mainly by Article 3 of the Cybersecurity Strategy, which is a document of the regulatory level and furthermore drafted in rather general terms, without in-depth specification of tasks or establishment of interaction mechanisms between actors. Nevertheless, an analysis of its provisions allows constructing the Figure 2.2, based on four pillars with a coordinating body.

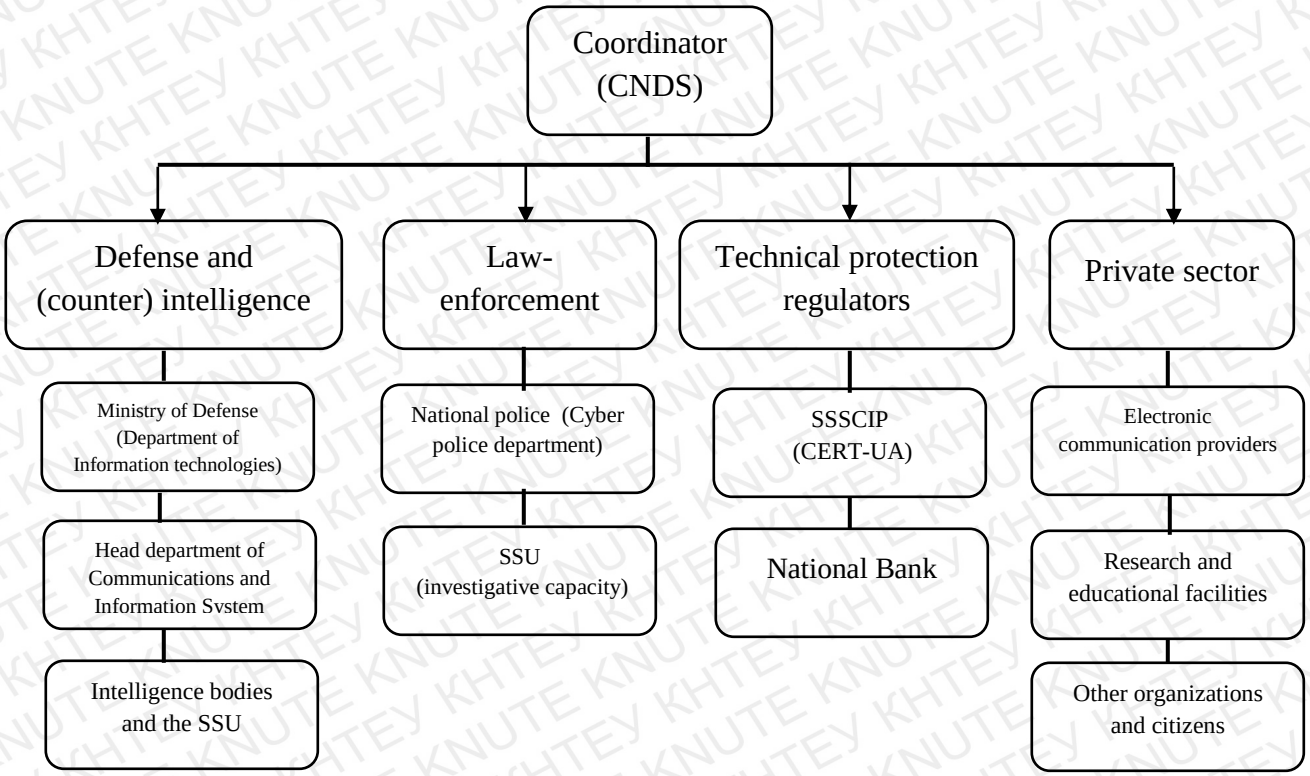

Figure 2.2. Organization system of cyber security in Ukraine

Source: composed by the author based on Streltsov, 2017

The Coordinator The Council of National Security and Defense carries out the coordination and control of the activity of the subjects of the Sector of Security and Defense that enforce the cybersecurity of Ukraine. The area-specific body of the Council is the National Coordination Center of Cybersecurity. Amongst its tasks are analysis of the state of cybersecurity and various parameters thereof; prognostication and detection of cyber threats; development, implementation and supervision of cybersecurity measures' propositions (including measures of information exchange between actors and measures of international cooperation), etc.

An example of the functions of the Center could be seen in its response to the `Petya` incident: the Center provided security recommendations to state establishments including their connection to a protected perimeter.

Defense and (counter) Intelligence Structures. The Ministry of Defense and the General Staff of the Armed Forces represent the military structures of this pillar. Their main tasks in the area of provision of cybersecurity are repelling military aggression in cyberspace; military cooperation with NATO in the areas of cybersecurity and mutual protection from cyber threats; cyber protection of informational infrastructure of the armed forces. For intelligence bodies the main cybersecurity tasks are: counterintelligence and investigative measures aimed at fighting with cyberterrorism and cyberespionage, evaluation of the preparedness of key infrastructure objects to possible cyber incidents; reaction to cyber incidents in the area of national security, etc.

Law-Enforcement Bodies. One key actor of this group is the Security Service of Ukraine, acting in its law-enforcement capacity. In this capacity, its functions in the area of cybersecurity are investigation of incidents connected to state information resources and other information that requires protection, of key informational infrastructure. The Service furthermore is tasked with prevention, identification, stopping and solving cybercrimes against the peace and security of humanity, or those, the consequence of which directly creates a threat to vital interests of Ukraine.

Technical Protection Regulators. This group is mainly represented by the State Service of Special Communication and Information Protection. Its tasks are forming and implementing state policy, state control of cyber protection of state information resources and other information that requires protection, of key informational infrastructure. The structure of the Service includes a specialized division, CERT-UA (Computer Emergency Response Team of Ukraine), which is directly responsible for counteracting the most serious cyber threats to the state with technical means.

The Private Sector. Although the Strategy does not directly give instruction to private sector actors, it does speak of the necessity to create the conditions for their participation in the following capacities. The first type of actor here is organizations that carry out activity in the area of electronic communications, information protection and/or are owners (managers) of key infrastructure objects. These organizations are to take part in the provision of cybersecurity of Ukraine, namely through obliging them to implement protection measures and to cooperate with state bodies in their respective tasks in the given area. Another form of participation of non-state bodies is the involvement of scientific and research organizations, educational facilities (as well as other organizations, public associations and citizens) in development and implementation of cybersecurity measures.

Unfortunately, the area of public–private partnership is only at an early stage of its development. As noted by D. Dubov, particularly with regard to the research and scientific aspects of it, Ukraine is severely lacking efficient specialized research institutions of the cybersecurity area (Dybov, 2014, p.255). Furthermore, if we speak of the aspects of cooperation between state bodies and business oriented organizations, the legal framework of such cooperation is also something that requires much work before it can properly function. At the same time, it is worth to note that these problems are not intrinsic only to Ukraine—questions of the functioning of public–private partnership are debated even in states with the most developed legal systems (Streltsov, 2017).

2.2. Cyber security assessment of Ukraine and its issues

Cyber security is named to be one of the most challenging and important risks around the world recent years. According to researches of World Economic Forum, cybersecurity takes leading positions between such risks as Economic, Environmental, Geopolitical, and Societal. In context of long-term risks, cybersecurity gives its place only to environmental challenges.

Cyber threats is a big challenge for businesses, which are main operators of states ***economies***. Another assessment of Allianz Risk Barometer, 2019, Business interruption and cyber incidents are tied at the top of the ranking at 32% (Allianz, 2019) and trend stay positive from 2015.

Table 2.2

The five biggest risks for small businesses with trends
(<250 m EUR of annual revenue)

№		2015	2015	2017	2018	2019
1.	Cyber incidents (e.g. cybercrime, IT failure, obsolescence, data breaches, penalties and offences	18%	24 %	25%	30 %	32%
2.	Changes in legislation and regulations (e.g. trend and tariff war, economic sanctions, anti-racism, Euro Zone disintegration, Brexit)	32%	28 %	26%	22 %	30%
3.	Natural disasters (e.g. storms, floods, earthquakes)	26%	25 %	28%	28 %	27 %
4.	Market development (e. g. volatility, intense competition / new market entry, mergers and acquisitions, market fluctuations	25,5%	28 %	26%	27 %	27%
5.	Business interruption (including supply chain disruption)	35%	31%	30%	33%	26%

Source: Allianz Risk Barometer, 2019

In addition, for Ukraine cyber threat must be in top five list of national risks, especially after the 2014 when Ukraine was faced with Russian aggression in the South of Ukraine. At the same time, the list of threats to the state's information security, as set out in the Doctrine of Information Security of Ukraine of 2017, is not exhaustive. In particular, the by-law does not take into account such threat to the national security

in the sphere of information interests as the information expansion of the aggressor state and its controlled structures. Such threat is currently defined by the term “hybrid war”, which is actually used to characterize the current state of information security in eastern Ukraine (Chyzhmar, Dniprov, Korotiuk, Shapoval, Olga Sydorenko, 2020).

It is vital to emphasize that statistics in the Ukrainian cybersecurity industry is a real deficit. It is hardly to find a structure or agency, which collects reliable information. If the statistics are relevant and true, it is spreaded only among the respondents themselves, and not available to general public. In this paper, the statistics and graphs will be taken from international organizations and agencies.

One of the most reliable indexes, which is concerned cyber security, is Global Cyber security Index (GCI). The GCI is designed to encourage the development of international cyber resilience among ITU member states. It focuses on domestic cyber resilience and is based on member-states’ self-assessments. Countries were assessed by following 5 pillars: Legal, Technical, Organizational, Capacity building, Cooperation (Global Cybersecurity Index Report, 2018). More about pillars in Annex E.

In 2018 Ukraine is not in the last place among the post-Soviet states, however, it is also difficult to state the level of information security in the country (Table 2.3).

Table 2.3

Post-Soviet states in the Global Cybersecurity Index, 2015, 2017, 2018

Country	Index	World Rating, 2015	Index	World Rating, 2017	Index	World rating, 2018
Georgia	0,5	12	0,819	8	0,857	18
Russia	0,5	12	0,788	10	0,836	26
Belarus	0,176	23	0,592	39	0,578	69
Azerbaijan	0,529	11	0,599	48	0,653	55
Ukraine	0,353	17	0,501	59	0,661	54
Moldova	0,382	16	0,418	73	0,662	53
Kazakhstan	0,176	23	0,352	83	0,778	40
Tajikistan	0,147	24	0,292	91	0,263	107
Uzbekistan	0,147	24	0,277	93	0,666	52
Kirgizstan	0,118	25	0,270	97	0,254	111
Armenia	0,176	23	0,196	111	0,495	79
Turkmenistan	0,088	26	0,133	132	0,115	143

Source: Global Cybersecurity Index Report, 2018

In 2018, Ukraine with the score of 0,661 takes the 54th place in the world, which is not a quite positive perspective for European county. According to GCI, Ukraine belongs to countries who have medium level of commitment to their cyber security issues. It means that they have developed complex commitments and engage in cybersecurity programmers and initiatives. Ukraine is among such countries as Uzbekistan, Moldova, South Africa, Cyprus, Nigeria, Azerbaijan, Mexico etc. The position of Ukraine among other countries is illustrated in Annex F.

In the graft, the score is increasing from year to year, which means that slowly but confidently Ukraine is moving towards development of cyber security capacities. In 2015, Ukraine took 70th place in the worldwide, in 2017 – 58th place, in 2018 - 54th place, which shows the positive trend.

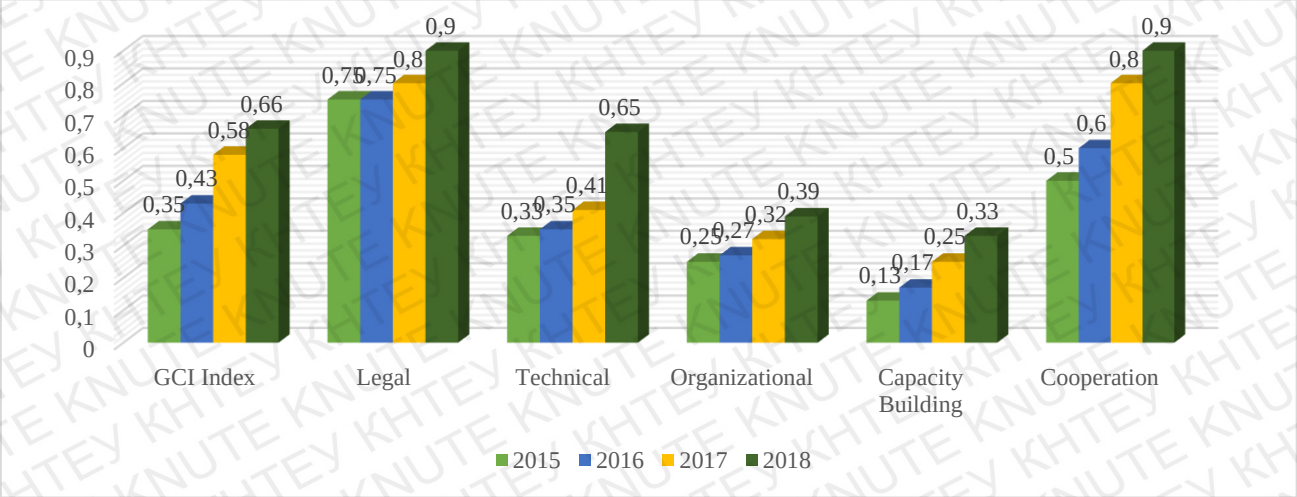

Figure 2.3. Ukraine: Cybersecurity Index and Key Components

Source: Global Cybersecurity Index Report, 2018

In addition, according to the graft, the lowest component of Ukrainian GCI is capacity building. This indicator is intrinsic to the first three pillars: legal, technical and organizational. To raise capacity building, it is important to promote public awareness campaigns, framework for certification and accreditation of cybersecurity professionals, provide professional training courses in cybersecurity, educational programs or academic curricula, etc. Cybersecurity is the most often tackled from a

technological perspective even though there are numerous socio-economic and political implications.

Another well-known Index, ***The ICT Development Index (IDI)*** has been produced and published annually by ITU since 2009. It is a composite index that combines 11 indicators into one benchmark measure. It is used to monitor and compare developments in information and communication technology (ICT) between countries and over time. The report features key ICT data and a benchmarking tool to measure the information society, the ICT Development Index (IDI). It also presents a quantitative analysis of the information society and highlights new and emerging trends and measurement issues.

In 2018, Ukraine took the 79th place among countries which shows low development of information and communication technologies. In the graph below, It is illustrated the comparative analysis of two indexes: IDI and GCI.

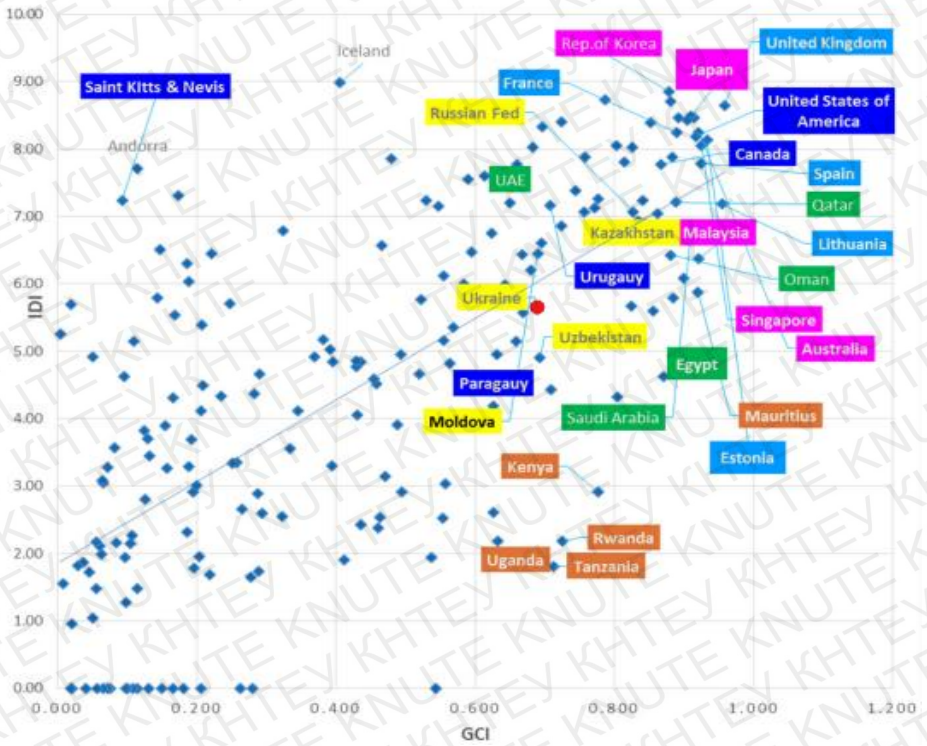

Figure 2.4. Comparative analysis of IDI and GCI in 2018

Source: Global Cybersecurity Index Report, 2018

Figure 2.4 shows that not all countries with high IDI scores have a similarly high score in GCI. For instance, Iceland took the top place in IDI scoring 8.98 while only 0.406 in the GCI. Andorra, and Saint Kitts and Nevis, also score high in IDI and yet very low in GCI, although some countries are maintaining their leading positions in both indices. Countries marked in yellow are Post-Soviet states. Considering Ukraine, this graph shows that GCI is higher than IDI. In order to IDI be effective and resilient, cybersecurity needs to be implemented and regularly updated to reflect the changing needs.

The third index, which is vital to be consider, is ***National Cyber Power Index (NCPI)***. The overall NCPI assessment measures the "comprehensiveness" of a country as a cyber-actor. Comprehensiveness, in the context of NCPI, refers to a country's use of cyber to achieve multiple objectives as opposed to a few. The most comprehensive cyber power is the country that has (1) the intent to pursue multiple national objectives using cyber means and (2) the capabilities to achieve those objective(s).

The below formula is used for calculation:

(1.1)

$$\text{National Cyber Power Index (NCPI)} = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

Ukraine was referred to the `Lower Intent, Lower Capability` countries. Countries that fall into this category either are not actively developing the capability and intent to project power in cyberspace, or have not published (or had published about them) a sufficient amount of information on their cyber strategy, cyber-attacks attributed to them, or capabilities used to measure cyber power in this study (National Cyber Power Index (NCPI, 2020).

To sum up, It was conducted a comparison of Indexes in 2018 into one graph. The conclusion could be made that Ukraine is considered not be a strong country in term of cyber security. It is important to improve all aspects of security and to develop the strong ICT to be competitive in cyber space in the global market.

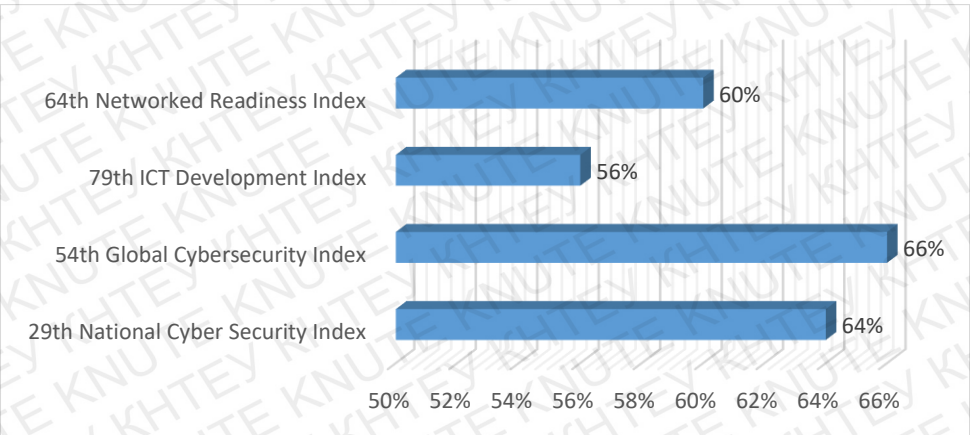

Figure 2.5. Comparison of fulfilment percentages of indexes in 2018

Source: created by author based on GCI, 2018 and NSCI, 2020 reports

Like any branch of government regulation, cyber security requires government funding. Therefore, this sector needs significant infusions. Cybersecurity is an integral part of the entire system of ensuring the National Security of Ukraine, and therefore its functioning takes place in many spheres of state power.

To clearly understand how well security sector of Ukraine is funded, it is necessary to analyze the budget classification of expenditures by programs. According to the Budget Code, software classification of expenditures and budget lending is used for implementation program-target method in the budget process. Such a classification expenditures and crediting of the state budget and local budget developed by the Ministry of Finance of Ukraine and by local financial authority on the proposals submitted by the main managers of budget funds under time of drafting the law on the State Budget of Ukraine or the draft decisions on the local budget, if it is a question of local self-government, in budget requests.

Program classification of expenditures and lending to the local budget is formed taking into account the typical program classification of expenditures and lending to the local budget, which is approved by the Ministry of Finance Of Ukraine.

It was considered the budget classification of expenditures by programs for the period from 2015 till 2019. This table shows general information about expenses State Budget of Ukraine, which include expenditures from the general and special funds of

the state budget. The largest part of the state budget, and this more than 90%, is the general fund. The funds of the general fund are intended for providing financial resources for general expenditures, those that are not aimed at a specific goal. The special fund provides for the purposeful use of budget funds - respectively for funding specific goals.

Table 2.4

Expenditures according to the program classification of expenditures and crediting of the state budget in the period from 2015 to 2019, billions of hryvnias

Code of budget classification	Indexes	Plan for 2015, taking into account the changes	Plan for 2016, taking into account the changes	Plan for 2017, taking into account the changes	Plan for 2018, taking into account the changes	Plan for 2019, taking into account the changes
1000000	Minister of Internal Affairs of Ukraine	31,4	40,541	48, 299	60,26	73,403
1007000	National Police of Ukraine	-	16,001	19,706	24,26	29,485
3601230	Cyber protection of the information and telecommunication system of the staff of the Ministries of Justice of Ukraine				8,4	
6500000	National Security and Defense Council of Ukraine	0,0603	0,0707	0,128	0,156	0,177
6520000	SBU	4, 436	5,414	6, 624	8,08	9,914
6640000	Administration of the State Service for Special Communications and Information Protection of Ukraine	0, 663	0,943	1,794	2,27	2,907
	Total for security	36, 575	62,969	76, 553	9,503	115,888
	Percentage, %	6,595	9,729	9,968	10,491	11,794
	Total expenditures	554,591	647,222	767,983	905,892	982,6

Source: Created by author based on data from The State Treasury Service of Ukraine

In this table, it is illustrated the amount of public funding for budget programs. These indicators determine only the total cost of a program. Each program includes in some percentage of the scope of cybersecurity. It is worth paying attention to the expenditures of the state budget of Ukraine for functional classification in 2018. Defense spending, which includes cybersecurity, was 8.84% of the total fund. In addition, form year to year the percentage of defense expenditures is increasing, however, it is still don`t enough to build a capacity with will be competitive in the international market.

Conclusions to part 2

Unfortunately, in Ukraine, cybersecurity is not sufficiently developed, which requires adopting the experience of cybercrime prevention in the advanced countries of the world. The main directions should be the development of new cyber police, promotion of international cooperation between different authorities in combating crimes committed using information technologies, training of specialists in cybersecurity areas, etc.

In addition, the system of main actors of cyber security space in Ukraine is not well structured. Organizations have different domains and priorities, and they rarely collaborate on common problems.

At the same time, the cybersecurity of Ukraine requires more and strengthened cooperation between international law enforcement agencies, private sector companies, academia, and other relevant concerned parties. It is very important that law enforcement agencies could cooperate with the Internet security industry to restrict criminal activity and source of its income from information crimes.

Law enforcement agencies should continue to explore the possibility of investigations, analytics, and police emerging from new technologies to in order to develop ICTs. Such tools will be invaluable for combating modern crime and for intelligence police.

PART 3. DIRECTIONS OF IMPROVING THE LEVEL OF NATIONAL CYBER SECURITY IN THE CONDITIONS OF GLOBAL COMPETITION

3.1. International cooperation as a direction of cyber security of Ukraine

As was discussed in previous two paragraphs, the question of improving cyber space is underlined by many international organizations. It is vital to emphasize that it is a global problem, which requires global actions. Cyberattacks are becoming more organized, coordinated and disruptive to the economy and critical infrastructure of government agencies and corporations, so they can reach a critical level which threatens national and Euro-Atlantic prosperity, security and stability.

Under these conditions, the key issue of all countries, even continents, of the world is to provide actions which drastically minimize (and, in some cases, eliminate) the disruptive effects of cyber criminals. One of the key global organization which is becoming a pioneer in cyber security is The North Atlantic Treaty Organization (NATO). It plays a significant role in establishing a cohesive approach to information security as part of national security. The range of potential uses of cyber technologies presents one of the main challenges for NATO considering its role in providing cyber security to Allies and Partners. Admittedly, given the potential damage of cyber threats to national security, the cyber defense has now become one of top NATO’s priorities.

The new NATO Strategic Defense and Security Framework adopted by the Heads of State and Government at the NATO Summit on 19 November 2010, effectively leveled cyber threats to military force, which, in turn, allows for a comprehensive cyberattack through the use of national armed forces. Cyber security was described as the second most significant NATO priority. NATO’s Cyber Security Policy, in effect, states cooperation with partner countries in developing an Alliance cyber protection network as a key mechanism for NATO's cyber security efforts (The North Atlantic Treaty Organization's, 2020).

The final recognition of the Cyberspace Alliance as an operational area for warfare was the result of the NATO summit held in Warsaw, Poland on 8-9 July 2016 (The Cyber police of Ukraine, 2020).

The countries of NATO spends millions of dollars yearly for defense. Protection is one of the main target of the Alliance. It is not mention in the Figure 3.1 but The USA spent 730149 million of dollars in 2019. This is a country which spends the most for its defense. Ukraine respectively spent 2110 million dollars in 2016 and 4080 in 2019 for its defense regardless the fact that the combat action is taking place on the territory of Ukraine since 2014. In Annex G the statistics of expenditures is illustrated.

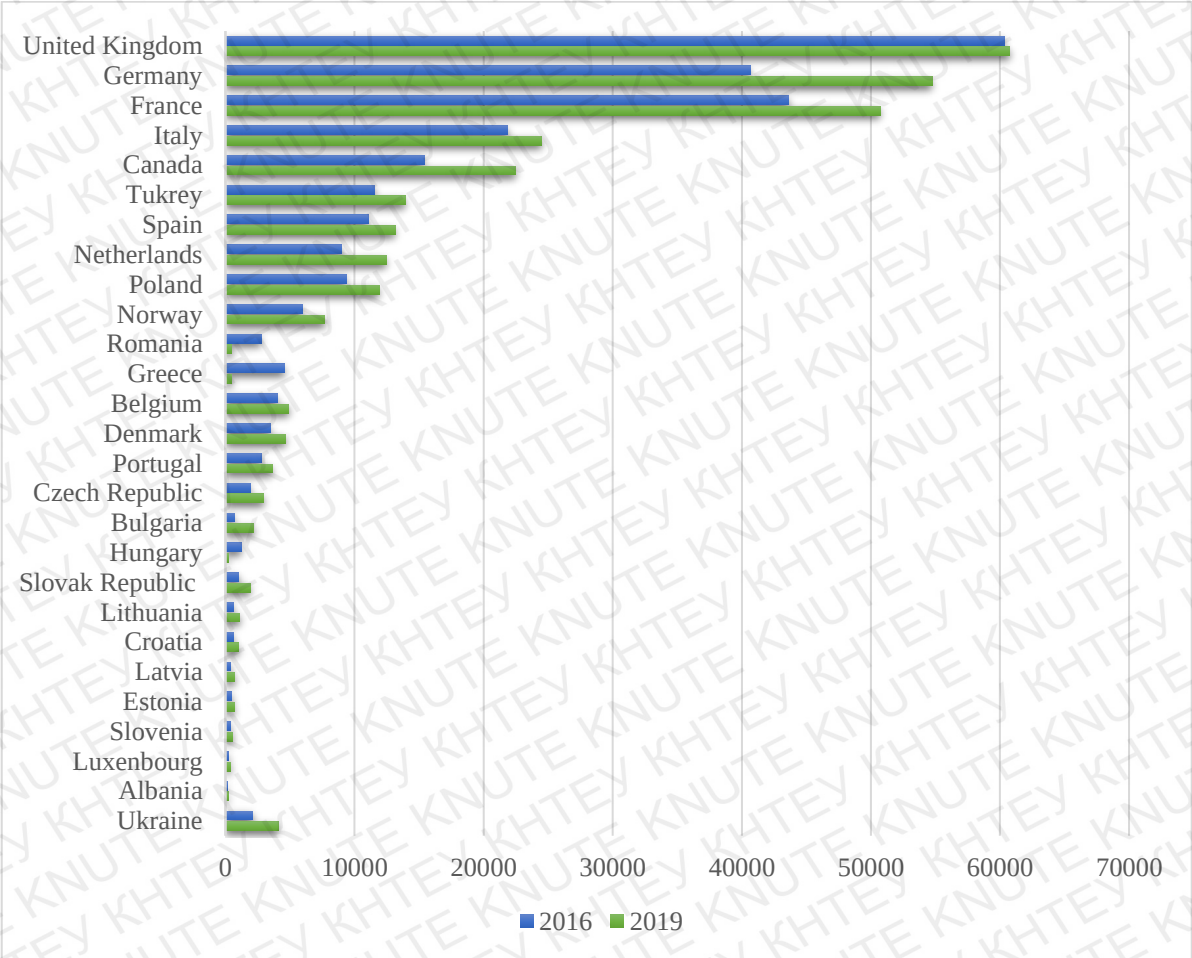

Figure 3.1. Estimated military spending of NATO European countries in 2016, 2019 (in million U.S. dollars)

Source: Statista, 2020

The role of NATO in cyber security can be divided into *two specific components*. The goal is the security of their networks, which was decided by the Allies at the NATO Summit in Newport, Wales, on 4-5 September 2014. Given the Alliance's widespread presence on the Internet, this role is too difficult. Consequently, NATO must secure all information and communication systems that are crucial for Alliance operations and missions in cyber domain. The second goal of NATO is to support its member countries in improving of their cyber defense capabilities (The Cyber police of Ukraine, 2020).

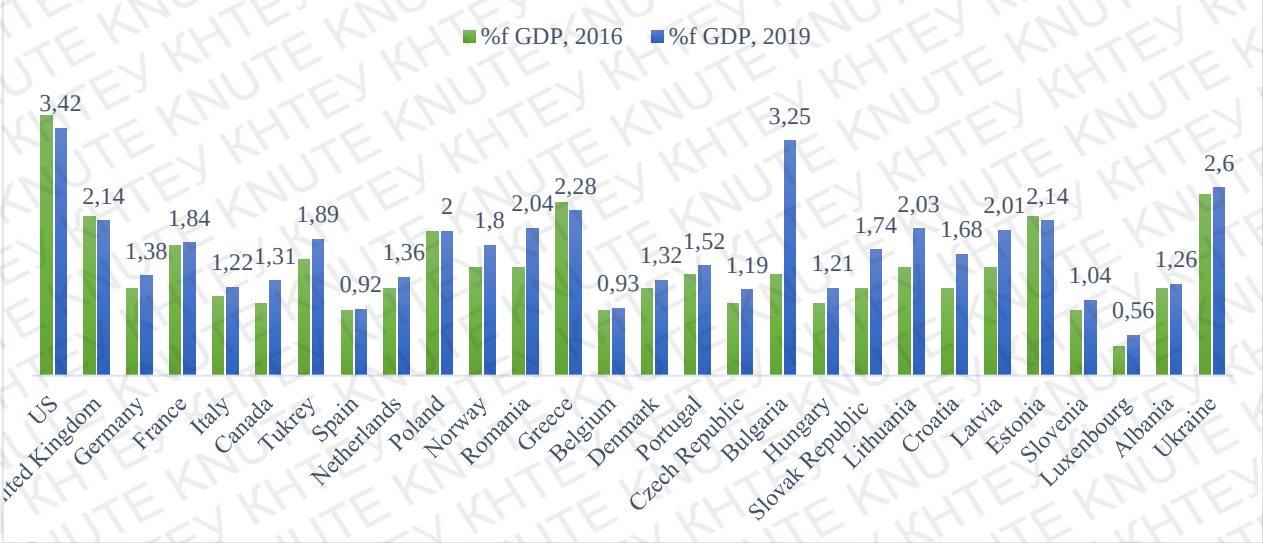

Figure 3.2. Comparison of share of NATO European countries defense expenditures in GDP in 2016 and 2019, %

Source: Statista, 2020

In Figure 3.2, the share of NATO European countries defense expenditures in GDP in 2016 and 2019 is illustrated. Compared to European countries Ukraine spent 2,6% from GDP to its defense. It is vital to note that expenditures raised in 2019. This positive trend will lead to increasing cyber defense expenditures. More in Annex H.

As it was researched previously, currently Ukraine faces an important problem of establishing a national cyber security infrastructure, which is capable of counteracting cyber threats to national security. The state of cyber security in Ukraine indicates that cyberspace remains a significantly vulnerable part of national security and remains highly susceptible to cyber threats.

Following international agreements, Ukraine cooperates in the area of informational security with foreign nations, their military forces, law enforcement agencies and special services, as well as with international organizations. Thus, Ukraine's strategic relationship with the North Atlantic Treaty Organization supports the objectives of international cyber security cooperation.

In January 2008, NATO adopted the Alliance's cyber policy framework, recognizing the effect of cyber-attacks on Estonia in October 2007, when government websites and other Estonian communication networks were disrupted. This led to a concerted effort by all NATO countries to improve cyber defense and information security. Consequently, NATO allies agreed on Memorandum to create an international NATO information defense center in Tallinn (Estonia).

In 2008, on the initiative of the Security Service of Ukraine, NATO-Ukraine Joint Working Group on Military Reform set up a working sub-group on cyber defense. This sub-group provided an impetus for the establishment of conceptual mechanisms for cooperation between Ukraine and the North Atlantic Alliance in consultation and exchange of information on cyber security. In 2009, the Alliance adopted a strategic document, "A Framework for Cooperation on Cyber Security between NATO and Partner Countries", which established a political and legal framework for collaboration and cooperation with partner countries, including Ukraine.

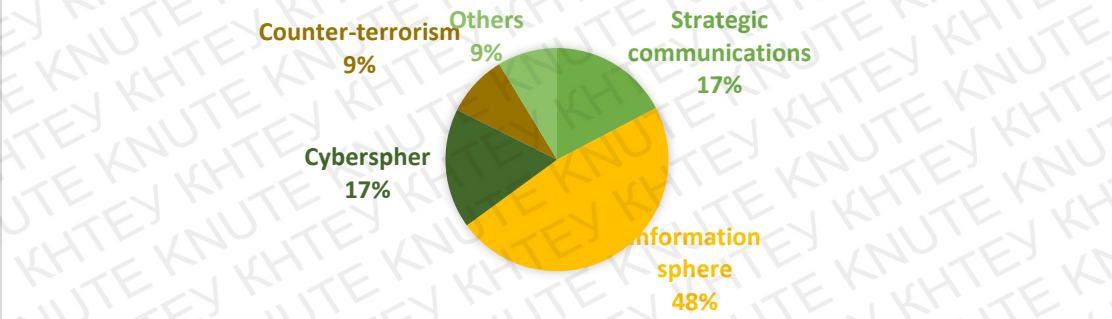

Figure 3.3. Key areas of Ukraine-NATO common countering to hybrid threats

Source: Kondrad Adenauer Stiftung, Synerging Energies report, 2019

The ***key objectives*** of cooperation between NATO and its partners in the field of cyber security are:

- to ensure the normal functioning of critical information and communication infrastructures;
- to establish effective measures to combat cyberattacks;
- to assist countries in restoring the proper functioning of the related infrastructure as a result of external cyber-attacks;
- implementation of a mechanism of prompt response to cybersecurity threats.

Presidential Decree No. 744/2014 of 24 September 2014 put into force the decision of the National Security and Defense Council of 28 August 2014 on urgent steps to protect and improve Ukraine's defense capability, which states that Ukraine's priority national interest in foreign policy is to further establish Ukraine's strategic partnership with the US, the EU and NATO. More in Annex K (Ukrinform, 2017).

One of the important field of activity of Ministry for development of Economy, Trade and Agriculture of Ukraine is economy of defense and security of Ukraine. The cooperation of Ukraine with NATO is included into this field. All documentation, which describes the work of Ukraine with NATO, can be found on the official website of the Ministry. In the framework of the agreements reached between Ukraine and NATO, a joint decision was taken to set up five trust funds for our country, with the fifth fund designed to fight cybercrime and to build cyber defense systems in line with the most progressive standards of NATO member countries. Estonia, Romania, Turkey and Hungary have contributed to the Campaign. The concept behind the formation of the NATO-Ukraine Cyber Security Trust Fund is that its intellectual and material capabilities would provide Ukraine with the requisite support solely for the advancement of defense technological capabilities, including the establishment of cyber incident investigation laboratories. The main goal of this Trust Fund initiative is to coordinate NATO member countries to support Ukraine in developing its cyber security

capability by providing hardware and software, software, technical assistance, advisory services and training.

The North Atlantic Treaty Organization supports not only with international cooperation and training but also with financing for cyber security development of Ukraine. The NATO trust funds for support of Ukraine include the separate clause for cyber defense development in accordance with the most progressive standards of NATO member countries.

The financing was divided *into two phases*:

I phase: Contributions - 965 thousand euros and the cost of training courses (a total of 1 million 65 thousand euros).

Such countries as Albania, Romania (+ advisor from 2016 to April 2018), Estonia (contribution in the form of training courses for € 100 thousand), Portugal, Turkey (+ advisor, until 2016), Hungary, USA (contribution in the form of training courses), Italy became partners in supporting of cyber security defense of Ukraine. .

In July 2017, the first phase of the program was completed. Ukraine has been provided with technical equipment and software for the establishment of CBU and Computer Communications in the Security Service of Ukraine and the State Special Services.

Phase II: Funding requirements will be determined separately.

The NATO Trust Fund offers an opportunity to boost the level of cyber security in Ukraine by consulting information security experts, developing the basic principles of the National Cyber Security Framework, working in NATO-Ukraine expert level boards in cyber security area.

Ukraine is therefore consolidating its efforts on implementation of NATO standards to be fully integrated to the global cyber defense framework. Nevertheless, the process of joining the collective security system is still slow, indicating that the current cyber capabilities not in line with NATO requirements (On the Cybersecurity Strategy of Ukraine, 2016).

2. Forecast assessment of the effectiveness of the proposed measures to increase national cyber security

In order to make a forecast, firstly, it is vital to consider all security risks through the prism of SWOT analysis. SWOT is an acronym for Strengths, Weaknesses, Opportunities, and Threats. SWOT analysis is a framework for strategic planning, opportunity analysis, competitive analysis, business and product development.

Table 3.1

SWOT –analysis of Ukrainian cyber-security space

STRENGTHS 1. High concentration of information well-educated employees 2. Cyber security policy development 3. The involvement of Ukraine into International communication with Cyber defense organization 4. Availability of Cyber Security strategy	WEAKNESSES 1. Weak legislation 2. Weak Cyber Security strategy 3. Weak collaboration of National agency on common problems. 4. Low awareness of society about the importance of cyber threats 5. The Russian penetration in the East of Ukraine (which effects cyber aspect as well) 6. Not improving the communication with international agencies 7. Low capacity 8. Low financing of cyber security issues. 9. Limited links between business and academia 10. Lack of accreditation for suppliers to SME and consumer buyers
OPPORTUNITIES 1. Increasing cooperation with international funds and organization 2. Digital transformation 3. To retrain Ukrainian IT resources into cyber security and defense resources 4. Increasing the financing of cyber security funds 5. Legislation improvement.	THREATS 1. Well-funded Global Competition 2. Lack of clarity in regulations for emerging technologies 3. The Russian aggression in the East of Ukraine including informational penetration 4. Coronavirus

Source: created by the author

Based on the researched weaknesses and threads, it will be described below the key recommendation according to improvement of current situation in cyber space.

1. **To improve organizational structures.**

Ukraine have national structure, which is responsible for cyber security in different aspects. However, the great disadvantage that these agencies have different domains and priorities, and they rarely collaborate on common problems.42

On the figure 5, it was proposed the organization system for Ukrainian cyber security defense. 44 The center of cyber (State Agency of Cyber Security) security should be established. CERT-UA, SSSCIP, Ministry of Internal Affairs of Ukraine, Ministry of Defense of Ukraine, Security Service of Ukraine, and SBU should directly over to State Agency of Cyber Security. It is proposed to be a center as it should be an organization that works exclusively on cyber security issues and coordinate the work of all other center.

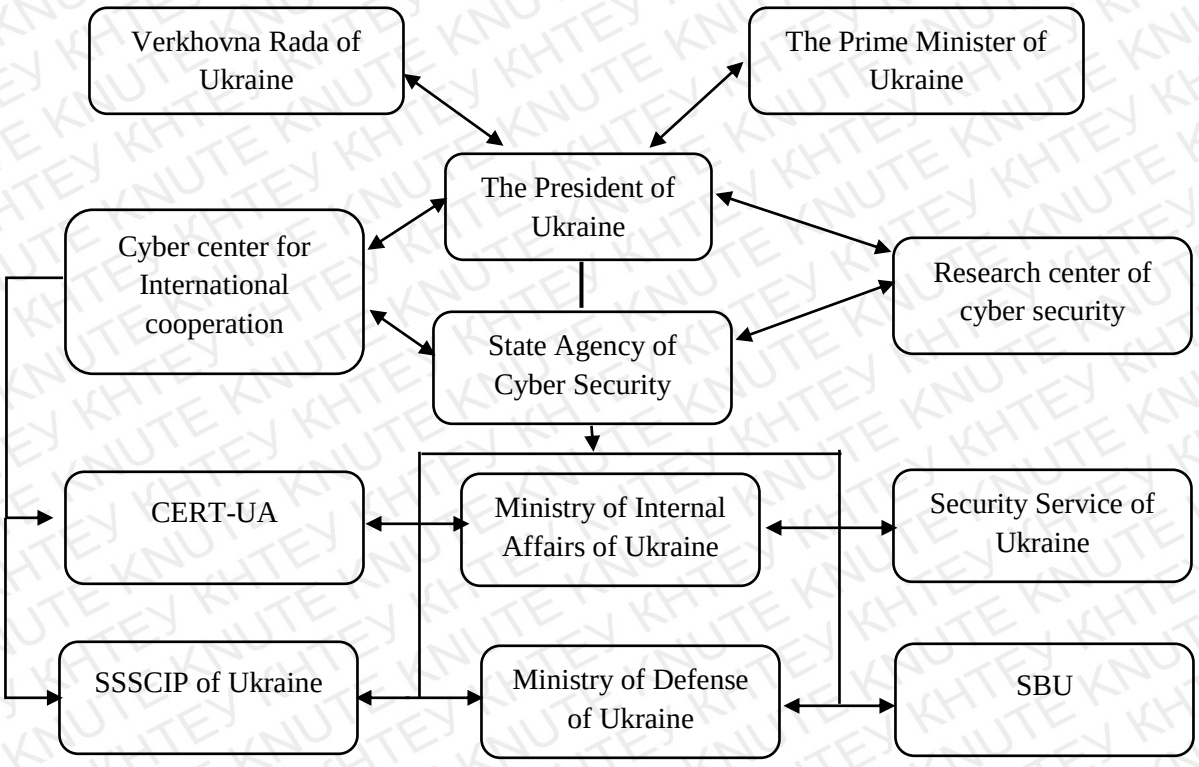

Figure 3.4. Proposed organizational structure of cyber system of Ukraine

Source: created by the author

Main activities of State Agency of Cyber Security should include: interaction with the administration domain UA., protection of state information resources,

interaction with state authorities, international cooperation in the protection of information resources, unified antivirus protection system, and determining the level of protection of information and telecommunication authorities' systems, making Cyber Security strategies and prognosis. In addition, the new research center is proposed to be established. The main responsibilities should include collecting the Ukrainian cyber statistics, increasing the awareness s of cyber accurate among the society, training and developing cyber specialists etc. Cyber center for International cooperation should be responsible for developing international cooperation on the global market and increasing the reputation of Ukraine as a country with developed cyber security system.

2. To establish proper legislation.

Regardless the fact, that the level of cyber security of legislation is considered to be the strongest point in Ukrainian cyber security but our country is still making steps towards creating conditions for proper protection of the information space of the state, specialized normative legal acts are adopted, entities responsible for formulating and implementing state policy in the information sphere, etc. are in place.

The legislation should cover all aspects of cyber issues with accordance to International legislation.

3. To develop a strong Cyber Security Strategy.

The global cyber security market size was valued at USD 156.5 billion in 2019 and is expected to expand at a compound annual growth rate (CAGR) of 10.0% from 2020 to 2027. Cyber security and defense against online threats undertake greater significance in today's digital changing landscape. It has become vital amid organization due to rapidly increasing frauds, cybercrimes, risk, threats, and vulnerabilities. Disruptive and emerging technologies in banking, retail, information technology, defense, and manufacturing sectors have offered new capabilities, facilitated automation, and offered ease of working in the recent past. However, these technologies have also emerged as a potent factor in the development of the global

threat landscape of exploits, vulnerabilities, and malware. The emerging threat landscape is observed with an increased number of cybercrime activities in the global digital era (Grand view Research, 2020).

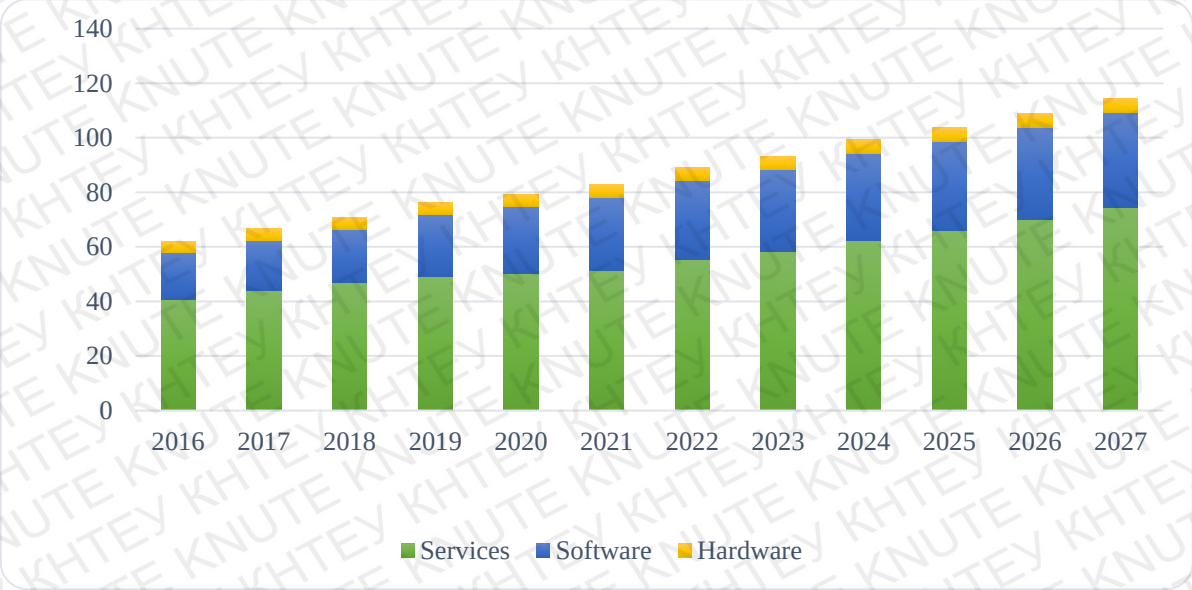

Figure 3.5. U. S. Cyber security market size, by component, 2016-2027, USD Billion

Source: Grand view Research, 2020

In the Figure 3.4., It is illustrated the increase if cyber security market of the USA. Our state should take actions in order to be up-to-date in the cyber security market. Ukraine is making steps towards establishing a clear vision of steps how to prevent cyber-attacks. However, National strategy doesn`t cover all key aspects that is why such necessary steps weren`t made. Following recommendations if adhered, while formulating or revising the cyber security strategy can help mitigate cyber risks to the national cyberspace. More about cyber market in Annexes L - N.

State Agency of Cyber Security should be responsible for making strategy. It should clearly define the scope, objectives and definitions of major key terms in the document in accordance with the country's actual threat landscape. Redefine the words "critical infrastructures" in the strategy because the existing definition i.e. "infrastructures that adversely affects the national economy and security when

compromise", leaves many critical computer networks out of the scope of critical infrastructures.

Include input from all national stakeholders; government, military, telecom providers, financial institutions, judiciary, civil society, religious leaders, and cyber security experts on domestic cyber security strategy or action plans:

- support the strategy by articulating a comprehensive plan of cyber actions, with clearly defined stakeholders, authorities, accountabilities, milestones; investments, outcomes etc.;
- emphasize on the need of reforming national legal framework, in the strategy, to effectively deal with cyber-criminals and offenders;
- ensure that there are effective technological controls for people, management, facilities, operations in place, at all levels;
- lay stress on the need of establishing information sharing framework to effectively share information regarding security incidents and breaches between the government and private sector;
- in the strategy, clearly define tasks and responsibilities of the CERTS/ CSIRTS from disseminating information about security advisories and cyber breaches to raising cyber awareness and forensically responding to cyber incidents, etc.;
- recommend various educational and training programs, cyber security toolkit etc., in the strategy, for netizen's self-training and raising cyber awareness in the country;
- encourage the development and promotion of indigenous security services and products;
- give advice on reinforcing private-public partnership to ensure continued cyber resilience of the national cyberspace;
- propose acceptable cyber norms in the strategy document to increase international collaboration and prevent cyber warfare in the future.

4. To raise financing of cyber funds.

In the Figure 3.6, it is illustrated the position of Ukraine concerning financing of defense industry comparing to some countries. Regardless the fact that on the East of Ukraine military operations are taking place because of Russian aggression since 2014, on the 2017, Ukraine had the smallest expenses for national defense (investment in cyber security is a small percentage from the overall defense expenses).

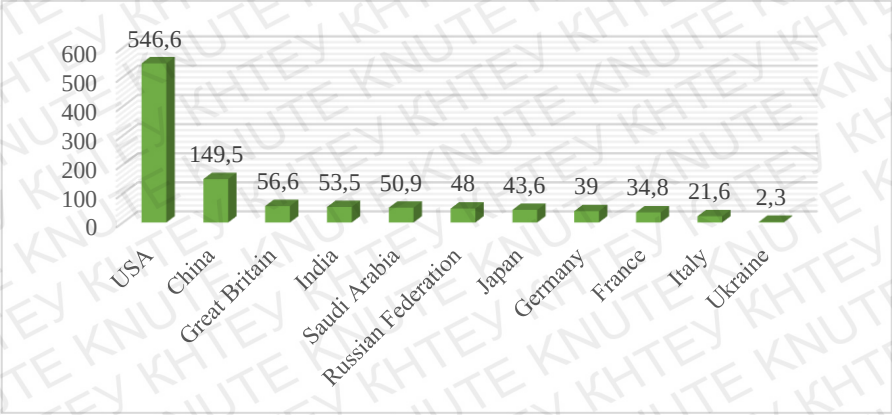

Figure 3.6. Military budgets of countries around the world in 2018 compared to Ukraine, billions of dollars

Source: Romanovskaya, Urbanovich, 2018

It is absolutely clear that the current budgeting of defense is not enough to establish a competitive cyber infrastructure. In addition, it should be taken into consideration that our state doesn`t have a coordination center which can investigate, plan the directions of expenditures and control the flow of money. As it was investigated previously, NATO allocated financing particularly for cyber security in 2017. The great some of this financing was directed to the funds of the Ministry of Defense of Ukraine.

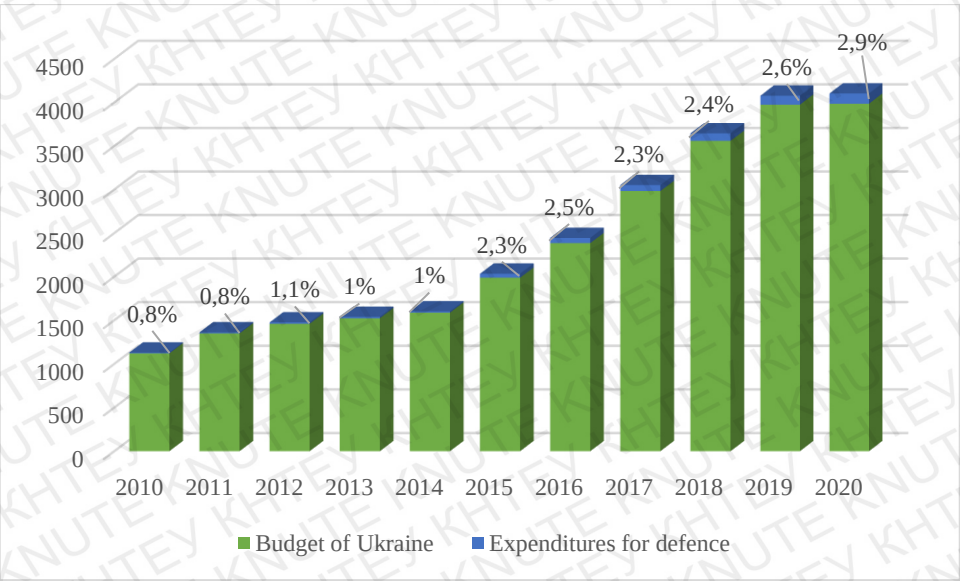

Figure 3.7. Share of defense expenditures from the general budge in 2010-2020, %

Source: Created by author based on data from The State Treasury Service of Ukraine

It was decided to investigate the trend of financing to the Ministry of Defense of Ukraine and to make a forecast of estimated funding in the coming years. There is no information in the public domain about the structure of budget; it should be taken into consideration that cyber security financing is a small part from the general budget. In the Figure 3.8, the forecast was performed with the smallest and the highest probability.

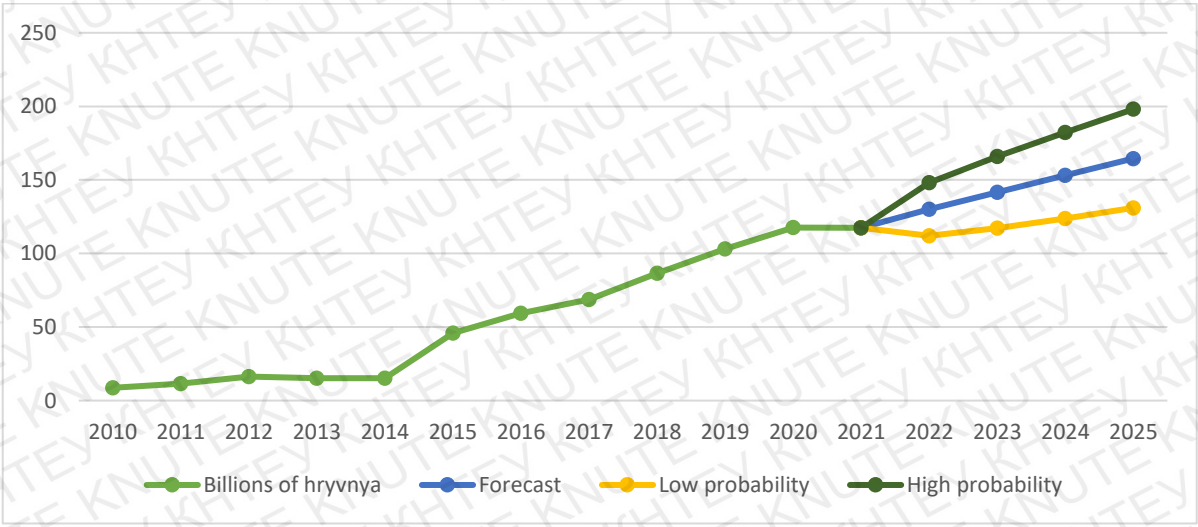

Figure 3.8. Forecast of financing of the Ministry of Defense of Ukraine for 2022-2025

Source: Created by author based on data from The State Treasury Service of Ukraine

The forecast was performed by Exponential Triple Smoothing (ETS) algorithm. According to it, the positive trend is expecting, it means that the financing of defense in Ukraine might increase. Even if trend with low probability will be taken, in 2023 the raise is expecting. The Ministry of Finance of Ukraine has already establish the budget for 2021, and it was declined from 117,6 to 117,5 billions of dollars. Because of the coronavirus crisis, the unstable politic situation and the Russian aggression in the East of Ukraine, the financing of cyber security might be postponed.

Table 3.2

Forecast of financing of the Ministry of Defense of Ukraine for 2022-2025

Period	**Forecast**	**Low probability**	**High probability**
2022	130,1037	112,03	148,18
2023	141,58481	117,26	165,91
2024	153,06592	123,78	182,35
2025	164,54703	131,02	198,07

Source: Created by author based on data from The State Treasury Service of Ukraine

In Table 3.2, the calculations of forecast are demonstrated.

5. To increase awareness of the cyber security issues.

It is not common to discuss the information security among Ukrainians. The existing problem in Ukraine, that we have lack of training and awareness of users and lack of coordination and cooperation between institutions and organizations. The increase of cyber accuracy will help to establish the process and systems if cyber security defense.

All these steps will help Ukraine to minimize cyber threats in country and to enter the global cyber security market. It is hard to predict when such important actions towards cyber security will be implemented. There are two important points such as COVID-19 and the Russian aggression on the East of Ukraine doesn't allow government to concentrate on the cyber problems or raise funds. Also, due to unstable political situation in Ukraine, we can hardly except the improvement in the near future.

Conclusions to part 3

All main weaknesses of cyber security system of Ukraine were identified, which include weak legislation, weak cyber security strategy, weak collaboration of National agency on common problems, low awareness of society about the importance of cyber threats, the Russian penetration in the East of Ukraine (which effects the cyber aspect as well), not improving the communication with international agencies, low capacity, low financing of cyber security issues, limited links between business and academia and lack of accreditation for suppliers to SME and consumer buyers.

One of the main direction which is required for improving cyber sphere is cooperation with international organization. More developed countries has already established advanced cyber security strategy. The next step is international strategy and cooperation as cyber security is a global issue. There are a plenty of cooperations, which formed such organization such as ITU, ISACA, NATO, HLEG. Some of that working with cyber security as a part of all their strategies, other are directly related to cyber issues.

One of the main direction of Ukraine is cooperation with NATO. Ukraine needs a cyber-security system interoperable with NATO-EU partners; the protection in cyberspace is an integral part of national security.

Ukraine is improving its own cyber defense through the use of NATO's Information Security Trust resources, and the experience of members- countries. Countries provide Ukraine with training courses, help to raise budget and helping to develop a strong defense strategy.

Other recommendations about improving the level of cyber security in Ukraine is improving organizational structures, establishing proper legislation, developing a strong Cyber Security Strategy, raising financing of cyber funds, and increasing awareness of the cyber security issues.

Conclusion

Because more than half of the world society is currently online, the issue of security is becoming more and more important for the world population. As of October 2020, 59 % of individuals, equivalent to 4,66 billion people, were using the Internet. This is a significant step towards a more inclusive global information society but also an important need for increased cyber protection. Countries are developing strategies for protecting their national cyber sphere. As the holder of significant data and a provider of services, the Government can play the most important role and take stringent measures to provide safeguards for its information assets. The Government also has an important responsibility to advise and inform citizens and organizations what they need to do to protect themselves online, and where necessary, set the standards we expect key companies and organizations to meet.

The primary duty of the government is to defend the country from attacks by other states, to protect citizens and the economy from harm, and to set the domestic and international framework to protect interests, safeguard fundamental rights, and bring criminals to justice. Authorities need to be aware of all markets of cybersecurity to provide measures.

Cyber threats are hitting the society in different forms. For example, cybercrime, cyber espionage, hacktivism, cyber warfare. As cyber threats became a new international risk for all states around the world, the term `cyberterrorism` is becoming more popular and more popular. In general, cyberterrorism could be described as premeditated, politically motived attacks by sub-national groups or clandestine agents against information, computer programs, computer systems, and data that result in violence against non-combatant agents.

Cyber security is a current issues for individuals, businesses, governments, and even industries. Finance and banking spheres are number one as a target for cyber

criminals. Pharmacy, energy and technological companies are also potential priority targets.

In order to prevent such loss of information and money, authorities around the world allocated the four main directions of struggle: defense & intelligence, government, other than defense & intelligence, enterprises, SME and consumers. Counties develop exclusive National Cybersecurity Strategies in order to have a clear vision of future preventing actions. Governments are collaborating and formatting different alliance such as ITU, ENISA, NATO, and ISACA, which helps to assess the level of cyber security and to develop recommendations about strengthening of cyber defense. The assessment of cyber security is performed in a form of The Global Cybersecurity Index (GCI), National Cyber Power Index (NCPI), ICT Index, which help to identify the leading countries in this sphere and deficiencies in national cyber systems.

Ukraine, like its international counterparts, is taking gradual steps to create a secure information society and ensure security at all levels of the cyber environment. Our state, in accordance with relevant laws and regulations, are developing cybersecurity at all possible levels. The Government of the country has developed special documents regulating activities in the field of cyber security - Cyber Security Strategy of Ukraine, the Doctrine of Information Security of Ukraine of 2017. The legal basis for cybersecurity in Ukraine is the Constitution of Ukraine, the laws of Ukraine on the basics of national security, the principles of domestic and foreign policy, electronic communications, protection of state information resources and other laws of Ukraine. This also includes the Convention on Cybercrime and other international treaties approved by the Verkhovna Rada of Ukraine, decrees of the President of Ukraine and acts of the Cabinet of Ministers of Ukraine. Other normative legal acts adopted in pursuance of the laws of Ukraine are included.

Activities to ensure national cyber security are carried out by: the Ministry of Defense of Ukraine, the Security Service of Ukraine, the State Service for Special

Communications and Information Protection of Ukraine, the National Police of Ukraine, the National Bank of Ukraine and intelligence agencies. Each of them is assigned certain tasks in the prescribed manner and according to their competencies.

Unfortunately, Ukrainian cybersecurity is not sufficiently developed. Compared to development of cyber security around the world Ukraine takes middle positions. Considering European countries, Ukraine takes low positions. In addition, the system of cyber security in Ukraine is not well structured. Organizations have different domains and priorities, and they rarely collaborate on common problems. Such indicators as capacity building, technical and organizational should be a priority for cyber development.

The main recommendations for improving the cyber space of Ukraine which were highlighted are to improve organizational structures, to establish proper legislation, to, increase awareness of the cyber security issues, to raise financing of cyber funds, to develop a strong Cyber Security Strategy.

Joint programs for many countries around the world in the process of developing the Cyber Security Strategy are identification management, risk management and cyber incident management and cooperation with international partners, including participation in various forums and conferences to transfer experience or accumulate experience, as well as joint programs to ensure cybersecurity. Ukraine currently joined to international organization, which ensure the participation in the global arena.

Ukraine has already establish a partnership with NATO in order to develop the cyber security system and defense. Considering the significant progress, mechanism of the Member States, Ukraine must become an active participant in these security processes. This cooperation will help to boost the reputation of the country and to establish the legal basis of national cyber security.

Thus, understanding the importance and urgency of ensuring mechanisms for implementing the cybersecurity strategy today is an integral aspect of the functioning of a healthy information society in Ukraine.

REFERENCES

Legislation:

1. Agreement on the Implementation of the NATO-Ukraine Trust Fund for Cyber Security between the Security Service of Ukraine and the Romanian Information Service from 23.07.2015 № 642_063. (2015). Retrieved from http://zakon.rada.gov.ua/laws/show/642_063 (assessed 20/11/2020) [In Ukrainian].
2. Constitution of Ukraine (1996). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
3. Decision of the National Security and Defense Council of Ukraine of March 4, 2016 "On the Concept of Development of the Security and Defense Sector of Ukraine" (2016). Retrieved from https://zakon.rada.gov.ua/laws/show/92/2016.
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016). Retrieved from http://zakon.rada.gov.ua/rada/show/984_013-16 (assessed 20/11/2020) [In Ukrainian].
5. Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" (2017). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19.
6. On approval of the action plan for 2017 on the implementation of the Cybersecurity Strategy of Ukraine / Legislation of Ukraine. (2017). Retrieved from: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (accessed 20/11/2020) [In Ukrainian].
7. On approval of the plan of actions for 2018 on implementation of the Cybersecurity Strategy of Ukraine / Legislation of Ukraine. (2018). Retrieved from: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80 (accessed 20/11/2020) [In Ukrainian].
8. On the basic principles of cybersecurity in Ukraine: the Law of Ukraine from 05.10.2017 p. 2163-VIII. (2017). Retrieved from

http://zakon.rada.gov.ua/laws/show/2163-19 (assessed 20/11/2020) [In Ukrainian].

9. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 “On the Cybersecurity Strategy of Ukraine”. Legislation of Ukraine. (2016). Retrieved from https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (accessed 20/11/2020) [In Ukrainian].
10. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 “On the Cybersecurity Strategy of Ukraine” Legislation of Ukraine. (2016). Retrieved from https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80 (accessed 24/03/2020) [In Ukrainian].
11. Presidential Decree «On the Decision of the National Security and Defense Council of Ukraine of May 6, 2015» On the National Security Strategy of Ukraine (2015). Retrieved from https://zakon.rada.gov.ua/laws/show/287/2015.
12. Presidential Decree On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine» (2016). Retrieved from https://law.gov.ua/laws/show/96/2016#n11.
13. Pro natsionalnu bezpeku Ukrainy [On the national security of Ukraine], 21.06.2018, No 2469-VIII. (2018). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19(in Ukrainian).
14. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of cybersecurity in Ukraine] (Ukraine), 05.10.2017, No 2163-VIII. (2017). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian).
15. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii [On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation], 17.01.2018, No 67-r. (2018). Retrieved from https://zakon.rada.gov.ua/laws/show/67-2018-r (in Ukrainian).
16. Relations with Ukraine / The North Atlantic Treaty Organization's official website.

(2016) Retrieved from: https://www.nato.int/cps/en/natolive/topics_37750.htm (accessed 20/11/2020).

17. Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Regulation on the Ministry of Defense of Ukraine" (2014). Retrieved from https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF.
18. The Convention on Cybercrime of the Council of Europe from 7.09.2005 № 2824-IV. (2005). Retrieved from http://zakon.rada.gov.ua/laws/show/994_575 (assessed 20/11/2020).
19. The Cyberpolice of Ukraine. Diskcoder. C virus was the cover up for the largest-scale cyberattack in the history of Ukraine. (2020) Retrieved from: https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/. (accessed 20/11/2020) [In Ukrainian].

Academia:

1. Alfred, N. (2018). US: Russia's NotPetya the most destructive cyberattack ever. Retrieved from https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/.
2. Ali N. S. (2019). `A four-phase methodology for protecting web applications using an effective real-time technique`. *International Journal of Internet Technology and Secured Transactions, 6(4), 303*.
3. Ali N. S., Shibghatullah, A. S. (2016). `Protection Web Applications using Real-Tie Technique to Detect Structured Query Language Injection Attacks`. *International Journal of Computer Applications, 149 (6).*
4. Al-Mhiqani M. N., Ahmad R., Yassin W., Hassan A., Abidin Z. Z., Ali N. S., Abdulkareem K. H. (2018). 'Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems'. *International Journal of Advanced Computer Science and Applications (IJACSA).*

5. Al-Mhiqani,M.N., Ahmad R., Abdulkareem K. H., Ali N.S. (2017). `Investigation Study of Cyber-Physical Systems: Characteristics, Application Domains, and Security Challenges`. *Journal of Engineering and Applied Sciences (ARPN), 12(22), 6557-6567*.
6. Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT), 7(3) 51–54.* Retrieved from https://doi.org/10.5121/csit.2017.70305.
7. Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G., & Feldman, L. (2017). The cybersecurity framework: Implementation guidance for federal agencies. *Draft NISTIR 8170. US Department of Communication.* Retrieved from https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf.
8. Bereza, V. (2018). Concept and classification of powers of the Cyberpolice Department of the National Police of Ukraine. *Bulletin of Kharkiv National University of Internal Affairs.*
9. Bezpalova O.I. (2017). Interaction of the National Police of Ukraine with other law enforcement agencies in the field of combating cybercrime as one of the directions of ensuring the components of the security and defense sector. Topical Issues in Combating. *Cybercrime and Trafficking in Human Beings: Scientific and Practical Conference, 21-24.*
10. Boes, S., Leukfeldt, E.R. (2017). Fighting Cybercrime: A Joint Effort. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, 3, 185–203.*
11. Bondarenko O.S. (2018). Cybercrime in Ukraine: causes, characteristic features and counteraction measures. *Comparative and Analytical Law, 1, 246-252*.
12. Butler, N. (2018). Why cyber-attack is the biggest risk for energy companies. *Financial Times.* Retrieved from https://www.ft.com/content/109350ea-c6f2-11e8-ba8f-ee390057b8c9.

*13.*Čelik P. (2019). Institutional measures for increasing the cyber security for business in the European Union. *Economic Themes, 351-364.*

14. Center for Internet Security (CIS). (2018). *CIS controls version 7.* Retrieved from https://learn.cisecurity.org/20-controls-download.

15. Collins A. (2019). The Global Risks Report. *World Economic Forum 2019, 14th Edition.* Retrieved from http://wef.ch/risks2019.

16. Da Silva, M.F. (2016). Cyber Security vs. Cyber Defense – A Portuguese View On the Distinction. Retrieved from https://www.academia.

17. Derzhavnyi tsentr informatsiinykh resursiv Ukrainy. (2020). Systema elektronnoi vzaiemodii orhaniv vykonavchoi vlady [System of electronic interaction of executive bodies]. Retrieved from http://dir.gov.ua/sistema-elektronnoyi-vzayemodiyi-organ (in Ukrainian).

18. Dewar, Robert S. ed. (2018). National Cybersecurity and Cyberdefense Policy Snapshots: *Collection 1, 2018, Center for Security Studies (CSS), ETH Zürich.*

19. Drobyazko, S., Alieksieienko, I., Kobets, M., Kiselyova, E., Lohvynenko, M. (2019). Transnationalisation and segment security of the international labor market. *Journal of Security and Sustainability Issues 9(2).*

20. Dubov D. (2016). Cyber space as a new dimension geopolitical rivalry. *Monograph, 328.*

21. Dubov D., Boiko V., Hnatyuk S., Isakova T., Ozhevan M., Pokrovska A. (2018) Public-private partnership in cybersecurity: international experience and opportunities for Ukraine. *Analytical report: General editorship of Dubov. Kyiv, 84.*

22. Durmanov, A., Bartosova, V., Drobyazko, S., Melnyk, O., Fillipov, V. (2019). Mechanism to ensure sustainable development of enterprises in the information space. *Entrepreneurship and Sustainability Issues, 7(2), 1377-1386.*

23. European External Action Service. (2019). *EU-Ukraine relations – factsheet.* Retrieved from https://eeas.europa.eu/headquarters/headquarters-Homepage/4081/eu-ukraine-relations-factsheet_en.

24. European Union Agency for Network and Information Security (ENISA). (2018). *ENISA threat landscape report 2018 (15 Top Cyber-Threats and Trends)*. Retrieved from https://doi.org/10.2824/967192.
25. European Union Agency for Network and Information Security (ENISA). (2019). *ENISA threat landscape report 2018 -15 Top Cyber-Threats and Trends*. https://doi.org/10.2824/967192.
26. Fishchuk, V., Matiushko, V., Cherniev, Ye., Yurchak, O., Lavryk, Ya., & Amelin, A. (2020). Ukraina 2030E – kraina z rozvynutoiu tsyfrovoiu ekonomikoiu [Ukraine 2030E is a country with a developed digital economy]. Retrieved from https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.htmlhttps://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (in Ukrainian).
27. Friedberg I., K. McLaughlin, P. Smith, D. Laverty, and S. Sezer. (2017). `Safety and security analysis for cyber-physical systems`. *International Journal of Information Security, 34, 183–196.*
28. Gercke M. (2019). Understanding cybercrime: phenomena, challenges and legal response. *ITU publication.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx.
29. Goss, D. (2017). Operationalizing Cybersecurity — Framing Efforts to Secure U.S. *Information Systems. The Cyber Defense Review, 2(6), 91–110.*
30. Homburger Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. Global Society. Retrieved from https://doi.org/10.1080/13600826.2019.15695.
31. Hutsaliuk, M. (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti [Current trends in organized cybercrime]. *Informatsiia i pravo, 1, 118–128 (in Ukrainian).*
32. Information Security Forum (ISF). (2018). The standard of good practice for information security 2018. Retrieved from https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/.

33. ITU Publications. (2018). Global Cybersecurity Index (GCI). Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

34. ITU. (2017). Global cybersecurity index 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

35. ITU. (2019). Index of cyber security indec.es Retrieved from http://cybersecurityindex.org/index.php/calculation.

36. Kellermann. (2017). Technology risk checklist. *Cybercrime and Security, IIB-2, page 1.*

37. Klochko, A.N., Kulish, A.N., Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. *Russian Journal Of Criminology, 4, 790-800. Retrieved from http://doi.org/10.17150/2500-4255.2016.10.*

38. Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. (2019). *Using quantitative methods to identify insecurity due to unusual business operations, Entrepreneurship and Sustainability Issues, 6(3), 1101-1012.*

39. Kostyuk N., Geers K. (2015). Ukraine: A Cyber Safe Haven? *NATO Publications: Cyber War in Perspective: Russian Aggression against Ukraine. Pp. 113-122.*

40. Kostyuk N. (2015). `Ukraine: A Cyber Safe Haven?` *NATO CCD COE Publications.*

41. Kravtsova M. (2018). The Current State and Directions of Countering Cybercrime in Ukraine. *Bulletin of the Criminological Association of Ukraine, 2018. No. 2 (19), 155-165.*

42. Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. *The African Journal of Information and Communication (AJIC), 18, 157–164. Retrieved from https://doi.org/10.23962/10539/21789.*

43. Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *The African Journal of Information and Communication (AJIC), 23, 1–26.*

44. MindTools. (2018). *SMART.* Retrieved from https://www.mindtools.com/pages/article/smart-goals.htm.
45. Minister of Justice and Correctional Services. (2018). *Cybercrimes Bill. Pretoria: Government of South Africa.* Retrieved from https://www.ellipsis.co.za/wp-content/uploads/2018/03/181023Clean_Cybercrimes_Bil.pdf.
46. Ministry for Development of Economy, Trade and Agriculture of Ukraine. (2020). Cooperation with NATO. Retrieved from https://www.me.gov.ua/Documents/List?lang=uk-UA&id=ed2cb323-2974-4ada-986c-6a1b4b60da41&tag=PerelikNormativnopravovikhAktiv.
47. Ministry for Development of Economy, Trade and Agriculture of Ukraine. (2020). *The economy of security and defense of Ukraine. Retrieved* from https://www.me.gov.ua/Tags/DocumentsByTag?lang=uk-UA&id=70fcebbe-4c3e-4303-8e54-e36f25570b55&tag=EkonomikaOboroniIBezpeki.
48. Morgan S. (2019). Report from Cybersecurity Ventures. *Herjavec Group.* Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.
49. Mykola Syomych, Iryna Markina, Dmytro Diachkov (2018). Cybercrime as a leading threat to information security in the countries with transitional economy. *Advances in Social Science, Education and Humanities Research: 2nd International Conference on Social, economic, and academic leadership, 217, 342–350.*
50. Myskiv G., Irshak O. (2019). `Financial aspect of Cybercrime: situation in Ukraine and the world`. *International Journal of Legal Studies (IJOLS), 365-376.*
51. Myskiv G., Irshak O., (2019). Financial Aspect of Cybercrime: Situation in Ukraine. *World International Journal of Legal Studies, 1(5), 365 – 376.*
52. Nath, S. (2018). Building capability with CMMI. *ISACA Journal.* Retrieved from https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=667.

53. National Cyber Security Index (2018). Retrieved from: https://ega.ee/wp-content/uploads/2018/05/ncsi_digi tal_smaller.pdf.
54. NATO. (2018). Relations with Ukraine. Retrieved from https://www.nato.int/cps/en/natolive/topics_37750.htm.
55. NATO. Defending against cyber attacks / Retrieved from https://www.nato.int/cps/en/natohq/ topics_118663.htm?selectedLocale=en (assessed 20/11/2020).
56. Nekrasov V., Polyakova A. (2017). This is war: Ukraine was shaken by the largest cyberattack in history. *Ekonomichna Pravda.* Retrieved from http://www.epravda.com.ua/publications/2017/06/27/626518/.
57. NIST. (2018). Framework for improving critical infrastructure cybersecurity. Retrieved from https://doi.org/10.1109/JPROC.2011.2165269.
58. Ostrovoy A.V. (2018). Analysis Of the Conditions For the State Policy Formation To Ensure Kibernetic Security in Ukraine. *Public Governance*. Retrieved from https://doi.org/10.32689/2617-2224-2019-17-2-296-306.
59. Pierre Audoin. (2013). `Competitive analysis of the UK cyber security sector`. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf.
60. Polytyuk, P., Vukmanovic, O., & Jevkes, S. (2017). Ukraine's power outage was a cyber-attack: Ukrenergo. Reuters. Retrieved from https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA.
61. Powers, E. W., Fancher, J. D., & Silber, J. (2016). Beneath the surface of a cyberattack: A deeper look at business impacts. Deloitte. Retrieved from https://doi.org/10.1007/978-1-4302-1115-0_14.

*62.*Roshchuk, M. (2018). Development of electronic government in Ukraine: legal aspects of providing information security. *Ukrainian Scientific Journal of Information Security, 24(1).*

63. Salhin, A., Kyiu, A., Taheri, B., Porter, C., Valantasis-Kanellos, N., & König, C. (2016). Quantitative data gathering methods and techniques. *Research methods for accounting and finance.* Retrieved from https://doi.org/10.23912/978-1-910158-88-3-3226.

64. Sandelson, M. (2019). Cyber-attack powerlessness in the energy industry? F-Secure cyber security company. Retrieved from https://blog.f-secure.com/cyber-attack-powerlessness-in-the-energy-industry/.

65. Sanjana Sharma. (2015). Cyber Security For The Defence Industry. Retrieved from http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry.

66. Shafqat N., Masood A. (2016). `Comparative Analysis of Various National Cyber Security Strategies`. *International Journal of Computer Science and Information Security, 1(14).*

67. Sharikov, Pavel A. (2019). Evolution of American Cyber Security Policies. *Mirovaya Ekonomika i Mezhdunarodnye Otnosheniya.* Retrieved from http://doi.org/10.20542/0131-2227-2019-63-10-51-58.

68. Shchehliuk, S. (2019). Morfolohiia tsyfrovoi ekonomiky: osoblyvosti rozvytku ta rehuliuvannia tsyfrovykh tekhnolohichnykh platform [Morphology of digital economy: features of development and regulation of digital technological platforms]. Lviv: Instytut rehionalnykh doslidzhen im. M. I. Dolishnoho NAN Ukrainy (in Ukrainian).

69. Sitdikova, L.B.; Starodumova, S.J. (2019). Corporate agreement as a means of providing security in the course of entrepreneurship development. *Entrepreneurship and Sustainability Issues, 7(1), 324-335.* Retrieved from http://doi.org/10.9770/jesi.2019.7.1.

70. Skrynkovskyy, R., Pawlowski, G., Harasym, P., & Koropetskyi, O. (2017). Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise. *Path of Science, 3(10), 5001–5009*. Retrived from doi: 10.22178/pos.27-6.

71. Speech by NATO Secretary General Anders Fogh Rasmussen to the chairpersons of the foreign affairs committees of the European Union member's states parliaments, Copenhagen. (2012). *NATO multimedia library*. Retrieved from http://www.natolibguides.info/nato-eu/documents (assessed 20/11/2020).

72. Sridhar, S., Hahn, A., & Govindarasu, M. (2019). `Cyber–physical system security for the electric power grid`. *Proceedings of the IEEE, 100(1), 210-224.*

73. State Statistics Service of Ukraine (SSSU). (2018). Security in Ukraine. Retrieved from: http://www.ukrstat.gov.ua.

74. Statista. (2020). `Average total cost per data breach worldwide 2020, by industry`. Retrieved from: https://www.statista.com/statistics/387861/cost-data-breach-industry/.

75. Streltsov, Lev (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. European Journal for Security Research. Retrieved from http://doi.org/10.1007/s41125-017-0020-x.

76. Symantec. (2017). Dragonfly: Western energy sector targeted by sophisticated attack group. Retrieved from https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyberattacks.

77. The Cyberpolice of Ukraine. Diskcoder. C virus was the cover up for the largest-scale cyberattack in the history of Ukraine. Retrieved from https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/. (assessed 20/11/2020) [In Ukrainian].

78. Tkachuk, N. (2019). Stan ta problemni pytannia realizatsii Stratehii kiberbezpeky Ukrainy [Status and problematic issues of implementation of the Cyber Security Strategy of Ukraine]. *Informatsiia i pravo, 1, 129–134 (in Ukrainian).*

79. Tkachuk, Nataliya (2017). The Role and Place of the Security Service of Ukraine in the National Cyber Security System. *The Journal of Eastern European Law, 44, 50-57.*

80. Tkachuk, Nataliya (2018). Countering Cyber Threats to National Security: Ukraine Defends Its Cyber Infrastructure in the Face of Attacks from Russia. Retrieved from https://www.researchgate.net/publication/328232415.

81. Ukrinform (2017) The Ministry of Defense has successfully repelled the cyberattack. Multimedia broadcasting platform of Ukraine. Retrieved from https://www.ukrinform.ru/ rubric-society/2256867-v-ukraine-sozdaut-kibervojska-poltorak.html. (accessed 09/11/2019) [In Russian].

82. Vakulyk O., Petrenko P., Kuzmenko I., Pochtovyi M., Orlovskyi R., (2020). Cybersecurity as a component of the national security of the state. *Journal of security and sustainability issues. 3(4), 133-139.*

83. Voitsikhovskyi, A. V. (2018). Kiberbezpeka yak napriam yevroatlantychnoi intehratsii Ukrainy [Cybersecurity as a direction of Ukraine's Euro-Atlantic integration]. *In Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii (pp. 42–48). Kharkiv: Pravo (in Ukrainian).*

Annex A

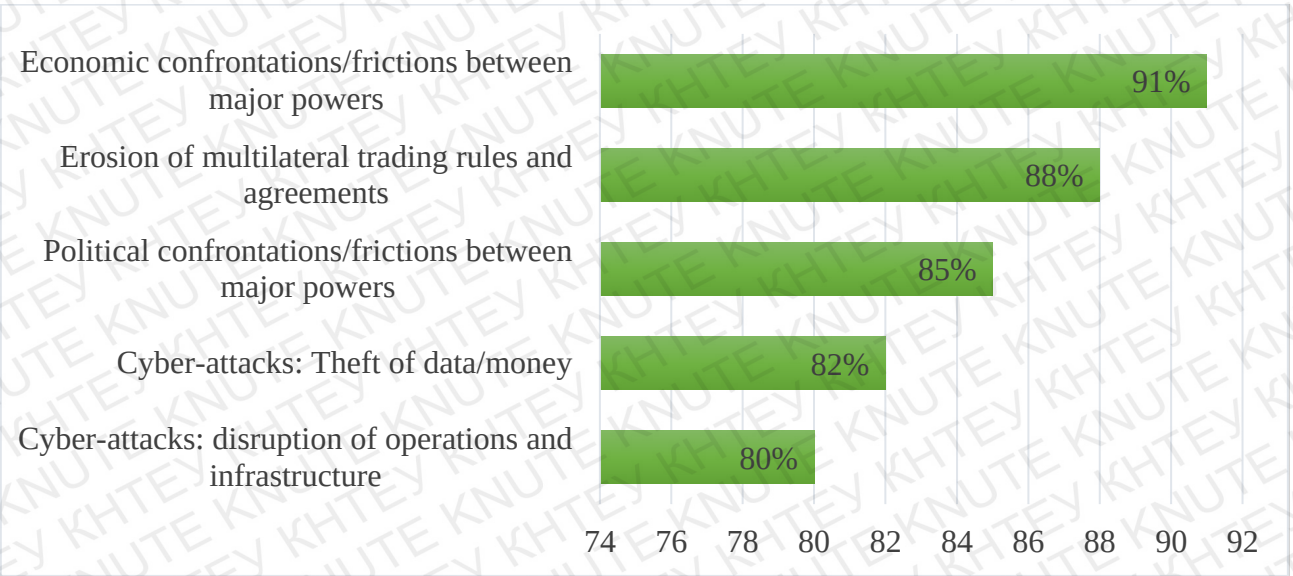

Figure 1. Percentage of businesses expecting short-term risks increasing in 2019

Source: World Economic Forum Global Risks Perception Survey 2018–2019

Annex B

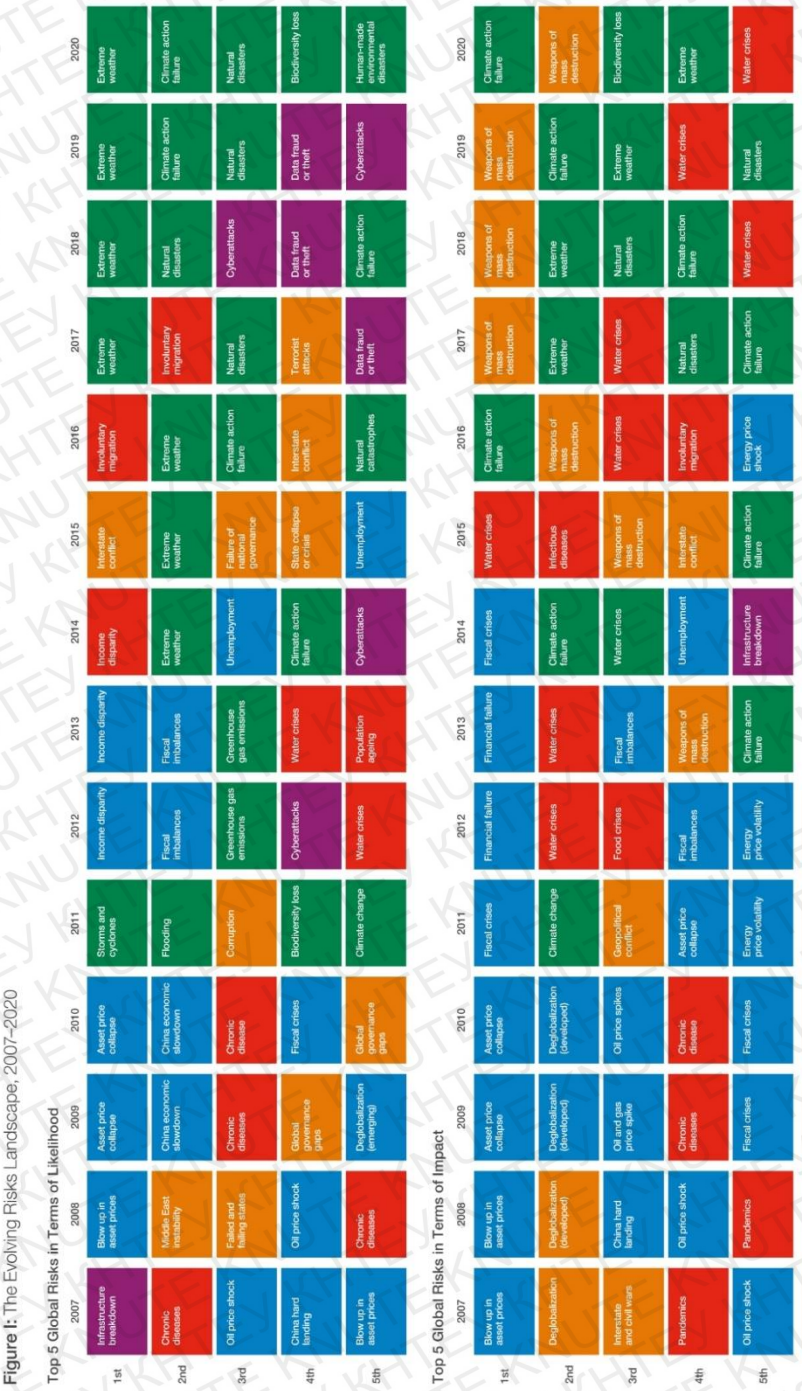

Figure 2. The evolving risks landscape, 2007 – 2020

Source: World Economic Forum, 2020

Continuation of the Annex B

Figure 3. The evolving risks landscape, 2007 – 2020

Source: World Economic Forum, 2020

Annex C

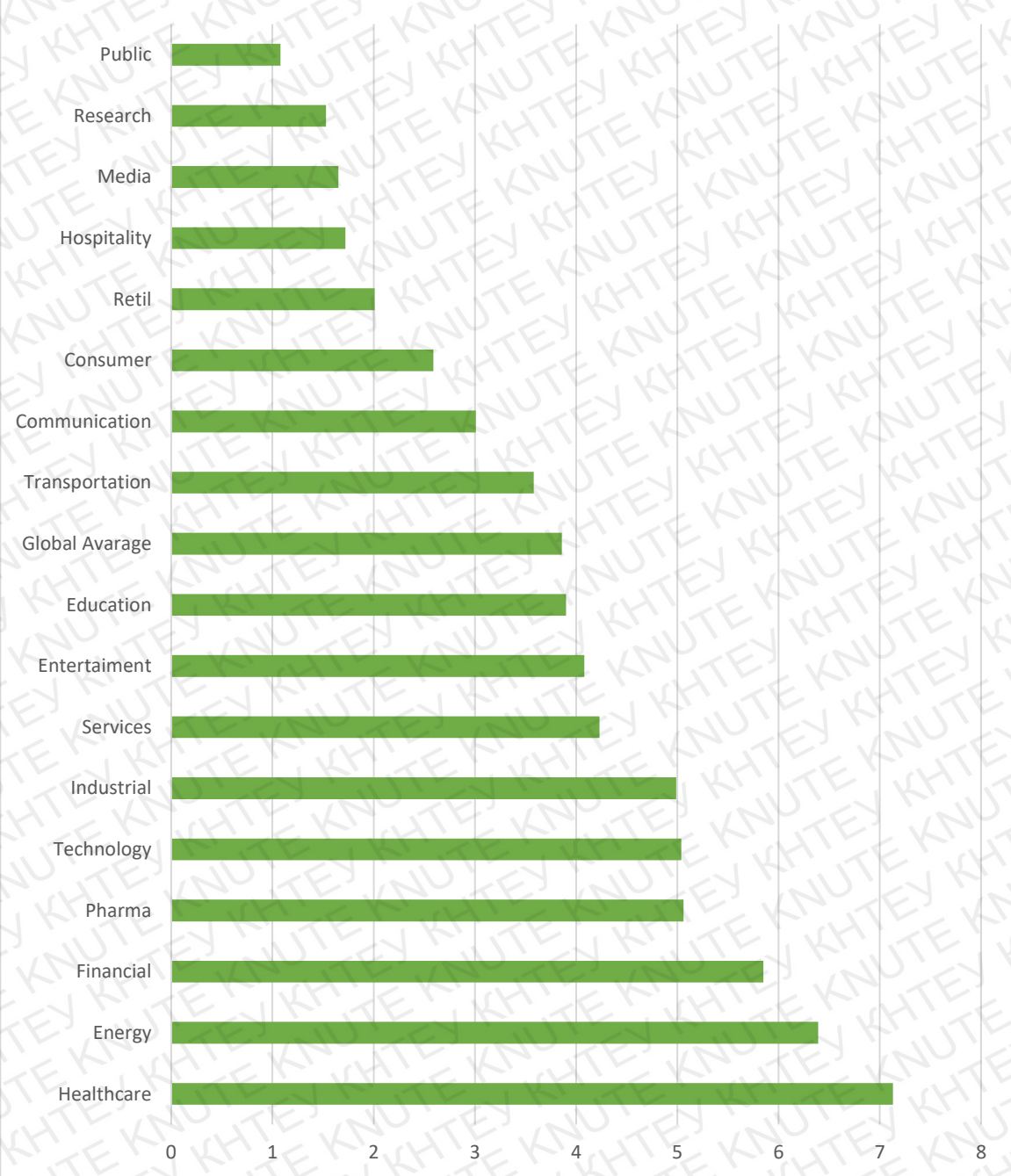

Figure 4. Average cost of data breaches worldwide as of 2020, by industry (in million U.S. dollars)

Source: Statista, 2020

Annex D

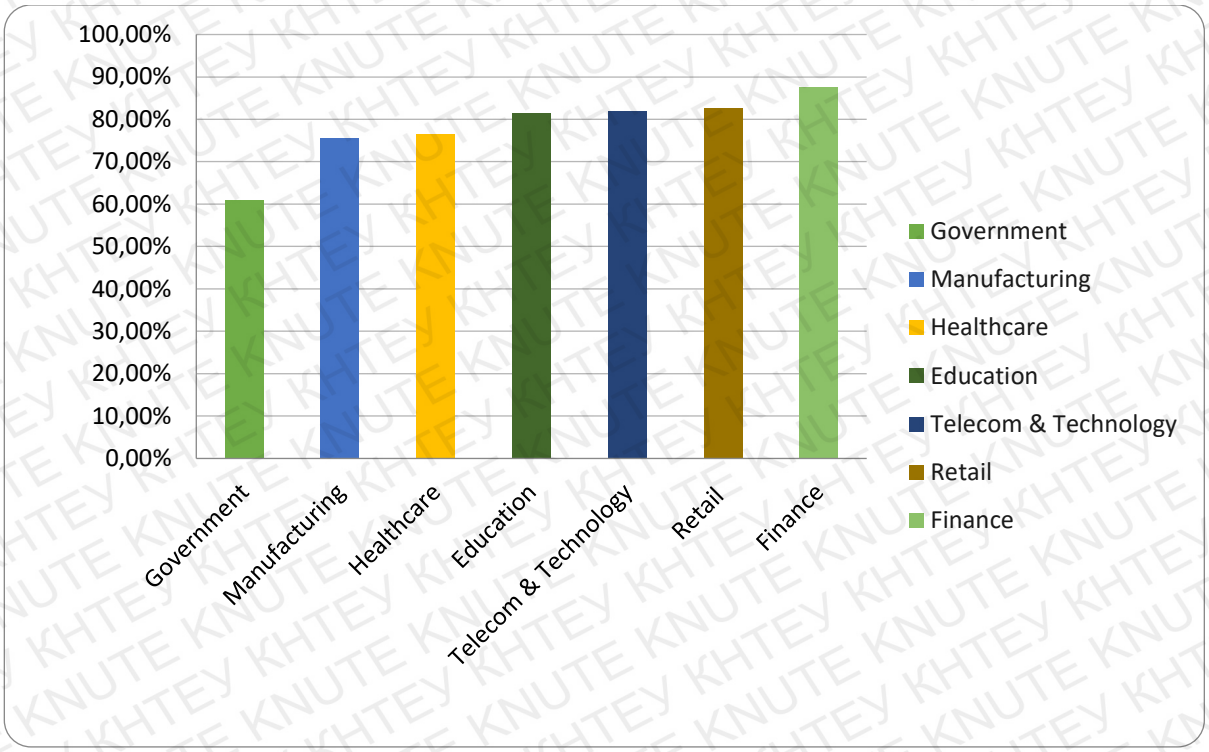

Figure 5. Percentage compromised by at least one successful attack in path 12 month, by industry

Source: composed by the author based on Hackmageddon, 2020 data

Annex E

Pillars of GCI

Legal: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

Technical: Measures based on the existence of technical institutions and framework dealing with cybersecurity.

Organizational: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

Capacity building: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building.

Cooperation: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

Source: GCI Report, 2018

Annex F

Global Cybersecurity Index 2018

Table 1: Level of commitment (high)

High		
United Kingdom	Georgia	New Zealand
United States of America	Finland	Switzerland
France	Turkey	Ireland
Lithuania	Denmark	Israel
Estonia	Germany	Kazakhstan
Singapore	Egypt	Indonesia
Spain	Croatia	Portugal
Malaysia	Italy	Monaco
Canada	Russian Federation	Kenya
Norway	China	Latvia
Australia	Austria	Slovakia
Luxembourg	Poland	Bulgaria
Netherlands	Belgium	India
Saudi Arabia	Hungary	Slovenia
Japan	Sweden	Rwanda
Mauritius	United Arab Emirates	Viet Nam
Republic of Korea	The Republic of North	Uruguay
Oman	Macedonia	
Qatar	Thailand	

Table 2: Level of commitment (medium)

Medium		
Uzbekistan	Kuwait	Cote d'Ivoire
Moldova	Bahrain	Iceland
Ukraine	Belarus	Botswana
Azerbaijan	Brazil	Ghana
South Africa	Czech Republic	Zambia
Cyprus	Romania	Cameroon
Nigeria	Colombia	Dominican Republic
Philippines	Jordan	Morocco
Serbia	Liechtenstein	Jamaica
Tanzania	Tunisia	Pakistan
Iran	Greece	Argentina
Montenegro	Bangladesh	Peru
Albania	Armenia	Burkina Faso
Mexico	Benin	Panama
Brunei Darussalam	Cuba	Samoa
Uganda	Malta	Ecuador
Paraguay	Chile	Venezuela
	Sri Lanka	
	Mongolia	

Figure 6. Level of commitment into cyber security of countries in 2018

Source: GCI Report, 2018

Continuation of Annex F

Table 3: Level of commitment (low)

Low		
Gabon	Afghanistan	Mali
State of Palestine	Barbados	Timor-Leste
Senegal	Myanmar	San Marino
Sudan	Saint Vincent and the	Marshall Islands
Gambia	Grenadines	Somalia
Ethiopia	Congo	South Sudan
Malawi	Cambodia	Saint Kitts and Nevis
Tajikistan	Mozambique	Sao Tome and Principe
Iraq	Bahamas	Djibouti
Algeria	Grenada	Solomon Islands
Nepal	Bolivia	Tuvalu
Seychelles	Sierra Leone	Guinea-Bissau
Kyrgyzstan	Eswatini	Cabo Verde
Guatemala	Guyana	Lesotho
Antigua and Barbuda	Papua New Guinea	Haiti
Syrian Arab Republic	Nicaragua	Honduras
Costa Rica	Belize	Micronesia
Tonga	Namibia	Central African Republic
Libya	El Salvador	Equatorial Guinea
Liberia	Turkmenistan	Kiribati
Bosnia and Herzegovina	Andorra	Vatican
Madagascar	Suriname	Eritrea
Lao	Mauritania	Democratic People's Republic
Fiji	Nauru	of Korea
Guinea	Chad	Dominica
Trinidad and Tobago	Vanuatu	Yemen
Zimbabwe	Angola	Comoros
Lebanon	Saint Lucia	Democratic Republic of the
Bhutan	Niger	Congo
	Burundi	Maldives
	Togo	

Figure 7. Level of commitment into cyber security of countries in 2018

Source: GCI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Eswatini	0.133	28	137
Namibia	0.127	29	141
Chad*	0.098	30	147
Angola*	0.097	31	148
Niger	0.094	32	150
Burundi	0.087	33	151
Togo	0.087	33	151
Mali*	0.085	34	152
South Sudan*	0.065	35	157
Sao Tome and Principe*	0.064	36	158
Guinea-Bissau*	0.055	37	162
Cabo Verde*	0.051	38	163
Lesotho*	0.051	38	163
Central African Republic	0.036	39	167
Equatorial Guinea	0.031	40	168
Eritrea*	0.020	41	171
Democratic Republic of the Congo*	0.008	42	174

Americas region

Member State	Score	Regional Rank	Global Rank
United States of America*	0.926	1	2
Canada*	0.892	2	9
Uruguay	0.681	3	51
Mexico	0.629	4	63
Paraguay	0.603	5	66
Brazil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.470	9	83
Dominican Republic	0.430	10	92
Jamaica	0.407	11	94
Argentina	0.407	11	94

Figure 8. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Peru	0.401	12	95
Panama	0.369	13	97
Ecuador	0.367	14	98
Venezuela	0.354	15	99
Guatemala	0.251	16	112
Antigua and Barbuda	0.247	17	113
Costa Rica*	0.221	18	115
Trinidad and Tobago	0.188	19	123
Barbados	0.173	20	127
Saint Vincent and the Grenadines	0.169	21	129
Bahamas	0.147	22	133
Grenada	0.143	23	134
Bolivia (Plurinational State of)	0.139	24	135
Guyana	0.132	25	138
Nicaragua	0.129	26	140
Belize	0.129	26	140
El Salvador*	0.124	27	142
Suriname	0.110	28	144
Saint Lucia	0.096	29	149
Saint Kitts and Nevis	0.065	30	157
Haiti	0.046	31	164
Honduras	0.044	32	165
Dominica	0.019	33	172

Arab States region

Member State	Score	Regional Rank	Global Rank
Saudi Arabia	0.881	1	13
Oman	0.868	2	16
Qatar	0.860	3	17
Egypt	0.842	4	23
United Arab Emirates	0.807	5	33
Kuwait	0.600	6	67

Figure 9. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Bahrain	0.585	7	68
Jordan	0.556	8	74
Tunisia	0.536	9	76
Morocco	0.429	10	93
State of Palestine	0.307	11	101
Sudan	0.294	12	103
Iraq	0.263	13	107
Algeria	0.262	14	108
Syrian Arab Republic	0.237	15	114
Libya	0.206	16	117
Lebanon	0.186	17	124
Mauritania*	0.107	18	145
Somalia	0.070	19	156
Djibouti	0.063	20	159
Yemen*	0.019	21	172
Comoros	0.015	22	173

Asia-Pacific region

Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10
Japan	0.880	4	14
Republic of Korea	0.873	5	15
China	0.828	6	27
Thailand	0.796	7	35
New Zealand*	0.789	8	36
Indonesia	0.776	9	41
India	0.719	10	47
Viet Nam	0.693	11	50
Philippines	0.643	12	58
Iran	0.641	13	60

Figure 10. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Brunei Darussalam*	0.624	14	64
Bangladesh	0.525	15	78
Sri Lanka	0.466	16	84
Mongolia	0.465	17	85
Pakistan	0.407	18	94
Samoa	0.367	19	98
Nepal	0.260	20	109
Tonga	0.208	21	116
Lao People's Democratic Republic*	0.195	22	120
Fiji	0.194	23	121
Bhutan	0.181	24	125
Afghanistan	0.177	25	126
Myanmar	0.172	26	128
Cambodia	0.161	27	131
Papua New Guinea*	0.131	28	139
Nauru*	0.101	29	146
Vanuatu	0.098	30	147
Timor-Leste*	0.082	31	153
Marshall Islands*	0.072	32	155
Solomon Islands*	0.061	33	160
Tuvalu*	0.057	34	161
Micronesia (Federated States of)*	0.040	35	166
Kiribati	0.028	36	169
Democratic People's Republic of Korea*	0.020	37	171
Maldives*	0.004	38	175

CIS region

Member State	Score	Regional Rank	Global Rank
Russian Federation	0.836	1	26
Kazakhstan	0.778	2	40
Uzbekistan	0.666	3	52
Azerbaijan	0.653	4	55

Figure 11. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Belarus	0.578	5	69
Armenia	0.495	6	79
Tajikistan*	0.263	7	107
Kyrgyzstan	0.254	8	111
Turkmenistan*	0.115	9	143

Europe region

Member State	Score	Regional Rank	Global Rank
United Kingdom	0.931	1	1
France	0.918	2	3
Lithuania	0.908	3	4
Estonia	0.905	4	5
Spain	0.896	5	7
Norway	0.892	6	9
Luxembourg	0.886	7	11
Netherlands	0.885	8	12
Georgia	0.857	9	18
Finland	0.856	10	19
Turkey	0.853	11	20
Denmark	0.852	12	21
Germany	0.849	13	22
Croatia	0.840	14	24
Italy	0.837	15	25
Austria*	0.826	16	28
Poland	0.815	17	29
Belgium	0.814	18	30
Hungary	0.812	19	31
Sweden*	0.810	20	32
The Republic of North Macedonia	0.800	21	34
Switzerland	0.788	22	37
Ireland	0.784	23	38

Figure 12. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Continuation of Annex F

Global Cybersecurity Index 2018

Member State	Score	Regional Rank	Global Rank
Israel*	0.783	24	39
Portugal	0.758	25	42
Monaco	0.751	26	43
Latvia	0.748	27	44
Slovakia	0.729	28	45
Bulgaria*	0.721	29	46
Slovenia*	0.701	30	48
Moldova	0.662	31	53
Ukraine	0.661	32	54
Cyprus*	0.652	33	56
Serbia	0.643	34	58
Montenegro	0.639	35	61
Albania	0.631	36	62
Czech Republic	0.569	37	71
Romania	0.568	38	72
Liechtenstein	0.543	39	75
Greece	0.527	40	77
Malta	0.479	41	82
Iceland	0.449	42	87
Bosnia and Herzegovina	0.204	43	118
Andorra	0.115	44	143
San Marino*	0.075	45	154
Vatican*	0.021	46	170

Figure 13. Global and Regional ranking of countries according to CGI, 2018

Source: CGI Report, 2018

Annex G

Table 2 : Defence expenditure

Million US dollars

	2013	2014	2015	2016	2017	2018	2019e	2020e
Current prices and exchange rates								
Albania	180	178	132	131	144	176	197	210
Belgium	5 265	5 199	4 204	4 259	4 442	4 843	4 761	5 173
Bulgaria	811	747	633	671	723	961	2 158	1 195
Canada	18 215	18 172	18 689	17 708	23 700	22 399	22 319	22 150
Croatia	850	1 064	883	837	924	966	1 002	986
Czech Republic	2 148	1 975	1 921	1 866	2 259	2 750	2 910	3 038
Denmark	4 217	4 057	3 364	3 593	3 780	4 559	4 557	4 718
Estonia	480	513	463	498	541	615	637	669
France	52 331	52 009	43 492	44 221	46 150	50 484	49 634	50 247
Germany	45 944	46 164	39 829	41 618	45 486	49 750	52 543	56 074
Greece	5 311	5 232	4 519	4 638	4 754	5 386	4 843	4 785
Hungary	1 280	1 210	1 132	1 289	1 708	1 615	2 051	1 829
Italy	26 665	24 481	19 574	22 388	23 911	25 629	23 556	24 853
Latvia*	281	294	282	403	485	709	692	722
Lithuania*	355	428	471	636	818	1 056	1 093	1 118
Luxembourg	234	253	250	236	326	356	381	422
Montenegro	65	69	57	62	65	76	77	97
Netherlands	10 229	10 346	8 672	9 114	9 646	11 167	12 268	12 067
North Macedonia	127	124	105	104	101	120	146	151
Norway	7 839	7 722	6 142	6 431	6 850	7 544	7 514	6 671
Poland*	9 007	10 104	10 596	9 405	9 938	11 857	11 923	12 043
Portugal	3 263	3 007	2 645	2 616	2 739	3 247	3 298	3 472
Romania*	2 452	2 691	2 581	2 645	3 643	4 359	4 608	5 498
Slovak Republic	969	998	987	1 004	1 056	1 297	1 802	1 753
Slovenia	507	487	401	450	477	546	573	584
Spain	12 610	12 631	11 095	9 978	11 893	13 194	12 629	14 069
Turkey	14 427	13 583	11 957	12 649	12 972	14 145	13 986	13 303
United Kingdom	62 258	65 658	59 492	56 154	55 674	60 307	59 365	59 634
United States	680 856	653 942	641 253	656 059	642 933	672 255	730 149	784 952
NATO Europe and Canada	**288 129**	**289 203**	**254 406**	**255 439**	**275 106**	**299 995**	**301 378**	**307 530**
NATO Total	**968 985**	**943 145**	**895 659**	**911 498**	**918 039**	**972 250**	**1 031 527**	**1 092 482**
Constant 2015 prices and exchange rates								
Albania	154	150	132	130	135	148	167	181
Belgium	4 501	4 400	4 204	4 196	4 216	4 330	4 423	4 919
Bulgaria	697	640	633	655	667	814	1 842	1 040
Canada	14 828	15 562	18 689	18 219	23 302	21 595	21 619	22 377
Croatia	708	892	883	831	883	860	927	949
Czech Republic	1 772	1 686	1 921	1 831	2 090	2 306	2 488	2 723
Denmark	3 572	3 399	3 364	3 587	3 659	4 185	4 375	4 633

Estonia	417	432	463	491	504	524	555	596
France	44 471	43 931	43 492	44 097	44 857	46 496	47 639	48 817
Germany	39 776	39 222	39 829	41 230	43 695	45 033	49 123	52 918
Greece	4 340	4 355	4 519	4 660	4 653	5 014	4 774	4 915
Hungary	1 089	1 032	1 132	1 285	1 604	1 429	1 867	1 793
Italy	23 046	20 786	19 574	21 934	22 757	23 427	22 509	24 299
Latvia*	239	245	282	401	459	617	619	651
Lithuania*	300	357	471	627	758	907	962	1 000
Luxembourg	201	212	250	235	312	318	348	391
Montenegro	56	59	57	59	59	63	67	86
Netherlands	8 633	8 649	8 672	9 056	9 253	10 031	11 468	11 460
North Macedonia	109	105	105	100	94	102	128	136
Norway	5 564	5 862	6 142	6 799	6 861	7 022	7 616	7 798
Poland*	7 648	8 521	10 596	9 807	9 752	11 016	11 454	12 077
Portugal	2 800	2 562	2 645	2 578	2 605	2 908	3 064	3 263
Romania*	2 127	2 309	2 581	2 617	3 437	3 763	3 999	4 863
Slovak Republic	806	832	987	1 012	1 030	1 186	1 693	1 668
Slovenia	430	411	401	447	458	491	530	552
Spain	10 568	10 607	11 095	9 969	11 485	12 056	11 984	13 635
Turkey	11 696	11 784	11 957	12 993	14 505	17 979	18 336	18 015
United Kingdom	62 313	61 316	59 492	62 208	63 503	64 969	65 629	67 236
United States	696 291	660 062	641 253	651 201	626 328	640 277	701 563	716 886
NATO Europe and Canada	**252 697**	**250 153**	**254 406**	**261 895**	**277 497**	**289 489**	**300 076**	**312 994**
NATO Total	**948 988**	**910 215**	**895 659**	**913 096**	**903 825**	**929 765**	**1 001 638**	**1 029 880**

Notes: Figures for 2019 and 2020 are estimates. The NATO Europe and Canada and NATO Total aggregates from 2017 onwards include Montenegro, which became an Ally on 5 June 2017, and from 2020 onwards include North Macedonia, which became an Ally on 27 March 2020.

* These Allies have national laws and political agreements which call for 2% of GDP to be spent on defence annually, consequently estimates are expected to change accordingly. For the past years, Allies' defence spending was based on the then available GDP data and Allies may, therefore, have met the 2% guideli when using those figures (In 2018, Lithuania met 2% using November 2018 OECD figures).

Table 6 : GDP per capita and defence expenditure per capita

2015 prices and exchange rates

	2013	2014	2015	2016	2017	2018	2019e	2020e
GDP per capita (thousand US dollars)								
Albania	3,8	3,9	4,0	4,1	4,2	4,4	4,5	4,3
Belgium	40,0	40,4	41,0	41,4	42,0	42,5	42,8	38,8
Bulgaria	6,6	6,7	7,1	7,4	7,7	8,0	8,3	7,8
Canada	42,9	43,7	43,6	43,6	44,4	44,7	45,1	41,2
Croatia	11,4	11,4	11,8	12,3	12,8	13,3	13,7	12,5
Czech Republic	16,4	16,9	17,7	18,1	18,9	19,4	19,8	17,8
Denmark	51,9	52,4	53,3	54,5	55,3	56,4	57,4	53,9
Estonia	16,6	17,1	17,5	18,0	19,0	19,8	20,6	18,8
France	36,2	36,4	36,6	36,9	37,6	38,2	38,9	34,4
Germany	40,1	40,9	41,1	41,7	42,7	43,2	43,3	40,4
Greece	17,9	18,1	18,2	18,2	18,5	18,9	19,3	17,9
Hungary	11,6	12,2	12,6	13,0	13,6	14,3	15,0	13,8
Iceland	50,2	50,7	52,6	55,3	56,4	57,1	56,9	50,3
Italy	30,0	30,0	30,2	30,7	31,3	31,5	31,7	28,1
Latvia	12,8	13,2	13,7	14,1	14,7	15,5	15,9	14,7
Lithuania	13,3	13,8	14,3	14,8	15,7	16,4	17,1	15,7
Luxembourg	97,3	99,1	101,4	103,4	103,0	104,1	104,4	95,9
Montenegro	6,2	6,3	6,5	6,7	7,0	7,4	7,7	7,2
Netherlands	44,1	44,5	45,2	45,9	47,0	47,9	48,5	44,2
North Macedonia	4,5	4,7	4,9	5,0	5,0	5,2	5,4	5,1
Norway	73,0	73,7	74,3	74,5	75,6	76,1	76,3	71,2
Poland	11,6	12,0	12,4	12,8	13,4	14,2	14,8	13,7
Portugal	18,6	18,8	19,3	19,7	20,4	21,0	21,5	19,5
Romania	8,3	8,6	9,0	9,5	10,2	10,7	11,2	10,6
Slovak Republic	15,2	15,6	16,3	16,6	17,1	17,8	18,2	16,5
Slovenia	19,9	20,5	20,9	21,5	22,6	23,4	23,8	21,9
Spain	24,4	24,8	25,8	26,5	27,2	27,8	28,1	24,9
Turkey	10,1	10,5	11,0	11,2	11,9	12,0	12,0	11,3
United Kingdom	43,5	44,3	45,0	45,5	46,1	46,4	46,8	41,2
United States	54,6	55,6	56,8	57,3	58,3	59,7	60,8	55,9
NATO Europe and Canada	**28,8**	**29,2**	**29,7**	**30,1**	**30,8**	**31,3**	**31,6**	**28,6**
NATO Total	**37,7**	**38,4**	**39,1**	**39,6**	**40,4**	**41,2**	**41,8**	**38,1**
Defence expenditure per capita (US dollars)								
Albania	53	52	46	45	47	51	58	64
Belgium	403	393	373	370	371	379	385	426
Bulgaria	96	89	88	92	94	116	263	150
Canada	423	440	524	505	639	584	580	595
Croatia	167	211	210	199	214	210	228	234
Czech Republic	169	160	182	173	197	217	233	254
Denmark	636	602	592	626	635	722	752	793
Estonia	316	328	353	373	383	397	419	449

France	674	662	653	660	669	691	710	726
Germany	493	484	488	501	529	543	591	636
Greece	396	400	418	432	433	467	446	461
Hungary	110	105	115	131	164	146	191	184
Italy	380	342	322	362	376	387	373	403
Latvia	119	123	142	204	236	320	323	341
Lithuania	101	122	162	219	268	324	344	358
Luxembourg	368	379	438	402	523	522	560	618
Montenegro	91	95	92	95	95	102	108	137
Netherlands	514	513	512	532	540	582	661	656
North Macedonia	53	51	51	48	45	49	62	65
Norway	1 095	1 141	1 183	1 299	1 300	1 321	1 422	1 444
Poland	199	221	276	255	254	287	298	315
Portugal	268	246	255	250	253	283	298	318
Romania	106	116	130	133	175	193	206	252
Slovak Republic	149	154	182	186	189	218	311	306
Slovenia	209	199	194	217	222	237	254	263
Spain	227	228	239	215	247	258	254	289
Turkey	154	153	153	164	181	221	222	215
United Kingdom	972	949	914	948	962	978	982	1 001
United States	2 201	2 072	1 998	2 015	1 926	1 958	2 135	2 166
NATO Europe and Canada	**423**	**417**	**422**	**433**	**457**	**474**	**490**	**507**
NATO Total	**1 039**	**991**	**970**	**984**	**969**	**992**	**1 064**	**1 087**

Notes: Figures for 2019 and 2020 are estimates. The NATO Europe and Canada and NATO Total aggregates from 2017 onwards include Montenegro, which became an Ally on 5 June 2017, and from 2020 onwards include North Macedonia, which became an Ally on 27 March 2020.

Annex K

IV. Strengthening Ukraine's interaction with the EU and NATO in countering cyber threats

In the framework of further development of Ukraine's interaction with NATO and the EU, first of all, it is necessary to take into account the current trends of cooperation between the EU and NATO. Further EU-NATO-Ukraine cooperation in the field of cybersecurity should be focused on the following areas:

- to complete the establishment of a clear cybersecurity coordination working system for the full implementation of the Cybersecurity Strategy of Ukraine to involve all national actors, including non-governmental organizations, and make NATO, the EU and other organizations' assistance more targeted and effective;
- to use the experience and practice of the EU and NATO in order to create a broad national cybersecurity certification scheme, develop a plan to respond to large-scale incidents and crises, deepen public-private partnerships and strengthen research;
- to initiate the accession of Ukraine to the NATO Cooperative Cyber Defence Centre of Excellence, which will help Ukraine to implement best practices and deepen its cooperation with the Alliance in this area;
- to increase Ukraine's defence technical potential in cybersecurity with the assistance of the NATO Cybersecurity Trust Fund and in cooperation with Romania;
- to develop cooperation on strengthening cybersecurity in Ukraine in order to prevent and neutralize possible Russian interference during electoral campaigns in Ukraine;
- to continue identifying critical infrastructure and its key operational vulnerabilities;
- to work out a national Emergency Response Plan in cyber space;
- to develop an instrument of risk sharing through the use of secure cloud services in order to minimize possible losses in case of cyber attacks on the data bases of state authorities;
- to use the best Western experience in order to strengthen interagency cooperation and state-private partnership, as well as to develop a specific effective mechanism for its practical application;
- to propose NATO and the EU to attract more external expert assistance for Ukraine;
- to combine efforts to develop a system of motivation for professionals engaged in cybersecurity and cyber defence.

Annex L

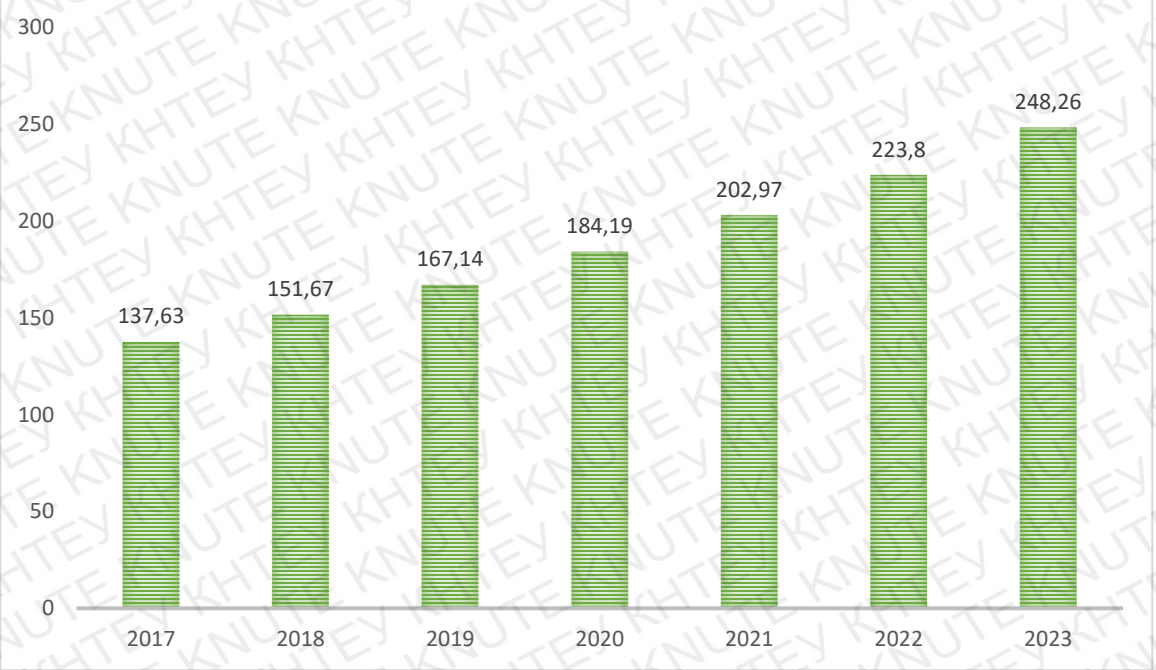

Figure 14. Size of the cybersecurity market worldwide, from 2017 to 2023(in billion U.S. dollars)

Source: Statista, 2020

Annex N

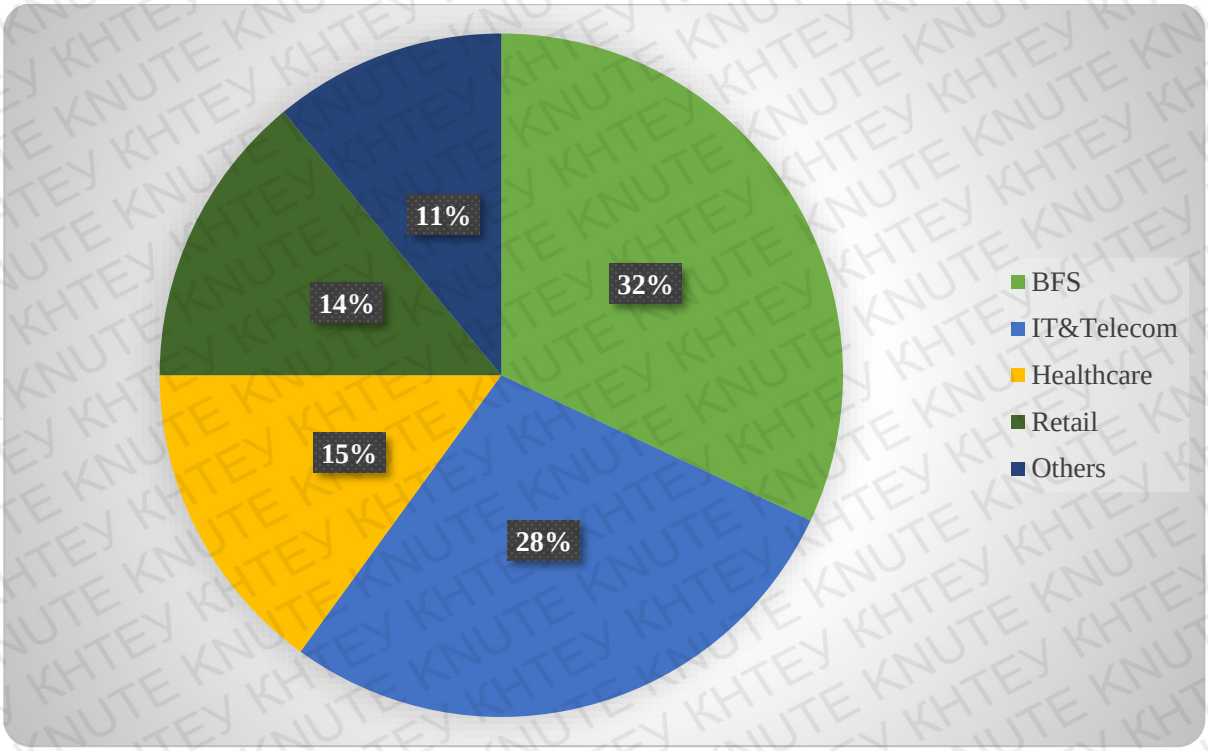

Figure 15. U. S. Cyber security market size, by industry, 2016-2017, USD Billion

Source: Grand view Research, 2020

* The banking and financial services (BFS)