Scientific and Technical Journal

Safety & Defense 5(1) (2019) 31–36

System Approach to Coherent Cybersecurity Strategy

Daniel MICHALSKI

Polish Air Force University, Dęblin, Poland; d.michalski@law.mil.pl, ORCID: 0000-0001-8202-6738

Abstract

Cyber-attacks affect not only our daily lives, but also national security by influencing elections, the economy, and communication. This article is an attempt to give an answer to the question included in the topic "How to build a coherent cybersecurity strategy?". The first part of the article addresses the paradigmatic issue of cybersecurity. The author shows the differences and relations between cybersecurity and cyber defense. At this point, the author presents a systems approach to the nation security and related it to the cybersecurity. The second part of the article has been dedicated to visualize the need of coherent cybersecurity strategy by analyzing data related to cybersecurity. In the end, the author proposes actions to achieve cybersecurity. This has been done based on existing analyzes of cybersecurity strategies and systems approach to the issue of the cybersecurity.

Keywords: cybersecurity, cyber defense, system approach, cyber defense strategies, cybersecurity strategies

1. Introduction

Since the rise of the internet in the 1960s, many changes have occurred from the technical and technological point of view. What is more, public opinion with regards to the internet has also changed. Nowadays, the internet is not only the main tool of communication, but now encompasses people's entire lives, from business to entertainment. The internet is so popular that we are taking about cyber society. The development of the internet gives mankind opportunities for faster communication, and bank transactions, advertisement, and simply new kinds of connecting people, but the new ways of connection created a new kind of threat as well. The development of the information society, coupled with the expansion of the internet's reach, is accompanied by the penetration of further aspects of human activity into cyberspace, and has created a big threat for every human activity.

In literature on the topic, there are several different types of cybercrimes mentioned, from cyber pornography through hacking to cyber terrorism. In the big generalization the crimes can be separated into three main categories:

- cyber-intrusions;
- cyber-theft;
- cyber-destruction. (Bujek, 2018)

All of this may affect individuals users, but also entire nations. What is more, the number of cybercrime types is still increasing with the growing influence of the internet in our lives. Continuous "digitalization" of society creates a gap between the ability of the internet and strategic thinking about security in cyberspace.

The gap mentioned above has been seen by cybersecurity specialists cybersecurity at the European Cybersecurity Forum (ECF). According to the recommendation of ECF "Closing the gap in the strategic thinking about security is needed. It is a strategic challenge and it requires significant costs. It must be reflected in the area of procurement. We need to spend money on cybersecurity," (European Cybersecurity Forum, 2017).

Having seen the threat creating by the gap between the ability of the internet and strategic way of thinking about cybersecurity the author decides to clime topic about cyber

security and cyber defense. Therefore, the aim of this article is to show in synthetic way the system approaches to cybersecurity, as an idea to build the coherent cybersecurity strategy, not to focused on specific process connected with that issue or procedures and methodology. Consequently, the author dedicates this paper to solving the main problem expressed in a question "How to build a coherent cybersecurity strategy in international community based on system approach?".

In order to achieve this goal, the author, based on theoretical research methods such as: analysis and evaluating literature of the subject, literature query, comparison and conclusion is trying to explains the terms connected with cybersecurity. After that, the author gives examples of cyber threats in the numbers of attacks that shows the need to build a common cybersecurity strategy at the national level and in the international community as well. Finally, the author gives an idea of how to develop a common strategy in cybersecurity for a better life. The literature base for the research was here: compact items, articles, reports, and internet sources.

2. The cybersecurity – paradigms issue

However, the term cyber security is new, there are a lot of different definitions which can be found in literature. In order to have better knowledge about the problem, the author will cite several of them while trying to find a common fraction which connects all of them. This intervention is critical even for future studies connected with a common strategy in the area of cyber security, due to the needs that arise from the common understanding of the problem.

Since cyberspace has become another dimension alongside land, air, sea and space, cybersecurity has become not only an issue of individual security, but also an aspect of national security. What is more, according to Gen. Stanisław Koziej, cybersecurity is a part of national defense that is of multi-sector nature. That means cybersecurity consist of information security counter-terrorism etc. (Koziej, 2011)

This shows how cybersecurity is a complex and complicated problem in national security. In order to have a common understanding of the problem, several definitions of cybersecurity have been presented below.

First, the Republic of Poland's Doctrine of Cybersecurity clams that "cybersecurity" means "the process of ensuring safe functioning in cyberspace of the state as a whole, its structures, natural and legal persons, including entrepreneurs and other non-legal entities, as well as IT systems and information resources of the global cyberspace they use" (BBN, 2015). This point of view is similar to that of the National Initiative for cybersecurity careers and studies (an official website of the Department of Homeland Security) which states that: "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". (NICCS, 2018).

The definitions mentioned above shares this same approach to security and understand security as a "process". It should be emphasized that from the academic point of view, security is a condition, not a process[1]. This approach is also supported by genesis of this term – in Latin "Secretarias" – understood as a condition of security, condition of certainty. What is more, the subject cannot be a process and a state as the same time (what is proposed in the second definition). In order to have an understanding of the cybersecurity, it is required to know what is security at the first place. The most common definition of security considers it as "the state of being free from danger or threat" (Oxford, 2017). Taking the argumentation mentioned above into consideration, the author propose is to adopt the third definition from "Republic of Poland politicly of the cyberspace protection". According to this document, cybersecurity is "a set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace" (Cyfryzacji, 2013).

Having a basic understanding of cybersecurity, based on the mentioned above definition it is necessary to define the term 'cyber defense'.

In literature, several definitions of the cyber defense exist in order to have a general understanding of cyber defense, the author presents three of them which gives a general overview of the problem of cyber defense.

According to the first definition, cyber defense is "actions [that] combine information assurance, computer network defense (to include response actions), and critical infrastructure protection with enabling capabilities (such as electronic protection, critical infrastructure support, and others) to prevent, detect, and ultimately respond to an adversaries ability to deny or manipulate information and/or infrastructure" (Dimitar Stevo Bogatinov, 2016). This definition presents defense as actions. Another definition shows the relations between cybersecurity and cyber defense "is all about giving an entity the ability to thwart cyberattacks on the go through cybersecurity. It involves all the processes and practices that will defend a network, its data, and nodes from unauthorized access or manipulation." (ecpiuniversity, 2017). Nevertheless, cyber defense should be related to the definition of defense with an added dimension of where this defense has to act – cyberspace. According to the most common definition of defense in the academic in community is "a counteracting of the enemy's assault" (Laprus, 1979). Taking this definition into consideration, cyber defense should be defined as a "counteracting of the enemy's assault in the cyberspace dimension".

Nevertheless, in related literature, something such as a systems approaches to security and defense exists. Based on these methods of understanding the issue, national security system is: "The national security system includes forces, equipment and resources designed by the state to carry out tasks in this area, respectively organized, maintained and prepared. It consists of a subsystem management and executive subsystems, including operational subsystems (defensive and protective) and subsystems of support (social

[1] Security – the state of being free from danger or threat (Oxford, 2017)

and economic)." (Narodowego, 2014). However, a defense system is "a coordinated set of management elements and executive elements, as well as the functions and processes implemented by them, as well as the relations between them. SOPs create all the forces and resources intended for defense tasks, organized, maintained and prepared for these tasks" ((MoD), 2009). It includes:

- Managing system;
- Military system – National Forces;
- Non-military system – which supports military system.

According to these definitions of national security and defense, there are two main approaches namely cyber defense and cybersecurity. It has to be pointed out that cybersecurity contains all of the country's or organization's resources focused to provide security in the cyberspace. On the other hand, cyber defense comprises of the military means and the resources supporting their activities and they were created in order to defend the country or organization against cyber threats.

The research literature contained in this chapter shows different approaches to cyber defense and cybersecurity by first defining cybersecurity as a state and cyber defense as a counteraction against cyber threats. This shows that cybersecurity cannot exist without cyber defense. The second approach, including a systemic point of view to the issue of security and defense. This method also shows that cybersecurity consists of cyber defense but also it shows that cybersecurity is more complex and it requires efforts made by the whole country or organization.

3. The need for a coherent cybersecurity strategy

The dependence of human life on technology is increasing year by year as people use the internet to get information, communicate with each other, etc. Moreover, digital technology is used to vote in elections, conduct bank transactions and other government and business activities. That is why cybersecurity is assigned not only to individual safety, but also to national security. The importance of the cybersecurity problem could be shown by the numbers of internet users.

An analysis of global internet usage and population statistic shows that the number of the internet users is still growing and at this time there are over 4 million users. Continents with the biggest percentage relation between the total population and internet users is North America (95%) and Europe (85,2%). These people are threatened by different kind of cybercrimes. The problem of cybercrime across the world has been shown in "Nation Cybersecurity Insights Report – Global Results". According to this report[2]:

- 978 million people in 20 countries were affected by cybercrime in 2017.
- 44% of consumers were impacted by cybercrime in the last 12 months.
- The most common cybercrimes experienced by consumers or someone they know include:
  - Having a device infected by a virus or other security threat (53%)
  - Experiencing debit or credit card fraud (38%)
  - Having an account password compromised (34%)
  - Encountering unauthorized access to or hacking of an email or social media account (34%)
  - Making a purchase online that turned out to be a scam (33%)
  - Clicking on a fraudulent email or providing sensitive (personal/financial) information in response to a fraudulent email (32%)

As a result, consumers who were victims of cybercrime globally lost $172 billion globally – an average of $142 per victim – and nearly 24 hours globally (or almost three full work days) dealing with the aftermath. The information mentioned

[2] The report was conducted based on information from: Canada, United States, France, Germany, Italy, Netherlands, Spain, Sweden, United Arab Emirates, United Kingdom Australia, China, Hong Kong, India, Indonesia, Japan, New Zealand, Singapore, Brazil, Mexico.

Table 1. World internet usage and populations statistic

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2017 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

Source: https://www.internetworldstats.com/stats.htm [access: 24/04/2019].

above shows the seriousness of the situation (Symantec, 2018, p. 4).

Furthermore, the report shows the common traits of cybercrime victims. Firstly, the report considers overconfidence in the cybersecurity of the users as a reason of becoming a victim of cybercrime: "Consumers who've fallen victim to cybercrime, emphasize the importance of online security more than non-victims, yet they're more likely to contradict their efforts through simple missteps" (Symantec, 2018, p. 5). Secondly, the report shows that 28% of the victims own more than one digital device. The last most important cause of becoming a cyber victim is "dismiss the basic", which means that the victims practice new security techniques such as "fingerprint ID (44%), facial recognition (13%), pattern matching (22%), personal VPN (16%), voice ID (10%) and two-factor authentication (13%). What is more, 20% of cybercrime victims globally use the same password across all online accounts and 58% shared at least one device or account password with others" (Symantec, 2018, p. 5).

Reasons such as "the same password in several devices or accounts" and the data mentioned above related to becoming a cyber victim may have shared denominator – lack of knowledge of user about cybersecurity.

However, cyber threats impend not only individuals users, but also (and maybe mainly) to nations, and the sovereignty and independence. The expenditure on military purposes are growing "World military expenditure was $1686 billion in 2016, an increase of 0.4 percent in real terms" (Nan Tian, 2017).

This money is spent not only on soldiers and regular equipment such as tanks, aircrafts, and ships, but also a cyber operations capabilities. More than 30 countries are developing offensive cyberattack capabilities, according to US chief of intelligence James Clapper (Ranger, 2017). The problem of cyberattacks has increased recently. In 2017, U.S. intelligence agencies accused Russia of interfering in the election in 2016. Recent newspapers headlines said that United Stated and Britain blame Russia for global cyberattacks: "The United States and Britain on Monday accused Russia of launching cyberattacks on computer routers, firewalls and other networking equipment used by government agencies, businesses and critical infrastructure operators around the globe." (Jim Finkle, 2018)

Taking all of this into consideration, due to the many types of cybercrimes that threaten not only individuals users, but also entire nations, connected with different ways of carrying out cyber threats, and considering of the numbers of users and number of cyber victims across the world, with the common traits of the cybercrime victims shows up one very important thing – strong cyber resilience needs a collective and wide-ranging approach. This approach should be included in the multinational strategy of cybersecurity and cyber defense.

4. Developing acoherent cybersecurity strategy

First of the all, before giving an answer to the question: "how can a coherent cybersecurity strategy be developed?", it is crucial to know what exactly such a strategy is? In general, the strategy is a praxeological category, which means that it concerns the efficient action of everything that has a part in this action. Gen. Stanisław Koziej defines security strategy as "theory and practice of managing the security issues by a chief decision-maker (individual or collective), in particular setting the security goals and methods of achieving them" (Koziej, 2011). According to this definition, in order to build a coherent cybersecurity strategy the coherent goals and method to achieve them need to be defined.

It is important to point out that international organizations such as NATO and the EU are creating a cyber defense strategy. In the European Union the "European Union Agency for Network and Information Security" has been created. Agency has a key role to play in strengthening EU cyber resilience and response, but is constrained by its current mandate. NATO has created the Cyber Defense Committee, the lead committee for political governance and cyber defense policy in general, providing oversight and advice to Allied countries on NATO's cyber defense efforts at the expert level. At the working level, the NATO Cyber Defense Management Board (CDMB) is responsible for coordinating cyber defense throughout NATO civilian and military bodies.

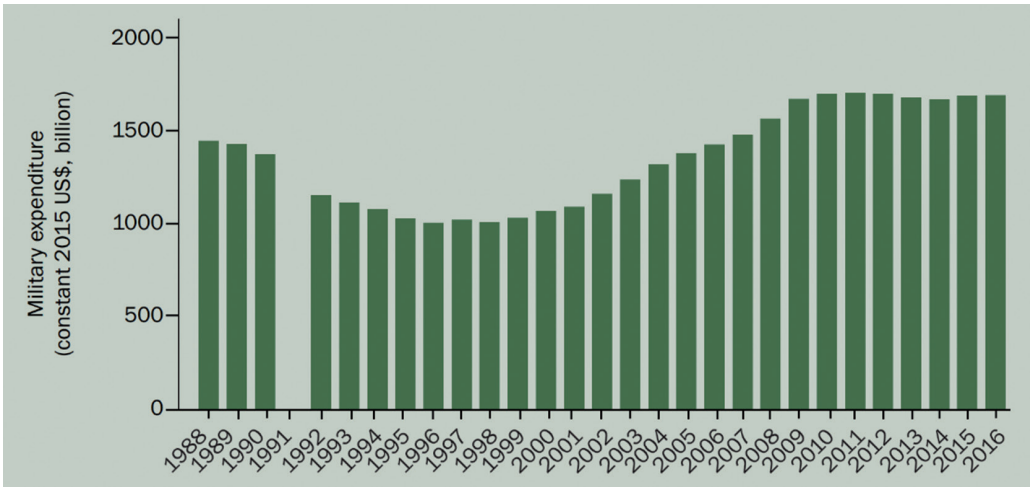

Figure 1. World military expenditure, 1988–2016
Source: Nan Tian, Aude Flerurant, Pieter D. Wezeman, Siemon T Wiezeman, Trends in world military expenditure, 2016, SIPRI Sact Sheet, April 2017.

Based on the research carried out, the cyber defense is only one part of cybersecurity. Due to a wide range of cyber threats from individuals to nations, the systems approach to cybersecurity has to be

implemented. That requires a complex and strategic point of view which regards to this issue. This has been confirmed in Cybersecurity Strategy of the European Union. ”Given that threats are multifaceted [cyber threats add by D.M.], synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU” (European Commission, 2013).

There are several different approaches to create a cybersecurity strategy. The EU strategy of cybersecurity present five strategic priorities:

1. Achieving cyber resilience;
2. Drastically reducing cybercrime;
3. Developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);
4. Develop the industrial and technological resources for cybersecurity;
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

The National Strategy to Secure Cyberspace identifies six major actions and initiatives to strengthen U.S. national security and international cooperation (U.S. Homeland Security, 2003):

1. Strengthen cyber-related counterintelligence efforts;
2. Improve capabilities for attack attribution and response;
3. Improve coordination for responding to cyberattacks within the U.S. national security community;
4. Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global “culture of security;”
5. Foster the establishment of national and international watch-and-warning networks to detect and prevent cyberattacks as they emerge;
6. Encourage other nations to accede to the Council of Europe Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive.

The approaches presented above to the priorities and actions treat cybersecurity too vaguely and focus mainly on cyber defense. According to the systems approach to cybersecurity, it is necessary to involve all elements of security such as social, economy, defense and safety.

5. Conclusion

More and more states are developing cyber forces for military purposes in preparation for a new kind of cyber war. Moreover, the cyberattacks have a destructive effect on the daily life of individual users, but also for nations and international organizations. The research conducted in this article shows the need for the development of a coherent cybersecurity strategy.

Cyber threats have become one of the new main threats for national security in both times of peace and war. The data presented in this article shows the growing threat from cyberspace. To promote cyber resilience in the international community, both public authorities and the private sector must develop capabilities and cooperate effectively. We must build on the positive results achieved via the activities carried out to create not only a defense system against cyber threats, but also to create the whole cybersecurity system.

Based on conducted research the coherent cybersecurity based on system approaches can be achieved by connecting the effort of all national and international systems:

- **Social system**
  - Changes to the mind-set of society – Societies has to be educated. The assumption must be that cyberspace is bound to be disrupted and degraded. This way of thinking must be mainstreamed into training, education, planning, etc.
- **Defense system**
  - The key capabilities to be prepared to execute mission assurance in cyberspace
  - Key stakeholders to focus on identifying vital military assets that are the most critical from the mission assurance point of view, and concentrate on their protection in the first place.
  - Cyberattacks and the cyber threat landscape to be viewed as closely interlinked with other types of attacks, mainly conventional attacks.
- **Security system**
  - Preparation of the organization to the cyber-attack.
  - Single methodology for risk assessment in the whole organization.
  - A database which would contain information about identified vulnerabilities.
  - Limits for risk levels at each level of the cybersecurity system hierarchy.
- **Economic system**
  - Cybersecurity supported by economy effort.
  - Manage IT resources and infrastructure so it facilitates the data collection and processing in a systematic way. (Bujek, 2018)

The action mentioned above presents the systems approach to cybersecurity. This approach gives a possibility of focusing all nations and/or organization resources to achieve one common goal, i.e. cybersecurity. What is more, in order to achieve coherent cybersecurity, it is most important to convict members of the organization to collaborate and exchange information about cyber threats.

The digitalization of our daily lives has opened up not only new possibilities with wider impact, but has also created a new kind of cyber threat. As a result, security sector must be ready to improvise, adapt to and overcome challenges. Improving intra-organization cooperation might be a means to the end, i.e. security in cyber space. Moreover, the systematic approach to cybersecurity has to be further developed. This approach will help us to focus all national and organizational resources on the problem.

Bibliography

[1] *Strategia Obronności Rzeczypospolitej Polskiej.* Warszawa 2009.
[2] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Warszawa 2015.
[3] Bujek, M. (2018). Cybersecurity as the basis for state and society security in the 21st century. *Safety&Defense*, p. 6.
[4] Cyfryzacji, M.A. (2013). *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.* Warszawa.
[5] Dimitar Stevo Bogatinov, M. B. (2016). *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare.* Macedonia.
[6] Ecpiuniversity. (2017). *ecpi university*. https://www.ecpi.edu/blog/what-is-cyber-defense
[7] E*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels: European Union 2013.
[8] European Cybersecurity Forum. (2017). The 3rd Annual Public Policy Conference dedicated to strategic aspects of cybersecurity. *Cybersec2017*, (str. 24). Kraków, Poland.
[9] Jim Finkle, D.C. (2018, April 16). https://www.reuters.com/article/us-usa-britain-cyber/u-s-britain-blame-russia-for-global-cyber-attack-idUSKBN1HN2CK
[10] Koziej, S. (2011). Bezpieczeństwo: istota, podstawowe. *Polityczno-Strategiczne Aspekty Bezpieczeństwa*.
[11] Laprus, M. (1979). *Leksykon wiedzy wojskowej.* Warszawa: Ministerstwo Obrony Narodowej.
[12] Nan Tian, A.F. (2017). Trends in world military,2016. *SIPRI Fact Sheet*.
[13] *Strategia Bezpieczeństwa Narodowego.* Warszawa 2014.
[14] NICCS. (2018, 08 18). *National Initiative For Cybersecurity Careers And Studies*. https://niccs.us-cert.gov/
[15] Oxford. (2017). *oxforddictionaries*. https://en.oxforddictionaries.com/definition/security
[16] Ranger, S. (2017, January 05). *ZDnet*. Pobrano z lokalizacji https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/
[17] Symantec. (2018). *Norton Cyber Security Insights Report Global Results.* Mountain View: Symantec Corporation.
[18] U.S. Homeland Security. (2003). *The National Strategy to Secure Cyberspace.* Washington.