DOI 10.34054/bdc000

BEHIND THE DIGITAL CURTAIN. CIVIL SOCIETY VS STATE SPONSORED CYBER ATTACKS

Proceedings of the conference

Promote Ukraine

Proceedings of the conference

BEHIND THE DIGITAL CURTAIN. CIVIL SOCIETY VS STATE SPONSORED CYBER ATTACKS

DOI 10.34054/bdc000

Brussels - 25/06/2019

Promote Ukraine

Publisher:
Promote Ukraine

Layout: Taras Vashkiv
Design: Maksym Stepanov

ISBN/EAN:978-90-9031770-0
DOI 10.34054/bdc000

Sponsors and partners of the conference

Djannet.com
East West Mentor
DigitYser
CyberDesk
Institute of Innovative Governance
БізнесWoman
Хмельницький національний університет
Львівський національний університет ім. І. Франка
Київський національний економічний університет
ім. В. Гетьмана

The authors are responsible for the editorial staff, the content and authenticity of the data, as well as the establishment of facts of plagiarism of materials contained in the collection of the conference.

За редакцію, зміст і достовірність даних, а також встановлення фактів плагіату матеріалів, розміщених у збірнику конференції, відповідальність несуть автори.

Contents

DOI 10.34054/bdc001

Behind the Digital Curtain: A Look inside the Russian Information War against the West

Marta Barandiy, Dr. iur.[1]

Introduction

In the post-truth world of Putin and Trump the international law is being spurned by some states; a development led by the two most powerful permanent members of the United Nation's Security Council. In the past few years this has resulted in the obliteration of trust between different public and private actors of international relations, and everyone became self-righteous (Mäger, 2016; Herszenhorn, 2018; Applebaum, 2019; Harding, 2018).

Next to journalists, lawyers, economists and political scientists, who are all experts on media, law, economic and political life respectively, everyone with access to a keyboard also claims to be an expert in these issues (i.e. bloggers, opinion leaders). The moment has come when all the crises - economic, ecological, migration, informational and political - are intertwined, and nobody can entirely figure out where they originated and how to address them but many declare to have «the solution» (Mäger, 2016; Herszenhorn, 2018; Applebaum, 2019; Harding, 2018).

[1] Ph.D. in International Law, Of Counsel at Asters law firm, Founder and Board Director at Promote Ukraine, Lecturer at Ukrainian Free University Munich

People are no longer observers but rather participants and targets of all possible conflicts that happen «remotely» – ideological and political, within and outside their country. The consequences of this «participation» have already affected their personal lives: religious-ethnic conflicts, Brexit, rise of the extreme right on the European continent, etc. (Nagan & Hammer, 2008).

At the same time, it is harder for scientists (scholars) to reach their potential readership, their expertise discarded when inconvenient. Moreover, the quality of research materials has decreased and it has become difficult to check the reliability of their sources. To this comes the increasing noise generated by ever more Internet outlets with dubious funding and nefarious goals, which disseminate rumors, untruths, historic revisionism, and even fake studies (Karnaushenko, 2015; Jeangène; Escorcia; Guillaum & Herrera, 2018).

Loss of control over dissemination of information that in seconds can reach millions of people, and can cause emotional outbursts and social unrest, is one of the consequences of globalization and the spread of the Internet which are both impossible to reverse.

The extent to which the information disorder has developed in the world is also the result of a «hybrid war», which has been waged by Russia, one of the biggest countries that have resisted globalization for over 20 years. Russia is trying to clench the past, to preserve what it calls «classical relations» between the states, although «the classical relations» between states (as Russia understands them) are not feasible anymore, due to the emergence of millions of «actors in the digitalized world», who have the ability to actively influence the processes of coexistence. As a member of the UN Security Council, Russia continuously blocks resolutions that

could solve burning issues of international relations (Syria, Venezuela, and Ukraine etc.). Russia deliberately paralyzes international public law and weakens interdependence between states, triggering political and information chaos in liberal democracies (Lukas & Pomeranzev, 2016; Chivvis, 2017; Gerasimov, 2013).

At the same time, Moscow experiments the introduction of controls over information within and outside its borders. Having problems with the freedom of speech (Report of the Freedom House on Russia, 2019), Russia undermines this norm in other countries through the activities of its agents of influence (Kamian, 2018; Mäger, 2016; Abrams, 2016). Russia creates conditions in which liberal democracies are forced to debate about the introduction of censorship for the sake of national security and sovereignty (Barandiy, 2018). As an example, citizens, politicians and officials in a country like Ukraine blame the existing licensed media for being Kremlin-mouthpieces, and call for «active or passive defense» against the Kremlin's infiltration in their national discourse (Barandiy, 2018). The consequences of such allegations vary from counter-propaganda (as active defense) to the attempts to shutdown certain media outlets (as passive defense). The urgency of the reaction depends on the level of the freedom of the media in a country, and whether it suffers from or is under imminent risk of military aggression of Russia.

Both, the military intervention, which is forbidden in international law, and interference in other states' affairs through information, which is not forbidden in international law, are inherent to the concept of foreign policy of Russia. Though the second aspect is often considered to be a form of war not only by Russia (which will be discussed below) but also by many Western states – Russia's war against liberal democracies aims to force back the international community to the «classic relations between states» time, without

supranational bodies like the EU or NATO (Syuntyurenko, 2015; Putin, 2014; Pieters, 2018).

One active actor that resists this «war» is civil society[2]. NGOs and activists worldwide cooperate with public and private actors, organize events and produce reports with the goal to raise awareness on the level and consequences of «interference». By now they have not managed to streamline the «information disorder» as the approaches of such «interference» differ depending on terminology, used in the states of the origin of such NGOs.

There is a terminology that has been circulated in the communication flow of legal and political systems of nation states, but only few of them are actually regulated by national or international law. The officials and experts use active measures (Russia, USA), interference in internal affairs (Russia) or election meddling (USA), hybrid or ideological war (analysts worldwide), information aggression and information attacks (Russia), psychological operations, fake news and disinformation (the USA, the EU), manipulation of information (France), Russian propaganda (Ukraine), propaganda of war and hate speech (Council of Europe, OSCE, Germany), cyber attacks (worldwide) etc.

Absence of common terminology amplifies the chaos and weakens the resistance of states against Russia's extraterritorial information influence operations (Ristolainen, 2017). Nevertheless, it is of paramount importance to establish common definitions because of the tight technological and human interconnections in the current global world order.

First of all, it is necessary to establish sources in politics and law of Russia that aim at information influence of the

[2] e.g. InformNapalm, Stopfake, EuromaidanPress, Bellingcat, EU Disinfo Lab etc.

Kremlin on other states. Russia acts in a «bubble of interpretations»; the purpose of this study is to connect the actions undertaken by Russia to the terminology Russia itself uses itself for such acts and «reciprocal» actions undertaken by other states against Russia. This is needed to understand the approach, worldview and mindset of the Kremlin's power elites and for the West to be able to resist or to adapt to the conditions imposed by Moscow (Bennett, 1995).

In this paper, I intentionally do not connect Russia's «measures» to officially existing terms in Russia as its actions are considered by Russians to be a «defense». At the same time, I do not connect Russia's «measures» to any existing western term or definitions, in order to avoid the confusion between those definitions and the findings in this study.

I propose to use the term that contains elements of Russia's «measures» that would resonate with all the states that have felt their impact. This term is «influence through information» («information influence») (Scott, 2016).

The purposes of the study are 1) to determine the place of «information influence» in Russia's concept of «interference in sovereignty» as interpreted by the law, science and rhetoric of the Kremlin, and 2) to offer a definition of ***«information influence» in relation to «interference in sovereignty»*** as defined by the Kremlin and, at the same time, as experienced by the Western states.

Terminology, used by the Kremlin. Basics

Information influence of Russia on foreign states has been systematically introduced into its concept of sovereignty after 2011 (Ivashov, 2012). The dates and chronology of the introduction of the concept of «information sovereign-

ty» are tied to past elections in Russia, which for decades have kept in power the same people by just rotating their positions. Thus, after Medvedev's «presidency» Putin's return to power took place in March 2012 (Pavlovskiy, 2014; Ziegler, 2012; Budraitskis, 2014). In May 2012, Igor Ashmanov, one of the founders of the Russian Internet called «Runet» talked about the necessity of introducing the notion of «digital sovereignty» (Коваленко, 2019). In February 2013, General Valeriy Gerasimov came up with the «ideology» of information aspects of geopolitical confrontation (HlavRadyoOnlain, 2012; Kasperskaia, 2014). In 2014 Putin's aide and advisor on Ukraine Vladislav Surkov (who in 2006 had already introduced the idea of «sovereign democracy») published an essay about «non-linear war» – Putin's method of information influence on Ukraine and other countries (Surkov, 2006; Dubovitsky (Surkov), 2014).

In internal affairs and in the international arena Russia is adopting laws and proposing agreements that reflect its approach to state sovereignty, the concept of (non-)interference and information security. These documents are governed by a specific terminology that is used by the state institutions involved in the drafting.

In September 2011, Russian Ministry of Telecommunication prepared the Convention of Information Security for the UN. Though this was not accepted by the majority of the Western states its content is relevant for understanding the Kremlin's readiness to introduce the state of information sovereignty in Russia with the accompanying reactive and pro-active measures in relation to foreign states.

The preamble of the Convention mentions that «political authority in connection with governmental policy issues related to the Internet is a sovereign right of States...». (Convention on International Information Security, 2011)

Art. 1 declares the aim of the Convention which is «to act against the use of information and communication technology to violate international peace and security, as well as to set up measures ensuring that the activity of governments in the information space will» among other:

- «be compatible with the right of each individual to seek, receive, and distribute information and ideas, as is affirmed in UN documents, while keeping in mind that this right may be restricted through legislation to protect the national and social security of each State, as well as to prevent the wrongful use of and unsanctioned interference in information resources»; (Convention on International Information Security, 2011)
- «guarantee the free exchange of technology and information, while maintaining respect for the sovereignty of States and their existing political, historical, and cultural specificities».(Convention on International Information Security, 2011)

Art. 2 defines the term **«information warfare»**–«confrontation between two or more states in the information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out **mass psychological campaigns** against the population of a state in order to destabilize its society and the government; as well as forcing a state to take decisions in the interests of its opponents». (Convention on International Information Security, 2011)

One more interesting term defined by the Convention is **«information weapon»** – «information technology, means, and methods intended for use in information warfare». (Convention on International Information Security, 2011)

Art. 6 puts limits on the states requiring that they refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between states or provoking «information wars»; that they refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another state; that they refrain from using information and communication technology to interfere with the internal affairs of another state; that they refrain from slander as well as from using insulting or hostile propaganda to intervene into or interfere in the internal affairs of other states; that they have the right and duty to take action against the proliferation of untruthful or distorted messages which could be considered as a means of interfering in the internal affairs of other states or as damaging world peace and security etc.

At the same time «this Convention will not apply in those cases when the actions in question are undertaken within the information infrastructure of one state, citizen, or corporation under the jurisdiction of that state, and the effects of those actions are only felt by citizens and corporations under the jurisdiction of that state, and no other state has grounds to assert its jurisdiction» (Art.3).

As we see the terms «information war», «information weapon», «mass psychological campaigns» have been in use and waiting for their «introduction in law» by Russia for many years.

Recent developments in Russia concerning a possible internet isolation introduced through a draft law reflected the Kremlin's idea of digital (internet) sovereignty (О внесении изменений в Федеральный закон ... № 608767-7; Danilenkov, 2017; Ristolainen, 2017). The digital sovereignty though is only a part of a wider concept of information sovereignty in Russia. This exact concept has been advocated

by Igor Ashmanov since 2012-2013 (Yarovaya & Ashmanov, 2013; Diplomatrutube, 2013). It justifies the control by the Russian government over information distribution in the country and securing the «independence» of this information from «external influence».

Igor Ashmanov is one of the most influential people from the IT industry in the entourage of the Kremlin's key decision-makers. He gives lectures on information sovereignty, also to hackers, so called *kiberdruzhynniki* (Tsarhrad TV, 2017), and participates in the hearings by the Russian lawmakers (Diplomatrutube, 2013; ABstudiya, 2018; Zappone & Massola, 2019). In 2018 he was Putin's confidant during the Russian presidential election. His and his partner Natalia Kaspersky's products cover over 50% of the Russian information security market (Kasperskaia, 2014). Because of their world view they expose in their advocacy activity and their business interests, it is natural that they lobby for the creation of a propaganda system and for the introduction of **information sovereignty** ideology, which consists of an **information shield** and an **information sword**, for both of which naturally their products should be used[3].

The «information shield» consists of reactive instruments to protect the Russian information space from external interference, while the «information sword» consists of attacking or preventive instruments of interference into information flows of foreign states, both aimed at «the disruption of the information sovereignty of the adversary» (Life TV, 2012).

[3] Natalia Kaspersky is owner of IT security company «InfoWatch» and social media «reputation scanner» «Kribrum», currently she leads the working group on cybersecurity of the Russia's government program «Digital Economy»; Igor Ashmanov is partner of Natalia, he is owner of the company «Ashmanov& Partners», he is believed to be both the inspiration and the executorof the Kremlin's concept of internet sovereignty.

According to Ashmanov, a state needs information and cyber-forces consisting of hackers in order to realize these information attacks. **Information attacks** are the «sword» of the information sovereignty, and «they are not forbidden by international agreements». What is important, according to Ashmanov, with the help of information attacks «military intervention in a foreign state can be justified» (Ashmanov, 2013; Tsarhrad TV, 2017).

The report «Facts of the interference in the information sovereignty of Russia before presidential elections. Preparation of Maidan technology in Russia», authored by both the Institute of Strategic Studies and Forecast (further ISSF) and the «Antimaidan Movement» (Елисеев, 2015), proposed to equate the attacks on the information sovereignty of Russia with military aggression, and to consider the foreign challenge to the propaganda of the Russian state aimed at the people of Russia as an encroachment on the Kremlin's information sovereignty (Geopolitika.ru, 2017).

The «Antimaidan Movement» was initiated by the Russia's Great Fatherland Party, which is co-chaired by the above-mentioned Igor Ashmanov. Although ISSF head Dmitriy Yegorchenkov participated in the drafting and presentation of the report, it is still not clear who «ordered» the report and what impact it has had in the Kremlin (ISIP RUDN, 2017).

Many of the terms used by the Kremlin, have been elaborated on in another document - the Report of the Temporary Commission of the Russian Federation Council «For the **protection of the state sovereignty** and prevention of the **interference in the internal affairs** of the Russian Federation» (further the «Report») that was established with Resolution of the Russian Federation 14 June 2017 №172 (further the «Temporary Commission»).

The Temporary Commission has investigated «facts of interference» in the sovereignty of Russia. Its task has been to provide Russia's Parliament, Ministries, the Central Electoral Commission, the Prosecution Office and other state institutions of the Russian Federation with recommendations on how to restrict possible «interference» in the internal affairs of Russia by international actors in the future.

The Temporary Commission is Russian «response» to the US-investigation on the Russian meddling in the 2016 presidential elections and other reciprocal acts that followed after these allegations (Заверняева, 2017). Two chapters of the Report are dedicated to the history of «American interference» in other states, particularly, in Russian affairs. The US norms of resistance against Russian influence in the world like «Patriot Act», «Freedom Act», «Magnitsky Act» and «Ukraine Freedom Support Act» are also mentioned in the Report.

The head of the Temporary Commission Andrey Klymov admits that «it is difficult to differentiate informing from interference» (Россия 24, 2017). This narrative is easily manipulated by the Kremlin who at home calls information coming from foreign sources an interference and restricts it; while disguising its own information interference as legitimate information and insists it must not be restricted because Western governments guarantee «freedom of speech» and «freedom of media».

Terms that have been used to expose foreign influence are **«foreign agents»** and **«undesirable organization»**. Politically active NGOs in Russia that receive grants from abroad are called «foreign agents» by the Russian government (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, p. 56). At the moment of establishment of the Temporary Commission

more than 90 NGOs had been identified as foreign agents, and by 2017, 11 organizations were designated as undesirable (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, p. 58).

Another interesting term is «vbros» – «news stories» that are «dumped» into social media, «washed» through the mass media in order to appear again in the social media as legitimate news (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, p. 59; Gostev, 2017). «Vbrosy» are dangerous as they can provoke the spread of false information about individuals and institutions at an impressive speed in huge volumes, «igniting people's emotions».

The other terms, used by the Russian decision and opinion makers are **«information confrontation», «containment of Russia», the collective West, «complex measures», «asymmetric measures», «complex approach», active operations, agent of influence, ideological diversion, ideological aggression, active measures, «sovereign expertise»** (scanning of every draft law on resistance to interference) (Komov, Korotkov & Dylevski, 2007; Belenkov, Gyulazyan & Mazlumyan, 2018; Ruptly, 2019).

Russian information influence on foreign states in terms of sovereignty

The breach of the sovereignty of foreign, often neighboring states by Russia is inherent to its modern doctrine of international law, and its approach to foreign policy is based on force, rather than the law, as the means to achieve its geopolitical goals (Tolstykh, 2016). Although «in theory» Russia respects international law, in reality it places the suprema-

cy of national interests over internationally agreed norms; it brings up historical, religious and other non-recognized scholarly arguments to justify its actions in international relations and prioritizes bilateral relations over multilateral agreements (Klishas, 2018; Mäger, 2016; Abrams, 2016).

For the last two decades, Russia has tested how far it can push the boundaries of tolerance of the international community to the breach of international law (Report of the Standing Committee on National Defence of the House of Commons (Canada), 2018). So far, only the reaction to the «hybrid interference» in Ukraine has had negative consequences for Russia in face of sanctions or dismissed participation in the decision-making process of some international organizations. Despite the reaction of the West, Russia has not changed its approach towards international law. Inside the country state media «used» West's reaction to boost popularity of Russian leadership (Kazun, 2016; Domańska, 2019). In international relations Moscow has tried to impose its vision of the «rightful transactions» onto the governments of other states, e.g. through UN Security Council meetings. Whenever Russia's message fails through official communication, it moves into attempting to replace foreign political decision-makers with the ones friendlier to Kremlin's «transnational activities» (Shekhovtsov, 2017).

By manipulating technology and achievements of Western democracies, such as the concept of human rights Russia tries to undermine Western democracies' values. For example, it «interferes in the sovereignty» of the Western states by financing their radical parties, undertaking information and cyber attacks, and stocking social divisions.

During the referendum campaigns in the UK and the Netherlands, as well as during the elections in Germany, Austria, Czechia, Italy, the United States and France, Russia engaged

in «informational-psychological pressure» on the electorate with the aim to weaken certain candidates and prevent inconvenient outcomes for the Kremlin (Bradshaw & Howard, 2017). In all of them the fear-mongering narratives that included migrants, Islam, and non-traditional life-styles were used.

The results have often been useful for Moscow for destabilizing Europe: the UK decided to leave the EU although a majority of the population as well as some national authorities now realize that it may be financially and reputationally ruinous; in Germany, for the first time since the World War II the far-right took seats in the parliament; in Austria and Italy the far-right entered the government.

One may argue that it is not proper to conclude that the narratives created by the Kremlin during the political campaigns in the above-mentioned states had swayed the outcome of the referenda or elections resulting in choosing Kremlin-friendly ideas and governments. While the exact effect of the influence has been empirically challenging to establish, the attempts to influence are beyond doubt (Political Warfare: Competition in a Cyber Era (Policy Paper), 2019; Bayer, Bitiukova, Bard, Szakács, Alemanno & Uszkiewicz, 2019).

The Temporary Commission claims that Kremlin's actions are solely the responses to the «information, sanction and diplomatic war that has been waged against Russia since 2014» from the moment of the «coup d'état» (the way the Kremlin calls Revolution of Dignity or «Euromaidan») in Ukraine, but, as shown above, Russia started claiming information sovereignty long before the 2014 events in Ukraine.

«Influence through information» in Russian interpretation

«Russia's official military doctrine, as well as statements by top Russian generals, describe the use of false data and destabilizing propaganda as legitimate tools, and information as another type of armed force (military power)», – says European Union Commissioner for Security Julian King (Barbarosie & Coalson, 2018).

Following every new offence originating from Russia, Western countries' leaders declare that the Kremlin meddles in their internal affairs – in the information space, cyber space, and political arena of their nations. Nevertheless, these statements have not yet shaped a united Western vision of how to counter this Russian foreign policy strategy. Whether respective governments realize it or not, all the acts of the Kremlin towards other states are part of Russia's system of international relations and have to be analyzed in their complex entirety.

Peter Dickinson writes in his article «From Crimea to Salisbury: Time to Acknowledge Putin's Global Hybrid War» that the West does not realize that the Kremlin's attacks are not isolated from one to another; its actual goal is to interfere, and these interferences constitute a «single coordinated global campaign» (Dickinson, 2018). Therefore, the problem is that the West mobilizes its power and resources to repel individual Russian attacks separately instead of learning about the Russian integral approach and preparing appropriate response.

At the same time, it has to be considered, that the measures of the Kremlin towards other states are often not coordinated and not thought-through, as they are executed by the different independent from each other actors within Russia's government (DenTV, 2019). Yet the common ground of these

measures implies restraining of the globalization processes, although they result in self-isolation of Russia from the liberal international community (Putin, 2014).

Russia's approach to secure «national interests»

Russia's approach to secure national interests differs from the one of the liberal states. It is based on realism rather than liberalism or constructivism in international relations (Ziegler, 2012). Thus, international law in the interpretation of the Kremlin is the law to which other states agree to adhere, but if it constrains the national interests of Russia, the latter should prevail (Mäger, 2016). At the same time, Russia accuses other states that prioritize national interests over international agreements of breaching international law (The Ministry of Foreign Affairs of the Russian Federation, 2018).

Contrary to the generally recognized principle of sovereign equality, Vladimir Putin as well as his advisors do not consider small states that are «unable to survive entirely by their own means» to be sovereign. Thus, Igor Ashmanov insists that Belgium and Germany, for example, are not sovereign states (Tsarhrad TV, 2017).

According to the Russian parliamentarians who drafted the Report on Interference in the Internal Affairs of Russia (which will be discussed below) only Russia, the US and China have the «highest level of sovereignty» (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018). Truly («globally») sovereign states are those states that have veto power in the UN Security Council, officially possess nuclear weapons and have special capabilities in the field of aerospace.

Vladimir Putin himself believes that there are only a few fully sovereign states in the world, stressing that the states that participate in military unions have only limited sovereignty (Putin, 2017). During the Valday Forum in 2007 Putin said that «for Russia, sovereignty is not a luxury, but the condition of survival in this world... Either Russia will be entirely independent and sovereign, or it will not exist at all, claiming that he was the only one able to ensure such independence. In terms of Putin's vision of foreign policy, Russia is ready and willing to use force to «protect its sovereignty» (Tkachenko, 2017). By creating this link between national interests (independence, existence of the state) and his persona, Putin cemented his regime for decades.

Internationally, Russia positions itself as a «defender» of «classic» international law that «allows regimes to act with impunity within the state borders even in case of crimes against humanity» (Россия24, 2018). This follows from the Kremlin's refusal to follow the approach of the liberal international community to include human rights as a factor in international relations. According to Putin's entourage, the concept of human rights is an instrument of interference and it is being used to «break down sovereignty» of states (Ashmanov, 2013). The vision of the Kremlin is that the «human rights in Russia are rights only as long as they do not contradict traditional values of Russian society», and that «no decision of an international court should prevail over the decision of Russian national courts» (Medvedev, 2018; Østbø, 2017). In these terms, in order to «protect national interests» (read regime) (De Mesquita, 2006). Russia has to be «secured» from what it calls «interference from outside», including the concept of human rights.

(Non)-interference as defined by Russia.
What is interference in the sovereignty of Russia?

According to the Temporary Commission of the Russian Federation for protection of sovereignty, the interference in the internal affairs are activities of foreign states, their legal or natural persons, their associations and unions, with the aim to change the constitutional order, territorial integrity of the Russian Federation, its internal and foreign policies, composition and structure of the state and local organs through elections, media, NGOs and educational programs (list non-exhaustive); these activities are beyond the generally recognized principles of international law or agreements of the Russian Federation with other states.

Moreover, the Temporary Commission has suggested to introduce this definition of interference into the law of the Russian Federation and investigate accordingly.

Forms of interference according to the Temporary Commission
(Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018)

According to the Temporary Commission, interference[4] is a direct or non-direct foreign support for political forces in certain states as well as the entire complex of measures of influence on the citizens of foreign states in order to change their behavior, form certain stereotypes, destabilize state institutions etc. This is political interference and it happens through informational and organizational means, using NGOs, foreigners, diaspora, «special operations», bribing of the state officials, politicians and journalists.

[4] non-military interference

The Temporary Commission considers the following to be interference:

a. Establishment and support of NGOs that participate in the political processes in «the interests of a foreign state», for example, when they are financed by the USA, the UK or the EU or when their leaders do study in the US and Baltic states. Such «foreign studies» are considered to be «anti-Russian» by the Temporary Commission.

b. Cooperation with educational institutions, financing of education programs with the goal of «further control» of this field in order to orient it to the Western model in political, economic, and social aspects.

c. Instrumentalization of mass media and social media to discredit the state institutions, the Kremlin's power apparatus and political leaders.

d. As separate forms of interference, the Commission mentions the «discreditation» of the Russian Orthodox Church; «politicization» of sport like exposing Russia's state sponsored doping program, and «instrumentalization» of the environmental issues.

According to the Temporary Commission, other forms of «interference in the internal affairs of Russian Federation» are stimulation of youth protests, meddling in elections, inciting ethnic conflicts or conflicts in the republics of the Northern Caucasus, the Volga region or in Crimea with the involvement of Crimean Tatar Mejlis-representation, and maligning of the Russian economic and political life in the world arena, and the use of such information inside of Russia.

The Temporary Commission considers the call of the Western leaders not to recognize the results of the elections of the

President of the Russia in Crimea to be an interference and breach of the Universal Declaration of Human Rights.

Legal and political acts and norms related to the «protection of sovereignty» of Russian Federation from foreign interference

The most relevant documents of strategic planning in this field are the Yearly address of the President of the Russian Federation to the Federal Assembly of Russian Federation, Concept of the foreign policy of the Russian Federation (Об утверждении Концепции внешней политики Российской Федерации № 640), Strategy of the national security of the Russian Federation (О Стратегии национальной безопасности Российской Федерации № 683), Doctrine of Information Security of the Russian Federation (Об утверждении Доктрины информационной безопасности Российской Федерации № 646), the Military Doctrine of the Russian Federation (О военной доктрине Российской Федерации № 146), the Strategy on the Development of the Information Society from 2017-2030, and a State Program «Digital Economy» 2017.

The following norms of Russian law are related to the «protection of Russia from interference»:

a. State service can only be performed by the people who have only Russian citizenship (О государственной гражданской службе Российской Федерации № 79-ФЗ);

b. Persons who take decisions related to the sovereignty and national security are forbidden to have accounts in foreign banks (О запрете отдельным категориям лиц открывать и иметь счета (вклады)... № 79-ФЗ);

c. NGOs that get finances from foreign sources and are politically active on the territory of the Russian Federation get the status of «foreign agents» (О внесении изменений в отдельные законодательные акты Российской Федерации ... № 121-ФЗ);

d. There are restrictions for the citizens with dual Russian-American citizenship to be members or heads of politically active NGOs; The activities of the politically active NGOs that get financing from the citizens or organisations based in the US can be suspended (О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека… № 272);

e. US-citizens who have been convicted of the crimes against Russian citizens are banned from entering the RF (О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека… № 272);

f. With the Law №129 of 23 May 2015 the definition of «undesirable organization» has been introduced. Undesirable organisations are those, whose activities constitute a «threat» to the constitutional order of the Russian Federation, or the defence and security of the country. Managers of such organizations are subject to criminal liability while foreign leaders of these organisations may be banned from entering the territory of Russia. Organisations, designated as undesirable are National Endowment for Democracy, Open Society Foundation, Open Russia, International Republican Institute. In January 2019, the case against the activist of the Khodorkovskyy's «Open Russia» Anastasiia Shevchenko has been introduced. The case became famous as the daughter of Anastasiia who had been disabled from birth and needed thorough care, got severely ill and died one week after her mother was detained.

g. Foreigners may not possess or manage more than 20% of the shares of a Russian media organization (О внесении изменений в Закон Российской Федерации «О средствах массовой информации» № 305-ФЗ);

h. Amendments to the Code of Administrative Offences related to «defamation of government». Fines and arrest up to 15 days have been foreseen for the breach of this law (О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека... № 272);

i. Amendments to the Law on Information and to the Code of Administrative Offences related to «fake news», have been adopted in March 2019 (О внесении изменений в Кодекс Российской Федерации об административных правонарушениях № 28-ФЗ). The Rosskomnadzor will block the websites that publish «fake information» under the label of factual messages.

Proposals on amendments and draft law in relation to the «protection from interference»

The Temporary Commission has proposed to legally «evaluate and regulate» the phenomenon of the «participation in the process of interference» in Russian internal affairs by the foreign *individuals* as they are performing «undesirable activity».

For several years the Temporary Commission has tried to create a «Black book of interference in the internal affairs of other states» (by other states than Russia, i.e. the USA). In 2017, the head of the Temporary Commission Andrey Klymov, announced that they were preparing such a «Book», using materials they got through inter-parliamentary cooperation with other states (e.g. Venezuela) (Климов, 2017).

The first edition of the Book should have been published in June 2018, however, as of February 2019 the Book has not been published. Moreover, Klymov recently stated that they work on a Black Book of foreign interference in the affairs of Ukraine and Venezuela (Климов, 2019). The Members of the Russian Parliament who participate in the Temporary Commission had a plan to create a «board of shame» to «uncover» the involvement of Russia's accusers in wrongful acts. The «board» is still work in progress.

On 22nd of April 2019 the Russian Parliament passed legislation on «internet sovereignty» (О внесении изменений в Федеральный закон ... № 608767-7). It will enter in force on the 1st November 2021. It provides changes to the Law on Telecommunications and to the Law on Information, information technology, and protection of information. It will result in transferring to state-control the points of traffic exchange and cross-border points of traffic transition, as well as creating pre-filtering systems with deep analysis equipment (DPI). It means that all the data coming to Russians will be «pre-checked» for their content (Rozendaal & Barandiy, 2019) and can be blocked in a similar way as China's Great Firewall. Igor Ashmanov has advocated for these norms for many years (Липатов, 2019). Putin praised the legislation, saying that «Russia must defend itself against the threat of foreign powers trying to disable the country's access to the global Internet» (Putin explains why the Americans would be fools to shut off Russia's Global Internet access, 2019). At the same time, this supposed threat is used as justification by the Kremlin to control the flow of information within the country (Ristolainen, 2017).

Place of the «information influence» in the Russian definition of interference

Among the 10 ways of interference identified by the Temporary Commission, there is one that refers to media and social media to discredit of the country, its power institutions, political leaders, etc. (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, p. 4-5).

The Temporary Commission accused London and Washington of interference through media (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, p. 68). For example, they «interfere» in the following ways:

1. Use of global media to spread «prepared» content that can contain fake news or conclusions that are based on intentionally wrong data or assumption. They are aimed at foreigners but many of these «vbrosy» also reach Russians. According to the Temporary Commission an example of such global media campaigns were the «information attacks» during Russia's military campaign in Syria.

2. Direct propaganda in Russian language through the US «state» media, and through the affiliated organizations with the aim to raise the number of opposition-minded people within Russia. The Temporary Commission named as examples of such propaganda the content of the home pages of the websites of Radio Freedom and Voice of America during the Russian Presidential campaign 2018 (Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty, 2018, pp. 71-72), while ignoring the mass of Russian government financed websites and TV-channels in dozens of foreign languages under the Sputnik and RT outlets.

3. Direct or indirect influence on Russian media, journalists and bloggers in order to involve them in the propaganda campaigns, e.g. through educational and trainings programs like «Open World – Russian leadership program». The Temporary Commission claimed that trough the programs a new platform for psychological influence on the people of Russia are being created for the «activation of the protest potential».

The criteria of «information interference» may be summarized as follows: preparation of the content by foreign actor (e.g. the USA or the UK); cross-border measures online and offline; «enabling of the measures from the side of the state» (e.g. using «state-financed» media); intention of the «influencer» to target Russian and foreign audience; the goal is to inflict the damage to (the power elites of) Russia.

It has to be noted that by putting the work of the media in such rhetoric helps covering the Russia's wrong doing. This rhetoric allows Moscow to «accept» or to «deny» the Russian misconduct despite the evidences. As a result of this rhetoric, international community «turns a blind eye» on Russia's wrong doing.

At the same time, the Temporary Commission introduced its world view into domestic legal system, e.g. by proposing amendments in legal acts related to «information security» (Отчет о деятельности Временной комиссии Совета Федерации ..., 2017). Thus, the Russian Federation Council considered recommendations of the Temporary Commission when adopting the following legal acts:

– The Law on Security of critical infrastructure;

– Amendments to the Law on Telecommunication;

– Amendments to the Law on Information, information technology and information security;

– Amendments to the Law on Mass media which allows blocking the websites and forces some media organizations to register as «foreign agents».

Consequences of «information influence» of Russia on foreign states – interference in other states' affairs?

According to Russian perception, sovereignty is an absolute power of the state. This approach is rejected by states that advocate for a more liberal world order.

There are many definitions of sovereignty. One of the well-established ones explains sovereignty as the capacity of a state to secure and to realize its own will, and the will of its nation (Barandiy, 2012).

Considering this definition, and generalizing Russian concept of interference, three main questions arise:

1. Does the information influence result in the change of the will of the nations and, therefore, does information influence constitute interference?

2. Does the use of the information and information technology as tools to modify the will of foreign nations constitute direct or indirect interference in national sovereignty of a state? Are consequences – a compulsory element of the interference?

3. Is there a breach of international law in the first and / or second case? What is the state's responsibility for such actions?

One has to answer these questions by applying a «mirroring approach» to the Russian concept of interference, from the

point of view of the West which suffers from Russian information influence.

1. Does the information influence result in the change of the will of the nations and therefore constitutes interference?

The correlation between the measures of interference and the change in the will of a nation has not been established yet, but, because of internet the Kremlin has direct access to millions of individuals in other states. Internet eliminates the other states as middlemen who could recognize, block or adjust these actions at the stage at the «entry» stage of these measures into their territories. In other words, by abusing democratic principles Russia's information acts, softly «forced» into foreign societies and into their legal systems, undermine the capacity of a state to secure its will and the will of its nation.

2. Does the use of the information and information technology as tools to modify the will of foreign nations constitute direct or indirect interference in national sovereignty of a state? Are consequences – a compulsory element of the interference?

International norms are yet to develop; however, the information war of Russia on other states can be de-facto characterized as interference in their sovereignty.

Firstly, Russian interference has a cross-border element: the argument of the populists that internal «fake news» weaken the state institution in the same way as external ones is not valid, as internal ones operate within that nation's legal system and it is possible to develop and enforce instruments of resistance to such «fake news» domestically, whereas extraterritorial enforcement does not exist in international law, which so far does not regulate the problem of cross-border influence through information.

Secondly, there is an intention of the Russian state officials and Russian state media to «stand up for Russia's interests» by any available means[5] (Mckew, 2017). Although interference is often executed by individuals, there is evidence that their actions are Kremlin-initiated and–sponsored (Grove, 2018).

Thirdly, measures of Russian interference are «forced» into the legal system of foreign states, often through «top-down imposed soft power» (Roslycky, 2011) and by abuse of the institute of democracy.

Fourthly, the instruments of the interference both online and offline are originating from Russia (state media, trolls, automated bots, fake news).

Lastly, there are consequences for the political discourse, as well as internal and external matters of concerned states (e.g. changes in state budgets, tightening of the freedoms, and creation of defense mechanisms, all of which constitute a threat to the international liberal order). In this case, the correlation between the interference of the Kremlin and the change of the will of the foreign nation does not even need to be established: evidence of «systematic attempts to interfere» should be already enough to «charge» the Russian Federation with interference, at least politically.

3. Is there a breach of international law in the first and / or second case? What is state responsibility for such actions?

The International Court of Justice in the case «Nicaragua vs. USA» established that for the interference to be wrongful there must be the element of coercion (Military and Par-

[5] See above-elaborated chapter «Russia's approach to secure national interests»

amilitary Activities in and against Nicaragua (Nicaragua v. United States of America, 1986).

At the same time, the element of coercion (force) has been «admitted» by Russia when it proposed to the UN the Article 2 of its Convention on International Information Security.

Conclusions

The ***«information influence» in relation to «interference in sovereignty»*** as defined by the Kremlin, and at the same time as experienced by the Western states, means ***an extraterritorial information activity*** *such as cross-border state-enabled information or information technology act, which has the capacity to affect the will or behavior of another state or its nation; it implies the intention by state officials and by the state coordinated individuals to directly or indirectly «defend the interests» of their state, as defined by its power elite, online or offline.*

Despite the «Nicaragua case», and raising of the question of interference on the international level by different actors, there is no generally accepted definition of interference in internal affairs apart from the military one, and there is no unique approach to the responsibility for these actions. Russia is unilaterally diverting this «non-approach» towards its own interpretation within its own legal system at the same time creating implications for politics and law of other states.

The challenge remains to determine whether states should set limits to «forced» information influence originating in a different legal system than their own, for now leaving the resistance to it almost exclusively to scholars and to the civil society activists worldwide.

References

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections QJ 15*, Vol. 15, No.1, 5-31.

ABstudiya (2018, September 19). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=-fyRlnBuUmhE

Applebaum, A. (2019, January 1). The Trump-Putin revelations tell us what we knew all along. *Washington Post*.

Ashmanov, I. (2013, April 24). Information Sovereignty-New Reality. Retrieved from https://docplayer.ru/31309942-Informacionnyy-suverenitet-novaya-realnost.html

Ashmanov, I. (2013, May 9). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=zpke-8h6awTk&app=desktop

Barandiy, M. (2012). Souveränität als Gewährleistung der Interessen der Staaten: völkerrechtliche und europarechtliche Aspekte. *Peter Lang Academic Research.*

Barandiy, M. (2018, March 3). Why are the Dutch demanding to shut down the EU's only anti-propaganda service? *Euromaidanpress.* http://euromaidanpress.com/2018/03/15/why-are-the-dutch-demanding-to-shut-down-europes-only-anti-propaganda-service/

Barandiy, M. (2018, October 26). What's wrong with Ukraine banning two propaganda channels? *Euromaidanpress.* http://euromaidanpress.com/2018/10/26/whats-wrong-with-ukraine-banning-two-propaganda-channels/

Barbarosie, L., Coalson, R. (2018, February 1). Banning Russian TV, Moldova Is Latest Hot Spot Fighting Krem-

lin Disinformation. *Radio Free Europe*. Retrieved from https://www.rferl.org/a/moldova-bans-reussian-tv-kremlin-disinformation/29013217.html

Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., Uszkiewicz, H. (2019). *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States*. European Union.

Belenkov, D., Gyulazyan P., Mazlumyan D. (2018). Informatsionnyy suverenitet Rossii i evropeyskogo soyuza, informatsionnaya politika зi informatsionnoe protivoborstvo: suschnostь i soderzhanie. *Mezhdunarodnyiy studencheskiy nauchnyiy vestnik (5)*. Retrieved from https://www.eduherald.ru/ru/article/view?id=18949

Bennett, P. G. (1995, April). Modelling Decisions in International Relations: Game Theory and Beyond. *Mershon International Studies Review, 39* (1), 19-52.

Bradshaw, S., Howard P. N., (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. University of Oxford.

Budraitskis, I. (2014, January). The Weakest Link of Managed Democracy: How the Parliament Gave Birth to Nonparliamentary Politics. *South Atlantic Quarterly, 113* (1), 169-185.

Chivvis, C. (2017). Understanding Russian «Hybrid Warfare» and What Can Be Done about It. Retrieved from https://www.rand.org/pubs/authors/c/chivvis_christopher_s.html

Common Declaration of the UNO, OSCE, OAS, and Africa on the Freedom of Expression, Fake News, Disinformation and Propaganda. (2017). Organization for Security and Co-operation in Europe. Retrieved from https://www.osce.org/fom/302796 .

Convention on International Information Security. (2011, September 22). Retrieved from http://www.mid.

ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Danilenkov, A.V. (2017, July). State Sovereignty of the Russian Federation on the Internet. *LexRussica*,7 (128).

De Mesquita, B. B. (2006). Game Theory, Political Economy, and the Evolving Study of War and Peace. *American Political Science Review, 100* (04), 637-642.

DenTV. (2019, March 19). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=p9fZzu-nXbGg

Dickinson, P. (2018, March 3). From Crimea to Salisbury: Time to Acknowledge Putin's Global Hybrid War. *Atlantic Council*. Retrieved from http://www.atlanticcouncil.org/blogs/ukrainealert/from-crimea-to-salisbury-time-to-acknowledge-putin-s-global-hybrid-war

Diplomatrutube (2013, April 24). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=YqnHqjczlWY

Domańska, M. (2019). *Conflict-dependent Russia. The domestic determinants of the Kremlin's anti-western policy*. Ośrodek Studiów Wschodnichim. Marka Karpia.

Dubovitsky, N., (Surkov, V.).(2014, May). Without Sky. *Bewildering Stories, No 582. Russian Pioneer, No 46.*

Fuhr, S. (2018). Report of the Standing Committee on National Defense of the House of Commons (Canada) «Responding to Russian Aggression against Ukraine, Moldova and Georgia in the Black Sea Region». Retrieved from http://mfa.gov.ge/getattachment/News/kanadis-parlamentis-tavdacvis-komitetma-saqartvelo/nddnrp14-e.pdf.aspx

Geopolitika.ru. (2017). *Facts of the interference in the information sovereignty of Russia before presidential elections. Report Preparation of Maidan technology*

in Russia. Retrieved from https://www.geopolitica.ru/books/fakty-vmeshatelstva-v-informacionnyy-suverenitet-rossii-pered-prezidentskimi-vyborami

Gerasimov, V. (2013). The Value of Science Is in the Foresight, *Voyenno-Promyshlennyy Kurrier, № 8* (476).

Gostev, A.(2017). *Global Pscyho-Manipulations. Psychological and Spiritually-Ethical Aspects*. Moscow: Institute of Psychology of Russian Science Academy.

Greenpeace hits back at Trump tweet on climate change denial. (2019, March 12). *BBC News*. Retrieved from https://www.bbc.com/news/world-us-canada-47543905

Grove, T. (2018, February 16). Kremlin Caterer Accused in U.S. Election Meddling Has History of Dishing Dark Arts. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/kremlin-caterer-accused-in-u-s-election-meddling-has-history-of-dishing-dark-arts-1518823765

Harding, L. (2018, October 13). Reporting on Trump and Putin amid the War on Truth. *The Guardian*.

Herszenhorn, D. M. (2018, February 10). *NATO accuses Russia of violating nuclear treaty*. Retrieved from https://www.politico.eu/article/nato-jens-stoltenberg-accuses-russia-of-violating-nuclear-treaty/

HlavRadyoOnlain. (2012, May 16). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=X29YMjBiE5k

ISIP RUDN. (2017, September 24). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=wSKG0EH0YS8

Ivashov, L. (2012, May 9). Evraziiskii soyuz: problemy, perspektivy (Eurasian Union: Problems, Prospects). *Voyenno-Promyshlennyy Kurrier, 18* (435).

Jeangène Vilmer, J.-B., Escorcia, A., Guillaume, M., Herrera, J. (2018). *Information Manipulation: A Challenge for Our Democracies* (report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces). Paris.

Kamian, H. (2018). On Limiting Freedom of Expression in Russia. Speech by Chargé d'Affaires, a.i. to the Permanent Council. Vienna,19 April 2018.

Karnaushenko, L.V. (2015). The intellectual sovereignty of the state and the problem of its security in the society of the XXI century. *Obshchestvo I Pravo № 4* (54),10-14.

Kasperskaia, N. (2014, December 29). Interview by Agarunov Dmitriy. Retrieved from https://xakep.ru/2014/12/29/interview-kasperskaya

Kazun, A. (2016). Framing Sanctions in the Russian Media: The Rally Effect and Putin's Enduring Popularity. *Demokratizatsiya: The Journal of Post-Soviet Democratization Institute for European, Russian, and Eurasian Studies, The George Washington University, Volume 24, Number 3,* 327-350.

Klishas, A. (2018). From Struggle for Law to Struggle for Sovereignty. *Pravo i Upravlenie. XXI vek,* 11-20.

Komov, S., Korotkov, S, Dylevski, I. (2007). Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law. *ICTs and international security (3).* Retrieved from https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2645.pdf

Life TV. (2012). I*nformational Sovereignty of Contemporary State and the main Instruments of its Ensuring.* Lomonosov Moscow State University.

Life TV. (2012, May 1). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?time_continue=928&v=gtZicnFQCJw

Lukas, E., Pomeranzev, P. (2016). Winning the Information War. *Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe*. Report by CEPA.

Mäger, K. (2016). Enforcing the Judgments of the ECtHR in Russia in Light of the Amendments to the Law on the Constitutional Court, *Juridica International, 24,* 14-22.

Mckew, M. (2017, October). The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you. *Politico Magazine*. Retrieved from https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

Medvedev, D. (2018). Marking the 25th anniversary of the RF Constitution. *Zakon.ru*. Retrieved from https://zakon.ru/publication/igzakon/7712

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). (1986,May 27). [judgement].

Nagan, W.P., Hammer, C. (2008). *The Rise of Outsourcing in Modern Warfare: Sovereign Power, Private Military Actors, and the Constitutive Process*. 60 Me. L. Rev. 429.

National Program of Russia 'Digital Economy 2024'.

Østbø, J. (2017). Securitizing «spiritual-moral values» in Russia. *Post-Soviet Affairs, 33* (3), 200-216.

Paris Call for Trust and Security in Cyberspace France Diplomacies (declaration). (2018, November 12).

Pavlovskiy H. (2014, July 1). Authorities, emotions and protests in Russia. *Karta pamyati: geroi i antigeroi*. Retrieved from http://gefter.ru/archive/12661

Pieters, J. (2018, October 15). Netherlands in «Cyber War» With Russia, Defense Minister Says. *NLTimes.*

Political Warfare: Competition in a Cyber Era (Policy Paper) (2019, April). Wilfried Martens Centre for European Studies. Brussels.

Putin explains why the Americans would be fools to shut off Russia's Global Internet access. (2019, February 20). Meduza. Retrieved from https://meduza.io/en/short/2019/02/21/putin-explains-why-russia-needs-internet-isolation-legislation

Putin, V. (2014, October 24). Speech at Valdai International Discussion Club XI, Sochi.

Putin, V. (2007, February 10). Speech at Munich Security Conference.

Putin, V. (2017, June 2). Speech at the Petersburg International Economic Forum. Retrieved from https://ria.ru/20170602/1495693004.html

Report of the Freedom House on Russia. (2019). Retrieved from https://freedomhouse.org/report/freedom-world/2019/russia

Report of the Temporary Commission of the Council of the Russian Federation on the Protection of Sovereignty. (2018).

Ristolainen, M. (2017). Should «RuNet 2020» Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West. *Journal of Information Warfare, 16*(4), 113-131.

Roslycky, L.L. (2011). *The Soft Side of Dark Power: A Study in Soft Power, National Security and the Political-Criminal Nexus with a special focus on the post-Soviet Political-Criminal Nexus, the Russian Black Sea Fleet and Separatism in the Autonomous Republic of Crimea.* [Groningen]: University of Groningen.

Rozendaal, V., Barandiy, M. (2019, March). *Russian Authorities are killing Internet. Promote Ukraine.*

Retrieved from https://promoteukraine.org/russian-authorities-killing-internet/

Ruptly. (2019, March 20). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=TeKOx-6eo9aA&feature=youtu.be

Scott, K. (2016). Dissuasion, Disinformation, Dissonance: Complexity and Autocritique as Tools of Information Warfare. *Journal of Information Warfare,14* (4), 25-42.

Shekhovtsov, A. (2017). *Russia and the Western Far Right (Routledge Studies in Fascism and the Far Right).*

Surkov, V. (2006, June 28). Our Russian model of democracy is called «Sovereign democracy» [Briefing].

Svetoka, S. (2016). *Social Media As A Tool Of Hybrid Warfare.* Riga. NATO Strategic Communications Centre of Excellence.

Syuntyurenko, O.V. (2015, October). Network Technologies for Information Warfare and Manipulation of Public Opinion. *Scientific and Technical Information Processing 42* (4), 205-210.

Taming the Hydra: How to Resist Kremlin's Information Aggression» (Policy Paper). Recommendations for Information Policy. Kyiv. (2018).

The Ministry of Foreign Affairs of the Russian Federation. (2018, September 25). *Comment of the Information Department of Russian MFA regarding Termination by Ukraine of the «Russian-Ukrainian Friendship Treaty»*. Retrieved from http://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3350379

Tkachenko S.L. (2017). The Coercive Diplomacy of Vladimir Putin (2014-2016). InKanet R. (Eds) *The Russian Challenge to the European Security Environment* (pp. 115-136). Palgrave Macmillan, Cham.

Tolstykh, V. (2016). The Current State of the Russian Doctrine of International Law: An Essay. *Russian Juridical Journal*, 3. Retrieved from http://electronic.ruzh.org/?q=en/node/900

Tsarhrad TV. (2017, October 21). [YouTube Channel]. Retrieved from https://www.youtube.com/watch?v=G-9RFGJjot8

Yarovaya, M., Ashmanov, I. (2013, May 1). *Today Information Dominance is the Dominance in Air*. Retrieved from https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe

Zappone, C., Massola, J. (2019, March 14). Russians eye Indonesia for information security expansion. *Sydney Morning Herald*. Retrieved from https://www.smh.com.au/world/asia/russian-information-control-experts-look-to-expand-to-south-east-asia-20190304-p511kn.html

Ziegler, Charles E. (2012, July). Conceptualizing sovereignty in Russian foreign policy: Realist and constructivist perspectives. *International Politics, 49* (4), 400-417.

Елисеев, И. (2015). В Росии создано общественное движение «Антимайдан» [Public movement «Antimaidan established in Russia»]. *Российская газета, 11* (6582). https://rg.ru/2015/01/22/antimaidan.html

Заверняева, С. (2017, June 14). В Совете Федерации создана комиссия по защите госсуверенитета России [The Federation Council established a commission to protect state sovereignty of Russia]. *Парламентская газета*. Доступно через https://www.pnp.ru/politics/v-sovete-federacii-sozdana-komissiya-po-zashhite-gossuvereniteta-rossii.html

Климов, А. (2017). Актуальные примеры вмешательства во внутренние дела России войдут в так называемую «Черную книгу» [Real examples of interventions into internal affairs of Russia will be recorded in so called «Black book»]. .Доступно через http://council.gov.ru/events/news/81751/

Климов, А. (2019). Материалы заседания рабочей группы нашей Комиссии будут использованы для подготовки «черной книги вмешательства» [The materials of the meeting of the working group of our Commission will be used to prepare the «black book of intervention»]. Доступно через http://council.gov.ru/events/news/101496/

Коваленко, А. (2019). Госдума приняла законопроект о «суверенном рунете» [Gosduma adopted a draft law on «sovereign runet»]. *The bell*. Доступно через https://thebell.io/gosduma-prinyala-zakonoproekt-o-suverennom-runete/

Липатов, Ю. (2019). Совет Федерации принял закон о защите российской части интернета [The Federation Council adopted a law on the protection of the Russian part of the Internet]. *Первый канал*. Доступно через https://www.1tv.ru/news/2019-04-22/364008-sovet_federatsii_prinyal_zakon_o_zaschite_rossiyskoy_chasti_interneta

О внесении изменений в Закон Российской Федерации «О средствах массовой информации» [On Amendments to the Law of the Russian Federation «On Mass Media»]. №305-ФЗ. (14.12.2014). Доступно через https://rg.ru/2014/10/17/ino-smi-dok.html

О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [On Amendments to the Code of the Russian Federation on Administrative Offenses]. № 28-ФЗ.(18.03.2019). Доступно через http://publication.pravo.gov.

ru/Document/View/0001201903180021?index=3&rangeSize=1

О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента [On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Profit Organizations Acting as Foreign Agent]. № 121-ФЗ. (20.07.2012). Доступно через http://kremlin.ru/acts/bank/35748

О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» [On Amendments to the Federal Law «On Communications» and the Federal Law «On Information, Information Technologies and Information Protection»] .№ 608767-7. Доступно через https://sozd.duma.gov.ru/bill/608767-7

О Военной доктрине Российской Федерации [On the Military Doctrine of the Russian Federation] .№ 146. (5.02.2010). Доступно через http://pravo.gov.ru/proxy/ips/?docbody=&nd=102135800&intelsearch=%EF%F0%EE%F4%E8%EB%E0%EA%F2%E8%EA%E0+%FD%EA%F1%F2%F0%E5%EC%E8%E7%EC%E0+%E8++%F2%E5%F0%F0%EE%F0%E8%E7%EC%E0

О государственной гражданской службе Российской Федерации [On the state civil service of the Russian Federation]. № 79-ФЗ. (27.07.2004). Доступно через http://www.consultant.ru/document/cons_doc_LAW_48601/

О запрете отдельным категориям лиц открывать и иметь счета (вклады), хранить наличные денежные средства и ценности в иностранных банках,

расположенных за пределами территории Российской Федерации, владеть и (или) пользоваться иностранными финансовыми инструментами [On prohibiting certain categories of persons from opening and holding accounts (deposits), storing cash and valuables in foreign banks located outside the territory of the Russian Federation, and owning and / or using foreign financial instruments]. № 79-ФЗ. (07.05.2013). Доступно через https://rg.ru/2013/05/14/zapret-dok.html

О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации [About measures of influence on persons involved in violations of fundamental human rights and freedoms, rights and freedoms of citizens of the Russian Federation] .№272.(28.12.2012). Доступно через http://kremlin.ru/acts/bank/36642

О Стратегии национальной безопасности Российской Федерации [About the National Security Strategy of the Russian Federation]. №683.(31.12.2015). Доступно через http://www.kremlin.ru/acts/bank/40391

Об утверждении Доктрины информационной безопасности Российской Федерации [On approval of the Information Security Doctrine of the Russian Federation].№646.(5.12.2016). Доступно через http://kremlin.ru/acts/bank/41460

Об утверждении Концепции внешней политики Российской Федерации [On approval of the Concept of the foreign policy of the Russian Federation]. № 640. (30.11.2016). Доступно через http://kremlin.ru/acts/bank/41451

Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению

вмешательства во внутренние дела РФ (2017). Отчет о деятельности Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела РФ в период с июня по декабрь 2017 года [Report on the activities of the Interim Commission of the Council of the Federation to protect state sovereignty and prevent interference in the internal affairs of the Russian Federation from June to December 2017]. (2017). Доступно через http://council.gov.ru/structure/commissions/iccf_def/plans/88007

Россия 24. (2017, June 27). [YouTube Channel]. Доступно через https://www.youtube.com/watch?v=F7rZx-QrW3wA

Россия 24. (2018, April 23). [YouTube Channel]. Доступно через https://www.youtube.com/watch?v=EuAG-z7sxVEg

Grateful to Ivanna Bilych, Evhenia Kolomiyets-Ludwig and Thomas Theiner for their support and review of this article

DOI 10.34054/bdc002

Extraction, Integration and Data Processing in the SIEM «SPLUNK» Using «NESSUS» Vulnerability Scanner

Petro Venherskyi[6], Roman Karpiuk[7]

Abstract. In this work we propose: creating an integrated environment between the Nessus vulnerability scanner and Splunk's security information and event management system; development of analytics for the help of information security specialists to develop and analyze vulnerabilities discovered in systems.

The urgency of the topic lies in the fact that the standard methods that provide the individual SIEM «Splunk» or the vulnerability scanner «Nessus» is not enough for the complete review of problems in the system and as a consequence of the implementation of a specialist in analyzing and making the necessary decisions. The practical relevance is to properly integrate these two products, as well as develop a unique analytics for quick and easy analysis.

Key words: information and security management system, vulnerability scanner, security event management, Splunk system, Nessus scanner.

[6] Professor, Department of applied mathematics and informatics, Ivan Franko National University of Lviv, Ukraine, petro.vengersky@gmail.com

[7] Security Analyst, SecOpsTeam, SoftServeInc, Lviv, Ukraine, simmpplee@gmail.com

Introduction

Currently, more and more attention is being paid to ensuring the security of information in large institutions and companies, as well as in medium and small organizations. Objects that protect different levels of access, all kinds of deployment of computing environments and various topology network interactions. The task of providing security through universal means of detecting and preventing attacks is complicated, including due to the rapid increase in the number of users and a variety of types of devices, the use of cloud technologies and multiple increases in the volume and speed of transmission and processing of information. One of the classes of tools that enables the security of systems of any level and set of devices is the information and security management system (SIEM). The advantage of these solutions lies in a flexible approach when implementing and independent of the set of specifications and platforms for the ultimate protected infrastructure.

Vulnerability Scanners

Vulnerability Scanners are software or hardware tools for diagnosing and monitoring networked computers that scan networks, computers and programs to detect possible security issues, evaluate and eliminate vulnerabilities. Vulnerability scanners allow you to check various applications in the system for the presence of a «guillotine» that can be used by traps. Low-level tools, such as port scanners, can also be used to detect and analyze possible applications and protocols that run on the system[8].

[8] https://www.tenable.com./products/nessus/nessus-professional, General Information, main page about sub-product)

Security Information and Event Management

SIEM (security information and event management) is a combination of two terms that indicate the scope of application software: SIM (Security information management) – information security management and SEM (Security event management) – management of security events. SIEM technology provides real-time analysis of security events (alarms) coming from network devices and applications. SIEM is represented by applications, devices or services, and is also used to log data and generate reports for compatibility with other business data. The term itself was invented by Gartner in 2005, but since then the very concept and all that belongs to it, has undergone many changes. (https://www.splunk.com, General Information, main page)

Integration

As a vulnerability scanner, we used the product from Tenable Company Nessus [2] (https://www.tenable.com./products/nessus/nessus-professional, General Information, main page about sub-product). As an SIEM system – «SPLUNK» [1] (https://www.splunk.com/, General Information, main page).

1. First of all, we need to install Splunk's special application (add-on) – «Splunk Add-on for Tenable», This application allows you to interact with Spline from Nessus, that is, it contains all the necessary scripts for the correct work

2. The second step is to generate keys for API access to Nessus-a. To do this, you need to generate two keys «Access Key» and «Secret Key» on the scanner itself

3. Next in Splunk, you need to create an index that will record (index) the data coming from the vulnerability scanner.

4. After creating the index, you must add the input parameters (inputs) in the already installed application for Nessus. This is where we need pre-generated access keys.

For a more detailed description of the manual, use the official documentation: https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/integrations/How_To_Guide_Splunk_v2.pdf.

After receiving two «portions» of data there is a completely logical question – «And how do we combine these data?». After all, if these data are different then there is no use for them for analytics. We will return to this question a bit later. But I suppose I need to realize that all the data that is received by Splunk is reliable.

After analyzing the data obtained at Splunk-u with the results on Nessus-I, we see one, however, extremely critical non-conformance. Splunk does not receive the «Plugin Output» field. This field is extremely important because it includes where the vulnerability was detected, and may also contain local recommendations for addressing certain vulnerabilities.

It's not hard to guess that the problem with the appliance that extracts data for Splunk.

So, after the study, a weak spot was found. This is a python script called «nessus_data_collector.py». All further corrections are indicated in the work.

After analyzing all the above, we can conclude that in order to assess the picture of information security, we must work on the vulnerability data in the system. Vul-

nerability scanners should be used to automate inspection and detection of inconsistencies. Although all the actual solutions for vulnerability scanners have their own, by default, standard data display system, however, for IT analysts it will be difficult to operate, analyze, and ultimately decide if these data are found in different «places» of sources. Also, to perform a certain auto-correlation of events to detect more advanced attacks in order to adjust them on time, it is very difficult almost impossible if the information is dispersed across different resources. Therefore, in this case, the Security Information and Event Management (SIEM) system should be used for storing and processing raw data.

So, during the implementation, we examined the functioning of SIEM systems and vulnerability scanners in general. Considered some of the best representatives of these security tools.

Have made a direct integration between the Nessus vulnerability scanner and the SIEM Splunk representative. However, our integration did not end at the level of simple data transmission, but were built on the progress of dashboards. Since «raw» data is difficult to process, the analyst will have to spend a fair amount of time searching for the information he needs. That is why it took a lot of time to implement the correct display of input data. This greatly simplifies the perception of information and enables a cybersecurity expert to timely process certain IS incidents, as well as monitor certain trends in vulnerability in the company and, accordingly, make / provide some analytics.

Our dashboards which provide some views of corporate vulnerabilities (Fig.1-4):

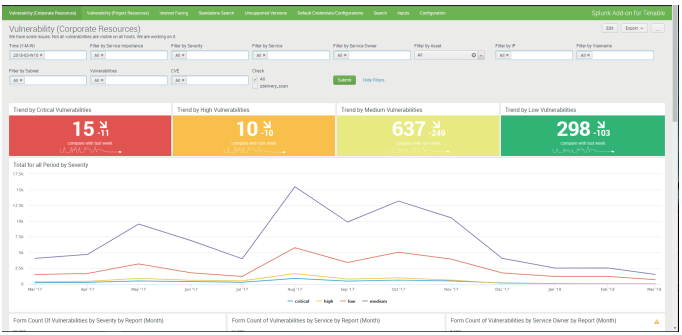


Fig. 1. Vulnerability (Corporate Resources). Part 1

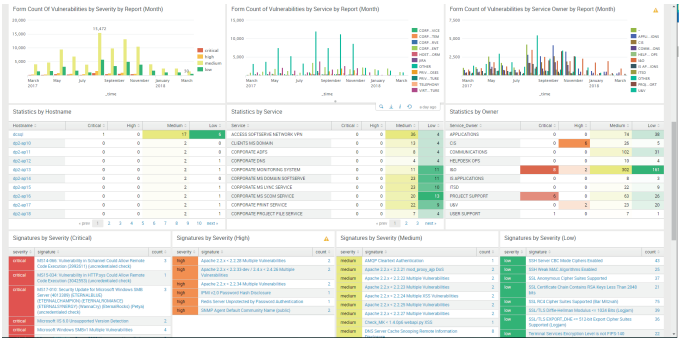


Fig 2. Vulnerability (Corporate Resources). Part 2

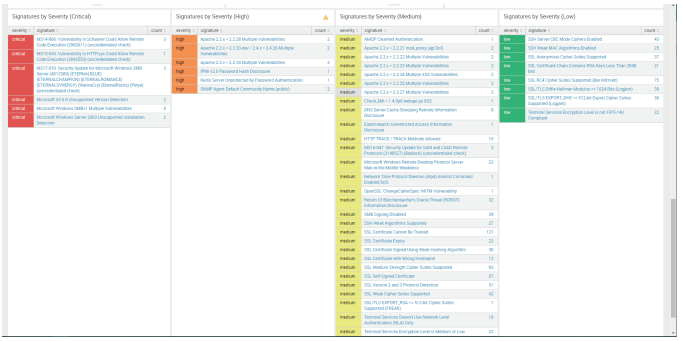


Fig. 3. Vulnerability (Corporate Resources). Part 3

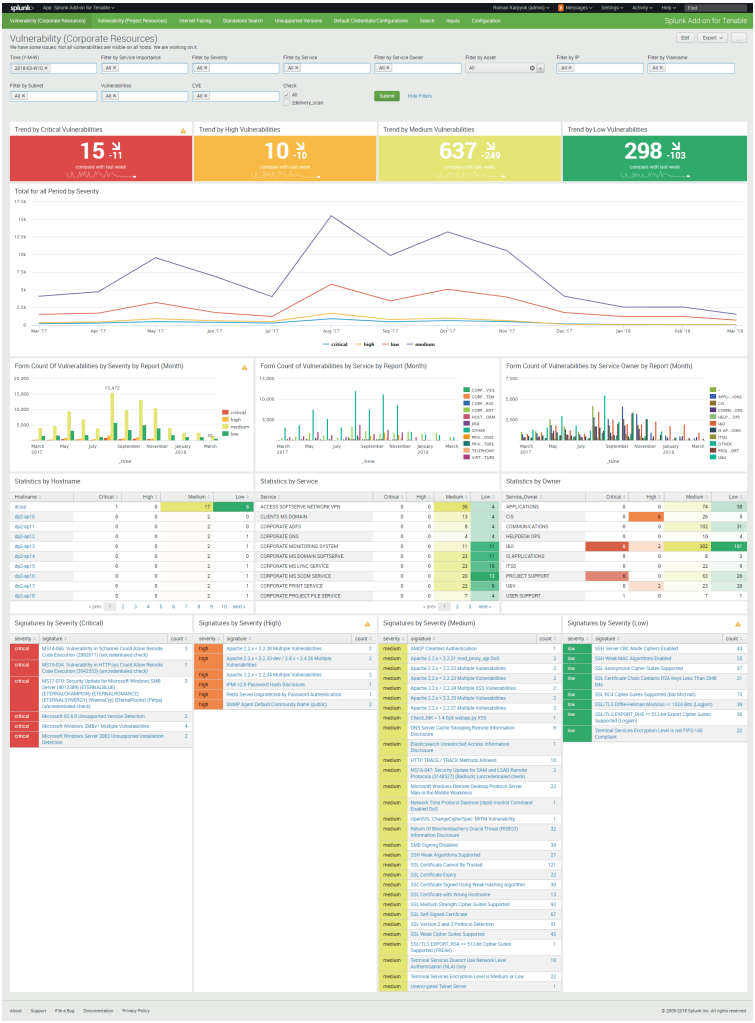


Fig. 4. Vulnerability (Corporate Resources). General View.

Conclusions

After analyzing all the above, we can conclude that in order to assess the picture of information security, we must

work on the vulnerability data in the system. Vulnerability scanners should be used to automate inspection and detection of inconsistencies. Although all the actual solutions for vulnerability scanners have their own, by default, standard data display system, however, for IT analysts it will be difficult to operate, analyze, and ultimately decide if these data are found in different «places» of sources. Also, to perform a certain auto-correlation of events to detect more advanced attacks in order to adjust them on time, it is very difficult almost impossible if the information is dispersed across different resources. Therefore, in this case, the Security Information and Event Management (SIEM) system should be used for storing and processing raw data.

References

Splunk Fundamentals. Bushfire resources. Retrieved from https://www.splunk.com

Nessus professional. Retrieved from https://www.tenable.com./products/nessus/nessus-professional

DOI 10.34054/bdc004

Legal and Ethical Aspects of Autonomous Weapons, Cyber Attacks, and AI

Igor Kotsiuba[9], PhD

One of the most important principles is the principle of proportionality, which means that damage to the civilian population and civilian objects cannot exceed the military advantage that the party expects to receive utilizing a cyber attack. The most significant difficulties, in this case, arise because of the close interconnection of civilian and military objects as well as civil and military infrastructure in cyberspace. Military facilities from IHL are those objects that by their location and purpose make an effective contribution to the military success of the state.

It is tough to make this distinction in cyberspace, when, for example, GPS-navigation, computer networks, the Internet work both for the civilian population and the success of the military operation. There is a great risk that civilian objects will be considered as dual-purpose objects and be destroyed – in cyberspace, however, almost everything will be a dual purpose object. How, in this case, does one consider this proportionality, how does one protect the civilian population and how does one determine if the damage to the civilian population would outweigh the military advantage or not?

[9] Partner, CyberDesk, Ukraine igor.kotsiuba [at] uacyberdesk.com

Also, the state will need substantial technical expertise to anticipate and calculate whether any damage will be done at all. From the point of view of the IHL, this involves the responsibility of the State party to the conflict: to calculate the damage, to provide for the possibility of a return journey, if it becomes clear that the civilian objects will suffer during the attack. But it is much easier to give instructions to stop a tank on its way to a city than to stop the work of viruses that have already been launched into a computer system, and the result of which was the failure of the objects.

Thus, although we can assert affirmatively that IHL regulates cybercrime, it obviously requires considerable refinement. Particularly relevant in the context of the application of IHL in cyberspace are the following issues:

- the contradiction between anonymity on the Internet and the need for individual criminal responsibility for military offenses,
- the state's obligation to ensure IHL compliance by States in cyberspace,
- direct participation in cyberconflicts and its possible consequences for IT companies and other possible non-state actors, even just private campaigns in military operations using computer technology.

Cyber-attacks can cause humanitarian problems, in particular, if they are not limited to the impact on a specific computer or computer system. Indeed, their results are usually seen in the real world.

There is, however, which is a certain complexity – the anonymisation of information. When conducting cyber attacks, autonomous weapon attack – anonymity is rather a rule than an exception. In some cases, it is not possible to determine

the sender. The main challenge stems from the fact that all rights are based on the establishment of liability (in the IHL these are parties in the conflict or individuals). In particular, if it is impossible to establish who carried out a particular operation and, accordingly, if it is impossible to establish its connection with the armed conflict, it will be challenging to determine whether the IHL is generally applicable to this operation.

Technological Capabilities and Requirements of the IHL

Obviously, I have to determine if there are stand-alone armaments that reach such a level of difference, proportionality and precautionary measures, or if they can be developed in the future. Therefore, first of all, it should be made clear that if technically it is not possible to comply with certain requirements of the IHL with automated weapons, this is not enough reason to refuse these requirements. The use of autonomous weapons will simply be illegal. Current international meetings are in fact being focused on such issues.

The countries of the «big twenty» first agreed on the principles of handling artificial intelligence (AI). They are listed in a joint statement released on Saturday, June 8, 2019, according to the G20 summit in the Japanese city of Tsukuba.

Ease of Use of Force and Warfare

Some argue that using automated weapons it is easier to wage war and use force outside the state. But this is also true for many types of weapons and technology - it was true for new weapons in the Middle Ages, and it was true when the first artillery, aircraft and modern fleets were developed.

Compared to personal battles, all these technologies have simplified war. This question concerns the admissibility of war (jus ad bellum) and the issue of disarmament. It is understood that robots also fall under the general disarmament problem.

It may well be that (the possibility of)secrecy around the use of automated weapons and, as a result, the difficulties of attribution complicate the implementation of state liability and international criminal responsibility for the act of aggression. On the other hand, the fact that computer systems record everything simplifies the request for criminal liability, at least when the party uses automated weapons.

In addition, there may be a psychological problem, but I can not judge its reality. It can be argued that those who build and program automated weapons and those who can be the last person in a loop, even without knowing where these weapons will be used, feel less responsible. But there is no scientific research on such an effect or the opposite.

Robots and Systems are Not the Addressees of the Law

When trying to apply IHL norms, there are some preliminary questions that need to be clarified. Only human beings obey the Rules of Law, and only people are obliged to adhere to them. In the case of automated weapons, the IHL applies to those who develop, manufacture, program, and decide on their use. Regardless of how far we go into the future and regardless of how artificial intelligence will work, people will always be involved, at least during the conception of a machine. The man will decide that this car will be created, and then create a car. Even if one day the robots are being built, it's still the person who built the original work. This person is bound by law. The machine is not legally bound.

The Advantages are Not to Be Human

The main advantage of automated weapons or automated cyber attacks, from the point of view of IHL compliance, is that only humans can be inhumane, and only people can deliberately decide not to follow the rules. As soon as the robots have artificial intelligence, it is necessary to make sure that such an intelligence is not used - since intellectual intelligence is sometimes used – to circumvent the rules or to solve from an utilitarian point of view that failure to comply with IHL instructions as it is the best way which facilitates the achievement of the main goal of overcoming the enemy.

The Fundamental Issues of the IHL Have Become More Acute

The most elementary question that comes to mind is the definition of most armed conflicts, since outside the armed conflict robots could only be used if they could arrest a person and not use (deadly) force. As we know that there is no uniform definition of armed conflict, the issue is rather an international armed conflict and is not an international armed conflict.

What is the lower threshold of violence between the state and non-state actor (or between non-state actors), which makes it an armed conflict? This is not a specific issue for robots, and even where automated weapons are used, the answer must be given and given by the person. But the answer is even more important when using automated weapons.

Many other questions need to find an answer before an automated weapon can be programmed, for example:

• What is the geographical scope of the IHL and what constitutes the battlefield?

Automatated weapons raise the latter issue more acutely, but legally, considerations should be the same as for air bombing: can a belligerent attack on a target that would be a legitimate goal under IHL, far from the actual struggle, be restrained only by the rules of the IHL? Or in this place, the IHL does not apply at all? Or is international human rights law predominant as LexSpecialis?

Legal Issues for Autonomous Weapon Systems (AWS) and Autonomous Cyber Attacks

The main problems facing AWS from a legal point of view are twofold: on the one hand, AWS will adhere to the principle of distinction, and on the other hand, they must perform the same, if not a more demanding task, compliance with the principle. Proportionality, which states that, before the deployment of any weapon system, each State Party must determine whether a new weapon, means or method of warfare it is studying is being used., developed, acquired or accepted, in some or all circumstances, will be prohibited by international law. This section, after a short introduction, places these principles in the IHL and focuses on (1) the principle of distinction, (2) the principle of proportionality, and (3) attempts to outline the problems that cause the introduction of AWS in any combat roles.

Conclusions

The IHL has been elaborated on great detail in a number of areas, including the types of weapons that can be used in armed conflicts, and types of legitimate purposes.

The nature of aggression in Ukraine and the hybrid war, with its massive cyberattacks, showed that where there are indicators, their diplomatic assessment, OSINT and the results of modern criminology, all lead to understanding but not to responsibility. Similarly, cyberspace and attacks today, as well as autonomous lethal weapons of tomorrow, will have indicators, a diplomatic assessment, but too blurred of a legal conclusion and the irreversibility of responsibility.

DOI 10.34054/bdc005

The importance of elaborated training for information security specialists in the successful development of the country in current conditions

Petro Venherskyi[10], Mykhailo Kropyva[11]

Abstract. Cybersecurity is no longer an issue to be taken lightly. Be it an individual or a corporation it brings a huge amount of damage. Last year was terrible for a bunch of not only organizations but countries at large which were infected by global massive ransomware. Cyber-attacks are now on the rise coming in many different forms and are always evolving. To fight them efficiently we need a pool of qualified professionals who will continuously assess existing and potential threats and adjust security systems respectively and make them resistant to attacks.

Key words: educational program, cyberattack, application, network, operations security, attack scenario.

[10] Doctor of Physics and Mathematics Science, professor of information systems department, faculty of applied mathematics and informatics, Ivan Franko National University of Lviv, Ukraine.
[11] InfoSec Director, SoftServe.

Introduction

As of now, Ukraine has a great potential in terms of talents but educational opportunities do not meet current needs to the fullest [1]. To nourish a strong community of cyber security specialists we've united the efforts and developed an up-to-date bachelor program which balances theoretical knowledge and practical experience on real-life projects with seasoned IT experts [2,3]. Due to the fruitful collaboration of Lviv IT community and educational establishments we all benefit - students get high-quality education based on the latest tech developments, and companies get motivated graduates with relevant knowledge and experience.

The threat towards information security caused by the current war in the eastern part of the country.

During last five years cybersecurity attacks become real threat for the whole Ukraine making significant impact to critical infrastructure. Ukraine power grid cyberattack took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers.

Most affected were consumers of «Prykarpattyaoblenergo» (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours.

At the same time consumers of two other energy distribution companies, «Chernivtsioblenergo» (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and «Kyivoblenergo» (Ukrainian: Київобленерго; servicing Kyiv Oblast) were also affected by a cyberattack, but at a smaller

scale. According to representatives of one of the companies, attacks were conducted from computers with IP addresses allocated to the Russian Federation.

A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia.

Security measures showcased at SoftServe

During the attack an actor focused on all aspects of application and IT infrastructure security.

On the side of **Application Security**, it was found several software flaws in corporate applications that allowed actor to successfully penetrate the external network perimeter and get a foothold in the internal corporate network. Those were vulnerabilities of insecure file upload and SQL injection

On the side of **Network Security**, an actor was able to successfully escalate the initial penetration to the level of network access to several hundreds of internal network hosts, due to the lack of efficient network segmentation and access controls. Access to some critical business systems was obtained from the very initial point of penetration. The most significant role in successful penetration was caused by the fact that some development-related systems had both external (Internet) and internal network accesses.

On the side of **Operations Security**, an actor was able to find a set of severe weaknesses, that affect corporate security posture. They have found multiple operational deficiencies, such as improper security administration practices and in-

sufficient attention to user authentication controls and access management.The most severe cases were «default» root or Administrator passwords set on multiple operating systems. Using these weaknesses, it was possible to penetrate multiple corporate systems, including Jenkins software, Cisco and Citrix networking devices, and Windows- and Unix-based OS.

Attack scenario

Find available directories\files or resources at the known domains

Using the ***dirburster*** utility an actor has found a publicly available directory that contained PHP script with functionality of unauthenticated upload (without any verification). Thus it was possible to upload an arbitrary executable file to a victim system and get interactive access to the web server.

Get control over a web server

It was uploaded a web shell, that allowed actor to control the server remotely with *www-data* permissions.

Scan Internal network

It was installed *nmap* and *masscan* utilities on the web server which allowed actor to scan internal network for available services.

Establish persistent access to internal network

It was installed a reverse SOCKS proxy that allowed actor to stay connected to the internal network even if the initial penetration vector was detected and remediated.

Get access to system accounts

Actor discovered several Jenkins instances that allowed access without prior authentication to sensitive information, such as source code, list of users, stored credentials.

Use the deficiency in password management to obtain root access to Unix-based hosts

It was revealed a password for «root» account. This gave an actor root access to many Unix-based hosts, where the same typical password was utilized.

Use Jenkins vulnerability to get access to Windows-based host

The Jenkins Remote Code Execution vulnerability was used to extract NTLM hashes for the administrative accounts on corporate systems.

Use the deficiency in password management to obtain administrative access to Windows-based hosts

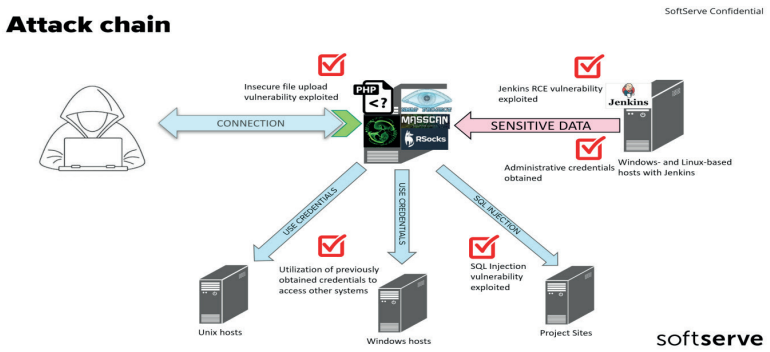
***Administrator** account had the same password on different hosts. This allowed an actor to get access to exploit Pass-The-Hash attack and get access to multiple Windows-based hosts,* where the same credentials were utilized.

Use Time-based SQL injection on vulnerable aaplications

An actor used ***sqlmap*** tool to inject commands via the *Login* parameter and remote code execution.

Use outdated vulnerable versions of WordPress

An actor utilized the *wp-scan* utility and found some outdated vulnerable WordPress instances.



Lessons learned and recommendations:

The dual-home networked hosts pose significant risk to the security of the IT infrastructure as they enable access to internal network once a relevant software vulnerability is found and exploited from the outside. Such deficiency must be eliminated on the level of network security design and security operations.

Setting unique and complex credentials to high-privilege user accounts is an essential practice of a modern security program. For secure management of local administrative credentials of Windows systems, using LAPS4 is strongly recommended.

Not all security vulnerabilities are easily discoverable by contemporary network-centric vulnerability scanners. Corporation must pay attention to a robust enterprise-wide application security testing program that would start from reviewing all potentially risky applications' security and continue by tracking changes made to those applications over time and testing the security of these incremental changes.

Obsolete operation systems are vulnerable to many known exploits. To resolve this security issue, the workstations should be upgraded to a more recent version of OS.

Changing the password of the krbtgt account as often as ppossible (e.g. once in a month or two) is significant to prevent the «Golden Ticket» attacks.

All scripts and applications with sensitive functionality should implement an authentication mechanism. Any upload functionality should validate files that are uploaded.

Enable robust authentication mechanisms at all Jenkins instances in the organization.

Update all the default or primitive password. Wherever possible implement a reasonable password policy.

Restrict direct SSH and RDP access under administrative accounts. *Sudo* and *«Run as...»* should be used for getting administrative access once logged in. Consider implementing a more sophisticated password management practices, such as Local Administrator Password Solution (LAPS).

Login parameter should be validated by the web application server and sanitized from any characters not expected as part of the login string according to the usernames convention.

Lack of cybersecurity specialists and their training at higher educational institutions.

The necessity of implementation of the provisions of European and international organizations aimed at introduction of modern educational and professional programs for the preparation of bachelor's degrees in cyber security, the development of modern curricula and programs based on the development of mini-projects with the support of mentors from IT companies for the development of professional skills of cyber security specialists, providing the required number of specialists able to effectively solve the problems of information security of society.

Joint educational programs on cybersecurity. The example of training provided at Ivan Franko National University of Lviv.

One example of such educational programs is the development of a new, innovative, practical cyber security program at the Ivan Franko National University of Lviv, which combines the study of the basics of cyber security, the legal and organizational principles of combating cybercrime, software, cryptographic mechanisms and technical means of personal protection, enterprises , institutions and the country as a whole. The structure of such a program is shown in Fig. 1, where the display of the prevailing part of the disciplines of information technology, the professional unit and the block of free choice of the student.

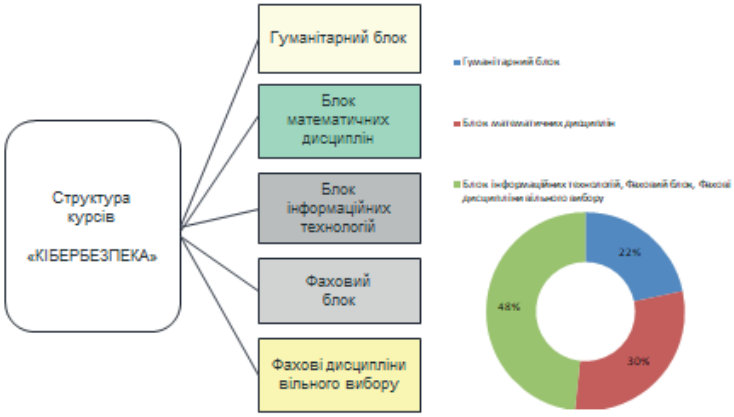


Fig.1 Structure of the education program cybersecurity.

It is also worth noting the practical orientation of this curriculum, so from the first year students study the basics of cybersecurity and the basis of team work, which then would use this knowledge in the implementation of team mini-projects. When performing mini projects, students have the op-

portunity to consult with the mentor appointed from the IT companies and help to execute the mini-project qualitatively (Fig.2).

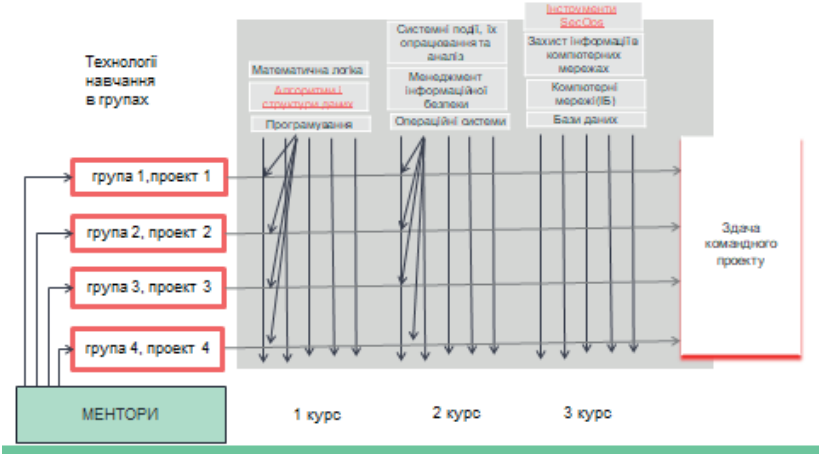


Fig. 2 Technologies of implementation of mini-projects.

Our program is different from other applications, that is, the development of applications for security, this is more application programming, the development of information systems for business, as we have a high level of mathematical training, then students have a logic of programming, they can manage projects and be able to climb higher the level for development management, that high level of programming is confirmed by prize-winning places on olympiads, hackathons and others.

Summary and outlook

Professional ability to analyze potential threats and risks of cybersecurity, the ability to detect signs of external influ-

ence, to simulate the possible such effects, to predict their consequences, the use of systemic software tools, the analysis of information security of objects and systems, using national and european standards, the formation of the complex measures to manage cybersecurity are the foundation, the main requirements of the professional competencies of educational programs for future cyber security specialists.

References

On the Basic Principles of Cybersecurity Protection of Ukraine. The Law of Ukraine of 10.05.2017 № 2163-VI. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

The standard of higher education in Ukraine: the first (bachelor's) level, the branchKnowledge 12 - Information Technology, specialty 125 –Cybersecurity. Retrieved from https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf

May, M. & Elliott, D. Consortium for Research on Information Security and Policy. Retrieved from https://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy

DOI 10.34054/bdc003

«Legal Asymmetry» in the Context of Liability of the State and State-Sponsored Cyber Attacks Actors

Oksana Bulda[12]

The globalized world is more and more confronted with the phenomenon of «hybrid war», which poses a new type of threat based on a combination of military and non-military means such as cyber-attacks, mass disinformation campaigns and many others.

Cyber-attacks are particularly dangerous as they can hit the country's strategic infrastructure, interrupt political processes and influence economic development. Therefore, hybrid war can destabilize and undermine entire societies. The increasingly widespread use of these new tactics, especially in combination, raises concerns about the adequacy of existing legal norms.

The legal framework for cyber security measures still has no definition of «hybrid war» and there is no unified legislation on the matter as well. However, the common understanding is that the main feature of this phenomenon is «legal asymmetry», as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to avoid legal consequences for their actions.

[12] IT Lawyer

Despite the complexity of «hybrid war», hybrid adversaries do not operate in a legal vacuum and that relevant domestic and international law norms must be applicable to their actions, although the question of attribution and hence accountability may raise difficulties. If, in the framework of «hybrid war», a state resorts to the use of force against another state, the latter state is allowed to invoke the right to self-defense but in practice, hybrid adversaries avoid manifest use of force that would reach the required threshold for triggering application of the above norms, thereby creating a legal grey area.

The «legal asymmetry» problem arises from the fact that international law does not generally hold states responsible for the actions of non-state actors as in most cases of cyber-attacks, states don't generally operate through formal state bodies. Instead, they use non-state actors who are less visible, more removed and offer plausible deniability. Thus, the liability will only be acknowledged if the state either recognizes and adopts the conduct of the non-state actor as its own, which is unlikely to happen, or the state directs or controls the non-state actor. As a result, the chances that a state will ever be held publicly accountable for cyber-attacks under existing legal framework are quite low.

The delay in the enactment of laws, outdated legal norms, rapid technologies development, collision of legislation, limited scope of the law applicability and cybersecurity low awareness – all together make it much difficult to incorporate the sufficient legislation in order to bring to justice not only the state sponsored cyber-attacks actors but also to hold the state accountable for such actions.

Various considerations determine the creation of laws in different countries, so their promulgation depends on a multiplicity of factors; for example, political issues or other is-

sues affecting local initiatives, or adherence to international agreements encouraging the same level of development for cross-border collaboration.

However, it is on account of these very conditions and characteristics that legislation is often postponed. The Budapest Convention has been in the ratification process for more than a decade.

Also, the evolution of technology should be considered; the development of standards may, therefore, fall far behind technological advances. Just as organizations continuously update their standards in response to evolving risks and new technologies, the law must be at the forefront when it comes to responding to present and emergent issues which may need to be regulated.

Perhaps the way to rectify this disparity between technological innovation and the enactment of appropriate legal measures, is to focus on regulating human behaviors, especially since technologies can become obsolete in a relatively short period. This may prove to be the most reliable way for regulation to be effective, but it is also important to note that this could lead to rising tensions in the future. An example of this might be trying to regulate the use of social networks, which are not supported by legislative enactment.

Similarly, the absence of legislation or agreements on specific aspects of certain issues can undermine international collaboration, even within the same territory. Public and private sectors face a challenge when it comes to access the information for investigations, with implications for security, the right to privacy, and commercial interests, mainly of tech companies.

The aim is therefore to have legal measures in place for protection at various levels and in various spheres. To this end,

legislators have also started to consider the requirements necessary for security in their countries, including their capacity to respond to large-scale incidents, the protection of their critical infrastructure, their ability to collaborate with other countries, and even to consider the development of a security culture which can be implemented in society.

Considering all above mentioned, in order to make the legislation truly effective, there is a need to define the unified common rules based on international, regional or national agreements and cross-border countries cooperation considering not only the legal side of the problem but the technical as well.

Bibliography

Council of Europe. (26 April 2018). Legal challenges related to the hybrid war and human rights obligations. Resolution 2217, Parliamentary Assembly, Committee on Legal Affairs and Human Rights. Available at https://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?FileID=24762&lang=EN

Payne, C., Finlay, L. (2019). International law cannot keep up with cyber-criminals. World Economic Forum. Available at https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/

Calam, M., Chinn, D., Porter, J. F., Noble, J. (2018). Asking the right questions to define government's role in cybersecurity. McKinsey&Company. Available at https://www.mckinsey.com/industries/public-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity

Rikk, R. (2018). National Cyber Security Index 2018. e-Governance Academy. Available at https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

Mendoza, M. A. (2017). Challenges and implications of cybersecurity legislation, Miguel Ángel Mendoza. WeLiveSecurity. Available at https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/

10.34054/bdc009

A Fast Empirical Method for Detecting Fake News on Propagandistic News Resources

Liubomyr Monastyrskyi[13], Yaroslav Boyko[14],
Bohdan Sokolovskyi[15], Oleh Sinkevych[16]

In this work, an effective method for detecting news reports about certain events with deliberately distorted content is proposed. The methodology consists in accumulating reliable information about a given event from reliable verified sources. Thereafter, there occurs a quantitative analysis of the reliability of information from the sources which are suspected in their integrity. To achieve this goal, we used the standard software tools for obtaining and processing information with the help of NLP techniques.

In our case, for collecting information the Python *requests* modules (data scraping) (Requests: HTTP for Humans,

[13] Prof., Head of Department, Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems E-mail: liu_mon@ukr.net
[14] Associate Prof., Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems, E-mail: yaroslav.boyko@lnu.edu.ua
[15] Associate Prof., Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems, E-mail: b_sokolovsky@ukr.net
[16] Assistance Prof., Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems, E-mail: deneb.acyg@gmail.com

2011) are used and for working with HTML data – the *BeautifulSoup4* ones (Beautiful Soup, 2012).

To date, there is a large number of effective tools for working with text information which use both direct rules based on rules and methods of artificial intelligence tools. Especially accurate results in many areas of NLP are provided by the machine learning, including deep machine learning. At the same time, the use of the latter is connected with the problems of providing the necessary volumes of computing resources which are not always acceptable. For the preliminary evaluation analysis, in our opinion, the best methods are based on the reasonable mathematical approaches and, at the same time, are not related to large volumes of computations. To achieve our goal we propose to use the text-based properties based on the TF-IDF statistics (Aggarwal, 2018). This is a statistical indicator used to evaluate the importance of words in the context of a document which is a part of collection of documents or corpus. The weight (significance) of words is proportional to the number of word uses in the document and is inversely proportional to the frequency of the use of words in other documents of collection. The TF-IDF indicator is used in the tast of text analysis and information retrieval. It can be used as one of the criteria for the relevance of a document to a search query, as well as when calculating the degree of affiliation of documents during clustering. The easiest ranking function can be defined as a total number of the TF-IDF of each term in the query. The most advanced ranking functions are based on this simple model (TF-IDF, 2001).

In our work, the implementation of TF-IDF statistics computation in the Python sklearn module (Scikit-learn, 2007) was realized . On the basis of the set of reliable news articles about a certain event, the main building was formed. In order to determine the degree of reliability of the article under

study we added the latter to this set and a similarity matrix was calculated. It has been found that the degree of similarity of the articles that relate to the reliable ones exceeds an index of 0.5, while the articles with distorted data refer to the main corpus with similarity levels in the 0.1 - 0.4 range for all experiments conducted by us. The main disadvantage of our results is that we consider small volumes of sets of articles, so in future research, we plan to automate the process of obtaining data for the rapid formation of large corpus, as well as the improvement of computational procedures.

References

Aggarwal, C.C. (2018). *Machine Learning for Text*. (Springer).

Beautiful Soup. (2012). A tremendous boon – Python 411 Podcast. Retrieved from https://www.crummy.com/software/BeautifulSoup

Requests: HTTP for Humans. (2011). Retrieved from https://2.python-requests.org//en/master/

Scikit-learn (2007). Scikit-learn. Mashine Learning in Python Retrieved from https://scikit-learn.org/

TF-IDF (2001). TF-IDF. Wikipedia. Retrieved from https://uk.wikipedia.org/wiki/TF-IDF

DOI 10.34054/bdc008

Features of Russian - Ukrainian Cyberwar

Volodymyr Lozynsky[17], Oleh Petryshyn[18],
Liubomyr Monastyrsky[19]

The collapse of the USSR was marked, in particular, by the beginning of confrontation between Russia and Ukraine, which grew into the Russian-Ukrainian war, including that in the cyberspace. There were both the conflicts in the cyberspace with attacks on the energy system of Ukraine and the hacker attacks from Russia using virus programs. Since 2014, Russia has begun the armed aggression and cyberwar against Ukraine.

In this report, we describe the technologies of the Russian cyber expansion towards Ukraine, the stages and peculiarities of cyber attacks, the formation of a cyber defense system in Ukraine, providing the cyber defense system in Ukraine and granting the effective assistance from Western partners in this area.

[17] Post-graduate Student, Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems, E-mail: volodymyr.l@vede.in.ua
[18] Post-graduate Student, Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems, E-mail: oleg.lpml@gmail.com
[19] Prof., Head of Department, Ivan Franko National University of Lviv, Department of Radiolectronic and Computer Systems,, E-mail: liu_mon@ukr.net

The hybrid war imposed on Ukraine by Russia involves concealing the true intentions and hostile cyber actions from Russia. A number of institutions and government departments in Ukraine as well as foreign organizations reported numerous cyber attacks and hostile actions from Russia in relation to Ukraine in cyberspace (Laurence, 2019).

In particular, Dmitry Shimkov, a former deputy head of the Presidential Administration during the IXth National Expert Forum in Kyiv, argued that most of the cyber attacks on the Ukrainian economic infrastructure were directed from the Russian Federation. Minister of Infrastructure Volodymyr Omelyan said that the Russian Federation initially tests cyber attacks to identify the weaknesses of the digital infrastructure of Ukraine. The Ministry experienced great losses as a result of such attacks. The Security Service of Ukraine (SSU) prevented cyber attacks on the Ukrainian courts from the Russian Federation.

The Main Directorate of the General Staff of the Armed Forces of the Russian Federation organized cyber attacks on the Kiev subway and Odessa airport. The cyber intervention in the «electronic cabinet of taxpayers» service of the State Fiscal Service of Ukraine was carried out 35 times. The chief specialist of Ukraine on cyber defense Sergey Demedyuk said that recently cases of skinning and fishing have sharply increased. In particular, in 2013, Russia «Operation Armagedon» launched the system of cyber espionage for the government agencies as well as law, power and defense structures.

There was also a message from Interior Minister Arsen Avakov about the attempts to access the data systems of the Central Election Commission (CEC) and district election commissions on the day of the presidential election received by the Foreign Intelligence Service, as well as a representative of the Ukrainian State Committee for Special Communications.

In the Chernihiv region, the Security Service of Ukraine arrested the group of hackers who had intentions to attack the e-election servers. The Deputy Prime Minister I. Klimpush-Tsintsadze and the deputy head of the Security Service of Ukraine Olena Frolova declared on cyberattacks by the Russian Federation. The Foreign Minister Klimkin reported that during the last four years 6,000 cyber attacks have been committed on the e-government website in Dnipro. Russian secret services planned to damage the communication network, which provides the presidential election – the Security Service of Ukraine

The information received in Ukraine is confirmed by our western partners. In particular, the Military Intelligence and Security Security Service of the Netherlands has recently accused Russia of trying cyber attacks at the Organization for the Prohibition of Chemical Weapons (OPCW) in Hague. The OPCW is involved in the investigation of chemical attacks in Syria and in Salisbury.

Microsoft experts believe that the attacks are carried out by a group of cybercriminals of the General Staff of the Russian Armed Forces which has been also engaged in the cyber attacks on the election headquarters of H. Clinton.

Representatives of CISCO announced infecting 500 thousands routers in 50 countries by Russian hackers, including in Ukraine. Routers were used to collect private information. The FireEye identified the following groups of Russian hackers who have shown themselves during the Russian-Ukrainian cyberwar: APT29 (Cozy Bear, Cozy Duke), APT 28 (Sofary Group, TsarTeam, PawnStorm, FancyBear).

Thus, repulsing the above-mentioned cyber attacks, a number of measures was introduced and launched a set of new approaches to the cyber defense. In particular, for the period

since 2014, there were features in conducting cyberattacks on the part of Russia, which required adequate actions by Ukraine. For example, the government created a group of cyberpolice experts in the Ministry of Internal Affairs to work on cyberattack warnings during the election campaign. The European Commission organized cyber education to protect the Central Election Committee. NATO helped Ukraine to establish a Cybersecurity Center before the elections. Estonia provided us with financial and technical help in the cyber defense field. To reduce the propaganda influence, it was blocked in Russia about 2 thousands fake shareholders and filed sanctions on about 300 Internet sites of the Russian Federation.

The effectiveness of cyber defense can be improved by creating complex counteraction mechanism and establishing a public-private partnership in the field of cyber security. There is no alternative to refusal of Russian software, social networks and payment systems. It is necessary to improve the legal and regulatory basis in the field of cybersecurity, possibly to create in the frame of the National Security and Defense Council a Cybercenter for protection against Russian cyber influences and hacker attacks.

Reference

Laurens, C. (14.02.2019). How Ukraine became a test bed for cyberweaponry. *Politico.* Retrieved from https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

DOI 10.34054/bdc007

Ризики бізнесу: зміна акцентів

Валентина Лук'янова[20]

Економічна система все більше стає відкритою і відповідно уразливою до зовнішніх ризиків і загроз. Будь-яке підприємство стає все більш залежним від змін умов зовнішнього середовища не лише країни відповідної локації, але світової економіки.

Метою розгляду у нашій статті є детальний аналіз із виявленням груп факторів ризику бізнес-середовища функціонування і загроз економічній безпеці підприємств.

В основу нашого дослідження покладено аналітичні спостереження німецької фінансової транснаціональної корпорації Allianz SE (щорічно опубліковані у Allianz Global Corporate & Specialty (AGCS). Основним напрямком діяльності компанії є страхування. Станом на 2013 рік, це найбільша у світі страхова компанія, 11 за величиною фінансова група та 25 найбільша компанія за оцінкою журналу Forbes. Також це найбільша фінансова компанія за обсягом доходу, станом на 2012 рік. Група Allianz присутня у більш ніж 70 країнах на 5 континентах (в т.ч. і в Україні). Майже 140 тис. співробітників обслуговують близько 88 мільйони клієнтів (Allianz. At a glance).

[20] Д.е.н., професор, зав. кафедри економіки підприємства і підприємництва, Хмельницький національний університет, Україна

Спостереження базуються на ґрунтовному аналізі близько 2000 експертами із 80 країн ризиків і загроз, що виділяють ризик-менеджери для успішного функціонування бізнесу у різних країнах світу. Найперше експерти оцінюють ризики і загрози безпеці підприємств з точки зору їх імовірності та величині збитків (прямих і непрямих втрат). Зведені результати дослідження подано у таблиці 1. Рейтинг відображає частку респондентів, що виділили важливість даного виду ризику серед 10 найбільш важливих у відповідні періоди.

Таблиця 1

Найбільші ризики і загрози бізнесу

Вид ризику (загроза)	Рейтинг, %				
	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Збої у виробництві	43	46	38	37	42
Кіберзагрози	12	17	28	30	40
Стихійні лиха	33	30	24	24	30
Ринкові коливання	19	15	34	31	22
Законодавче регулювання	21	18	18	24	21
Техногенні аварії	24	27	16	16	20
Політичні ризики	18	11	11	14	11
Репутаційні ризики	15	16	18	13	13
Технологічні зміни	10			12	15
Макроекономічні зміни		16	24	22	
Кліматичні зміни					10
Персонал	10	9	11		
Неякісна продукція	10				

Розглянемо більш розлого виділені групи ризиків і загроз за період 2014-2018 рр.

Найперше, варто відмітити стабільну присутність 8 видів ризиків у всіх звітах. Поряд з цим такі загрози як макроекономічні зміни (програми жорсткої економії, зростання цін на товари, інфляційні ризики) та нові технології (нанотехнології, 3Д-друк, штучний інтелект, дрони) відмічено лише у трьох з п'яти аналізованих звітів. Але варто зазначити появу у документах 2018 р. такого виду загроз як кліматичні зміни і зменшення впливу ризиків з боку персоналу (крадіжки, корупція, брак тощо). Але про ці зміни у тенденціях пізніше.

Пропонуємо детально проаналізувати тенденції ризиків і загроз за трьома напрямами:

1. Ризики і загрози природного характеру (класично їх найширших перелік при страхуванні) – таблиця 2.

Таблиця 2

Ризики і загрози природного характеру

Вид ризику (загроза)	Рейтинг, %				
	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Стихійні лиха	33	30	24	24	30
Кліматичні зміни					10

Рекордний розмір збитків від стихійних лих забезпечив повернення цього ризику в трійку найбільших на 2018 рік (3-е місце, 30% респондентів відмітили значимість даного ризику). Менеджери також стурбовані тим, що ситуація минулого року може передвіщати ще більше зростання інтенсивності і частоти даних збитків, внаслідок чого в верхню десятку рейтингу вперше потрапили кліматичні зміни (10-е місце, 10% відповідей). На жаль, щодо чисто форс-мажорних обставин глобальні зміни клімату вже

не можна віднести, так як це результат наступаючих наслідків діяльності людини і не лише природного, а більш штучного характеру (починаючи із токсичних викидів у атмосферу підприємств і транспорту і закінчуючи забрудненням води і землі як підприємствами так і звичайними сміттєзвалищами). З іншого боку кліматологи вже давно відмічають негативний вплив кліматичних змін на частоту та інтенсивність стихійних лих.

Відповідно до звітів рекордний розмір застрахованих збитків від стихійних лих, що склав в 2017 році $ 135 млрд., в зв'язку з ураганами «Харві», «Ірма» і «Марія» в США і на Карибах, забезпечив повернення цього ризику в трійку найбільших на 2018 рік (3-е місце, 30% відповідей).Вплив природних катаклізмів виходить далеко за межі фізичного збитку. У міру того як сфери економічної діяльності стають більш компактними і тісніше взаємопов'язані глобально, стихійні лиха можуть вплинути на значне число підприємств з різних сегментів, які, на перший погляд, не були схильні до впливу природних катастроф (forinsurer.com, 2018).

Респонденти побоюються, що 2017 рік може бути передвісником того, що інтенсивність стихійних лих буде рости під впливом змін клімату. У верхній десятці 2018 роки з'явився новий ризик – «Зміни клімату / Підвищення мінливості погоди» (10-е місце), пов'язаний, в тому числі, з тенденцією по урбанізації прибережних регіонів, продовженням зменшенням льодовиків (як у горах так і на полюсах) так і поступовим зростанням температури і більш різкою зміною пір року (весняний і осінній період подекуди зменшився до одного-підтора місяця).

2. Ризики і загрози зовнішнього економічного середовища (таблиця 3). Даний вид ризику теж носить більш систематичний характер (особливо за умов чистої конкурен-

ції), але змінює свій акцент у бік протекціонізму великих корпорацій, явного чи прихованого втручання у діяльність урядових структур і законодавчих органів (особливо в економіках, що розвиваються).

Таблиця 3

Ризики і загрози зовнішнього середовища

Вид ризику (загроза)	Рейтинг, %				
	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Ринкові коливання	19	15	34	31	22
Законодавче регулювання	21	18	18	24	21
Політичні ризики	18	11	11	14	11
Макроекономічні зміни		16	24	22	

«Відповідно до даних досліджень, компанії по всьому світу готуються до складного року: під впливом зростаючими політичними, законодавчими, регуляторними та іншими змінами, рівень невизначеності неухильно зростає по всьому світу» (fin.org.ua). Такі висновки зробили експерти у 2017 р. Але проаналізувавши результати таблиці 3 можна відмітити стабільно високі впливи загроз з боку змін у законодавстві (економічні санкції, протекціонізм) та макроекономічних змін (інфляція/дефляція, зміна цін на товари, програми жорсткої економії тощо).

Щодо факторів змін ринкової кон'юнктури, то значимість їх впливу сильно залежить від світових економічних криз, або регіональних економічних загроз (2016 р.).

Політичні ризики з одного боку є стабільно відносно невисокі, але сильно залежні від ескалації військових кон-

фліктів і політичних революцій (наприклад, 2014 р. відголосок війни на сході України і захоплення Криму, а 2017 р. – загострення у Сирії і загрози з боку Північної Кореї).

3. Інші ризики і загрози (таблиця 4). До даної групи увійшли ризики із значним негативним впливом людського фактору.

Таблиця 4

Найбільші ризики і загрози бізнесу

Вид ризику (загроза)	Рейтинг, %				
	2014 р.	2015 р.	2016 р.	2017 р.	2018 р.
Збої у виробництві	43	46	38	37	42
Кіберзагрози	12	17	28	30	40
Техногенні аварії	24	27	16	16	20
Репутаційні ризики	15	16	18	13	13
Технологічні зміни	10			12	15
Персонал	10	9	11		
Неякісна продукція	10				

За даними експертів (forinsurer.com, 2018) збої у виробництві ось уже шостий рік займають верхній рядок серед найважливіших ризиків в Європі, Азіатсько-Тихоокеанському регіоні, на Близькому і Середньому Сході. Цей ризик, на жаль, властивий будь-якому підприємству незалежно від обсягів бізнесу. Компанії стикаються зі зростаючою кількістю сценаріїв прояву ризику – від традиційних впливів, таких як матеріальні збитки, заподіяні об'єктам і ланцюжкам постачань стихійними лихами і пожежами, до нових факторів, що випливають з дигіталізації і взаємозв'язку, які зазвичай призводять до значних

фінансових втрат. Збої в роботі IT-систем, тероризм, інциденти, пов'язані з неякісною продукцією, несподіваними регуляторними змінами можуть призвести бізнес до короткострокової або тривалої перерви в діяльності, що здійснює істотний вплив на доходи підприємств.

За даними опитування експертів, кібер-інциденти вперше названі в числі найбільш шокуючих факторів, що сприяють збоям у виробництві, в той час як самі збої у виробництві стали, на їхню думку, найбільш вагомою причиною втрат після кібер-інцидентів. Згідно з даними Cyence Risk Analytics, в разі недоступності хмарного сервісу у постачальника хмарних послуг, що триває більше 12 годин, збитки можуть скласти 850 млн. дол. в Північній Америці і 700 млн. дол. в Європі, виходячи з того, що від недоступності до інформації постраждає 50 тис. компаній трьох різних сфер (фінанси, охорона здоров'я і роздрібна торгівля) в кожному регіоні (forinsurer.com, 2018).

Відповідно, ризик збоїв у виробництві займає друге місце за своєю недооціненістю. Компанії часто недооцінюють складність «повернення до нормального режиму роботи». Їм слід постійно коригувати свої плани реагування на надзвичайні ситуації, щоб вони відображали нову реальність збоїв у виробництві, що включає і загрозу кібер-інцидентів.

Кіберзагрози продовжують підніматись в рейтингу і у 2018 р. є другим за важливістю ризиком для підприємств (таблиця 1). П'ять років тому, за оцінками експертів (forinsurer.com, 2018), вони знаходилися лише на 15-му місці. Такі загрози, як порушення даних, хакерські атаки або ж збої у виробництві внаслідок кібер-інциденту підтверджують, що це головний ризик для бізнесу в 11 досліджуваних країнах, а також на Американському континенті, і другий за значимістю ризик в Європі та Азі-

атсько-Тихоокеанському регіоні. Він також є самим недооціненим ризиком в довгостроковій перспективі.

Нещодавні інциденти, пов'язані з появою програм-вимагачів WannaCry і Petya, призвели до значних збитків великого числа компаній. Інша програма-вимагач Mirai і масштабна розподілена атака типу «відмова в обслуговуванні» (DDoS) на ключові інтернет-платформи і сервіси в Європі і Північній Америці наприкінці 2016 року вписуються у зростаючу тенденцію – появу «кібер-ураганів». Хакери можуть вплинути на функціонування великої кількості підприємств, вибравши в якості мети, наприклад, загальні елементи інтернет-інфраструктури, від яких вони залежать. Ця тенденція, швидше за все, збережеться і в подальшому. Заходи щодо захисту даних знову повернулися в центр уваги після масштабних порушень в США. Вступ в силу Загального регламенту щодо захисту даних (GDPR) по всій Європі в травні 2018 року зробить перевірки ще більш ретельними.

Дані Барометра ризиків Allianz показують, що стурбованість кібер-загрозами серед компаній сегмента малого та середнього бізнесу зростає. Зокрема, для невеликих компаній цей ризик перемістився з шостого на друге місце, а для середніх компаній – з третього на перше місце рейтингу (forinsurer.com, 2018). Найбільш високі місця в рейтингу загроз кібер-інциденти займають серед компаній сегмента Розваги і Медіа, компаній, що надають фінансові послуги, а також компаній, що відносяться до сегменту технологій і телекомунікації.

Нові технології як фактор ризику теж зростають за рейтингом. Вони є другим найбільшим довгостроковим ризиком, поступаючись лише кібер-інцидентам, з якими тісно взаємопов'язані. Уразливість автоматизованих, автономних і самонавчальних машин до відмови або до дій кі-

бер-зловмисників буде в майбутньому зростати, що може призвести до значних порушень критичної інфраструктури. Незважаючи на те, що в майбутньому число незначних збитків, пов'язаних з автоматизацією і послабленням моніторингу, може скоротитися, на зміну їм можуть прийти більш значні втрати. Підприємствам потрібно бути готовим до нових сценаріїв несення відповідальності, поява яких викликано описаним вище переходом відповідальності від людини до машини або до виробника програмного забезпечення. Це зробить покладання відповідальності і надання страхового покриття для такої відповідальності більш складною справою.

Інший недооцінений різновид технологічних ризиків для таких країн як Україна – це зростання технологічного розриву у економічному розвитку, технологічне відставання і відповідні наслідки не лише в економічній сфері, але й технічній грамотності населення, соціальному розвитку, екологічним загрозам тощо.

Репутаційні втрати (13% у 2018 р.) – основна причина економічних втрат для підприємств які поряд з кіберризиками є загрозами інформаційної безпеки бізнесу. На жаль, ці два види ризиків тісно переплелись і часто їх ва;ко відокремити.

Закінчуючи аналіз таблиці 4 можна відмітити зменшення уваги до чисто суб'єктних видів ризиків зв'язаних з персоналом (крадіжки, шахрайство, неякісна робота тощо). Їх частка зменшується і з часом зникає із десятки найважливіших.

Найбільш важливі (імовірні та втратні) ризики і загрози у 2018 р. подано на рисунку 1.

Дана динамічна діаграма показує стабільність прояву факторів ризику форс-мажорних обставин (24-33 %) і

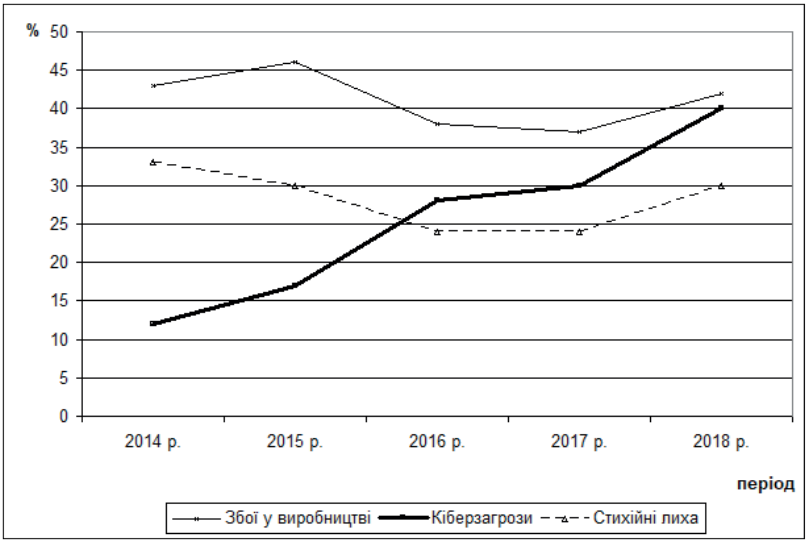


Рис. 1. Ризики і загрози у 2018 р.

значно випереджаючу їх хвилю (перше місце у рейтингу за весь період дослідження) загроз збоїв у виробництві (37-46 %). Також можна спостерігати стрімко зростаючу хвилю кіберзагроз (12-40 %).

Отже, можна зробити висновок, що з одного боку важко виділити дію окремих чистих видів ризиків і загроз на підприємницьку діяльність, а з іншого – значну потребу до збільшення інформаційної безпеки діяльності підприємства, що відображена не лише в кіберзагрозах, але й ризиках збоїв у виробництві, репутаційних та технологічних ризиках та ін.

Список використаних джерел

Allianz. At a glance. Retrieved from https://www.allianz.com/en/about_us/who_we_are/at-a-glance/

СБ Малакут *«Барометр рисков». Allianz назвал глобальные риски компаний в 2018 году.* Доступно через http://sb-malakut.com.ua/barometr-riskov-allianz-nazval-globalnye-riski-kompanij-v-2018-godu

Fin.org.ua. 10 глобальных бизнес-рисков предприятий в 2017 году. Allianz представил новый «Барометр рисков». Доступно через http://www.fin.org.ua/news/1228676

DOI 10.34054/bdc006

Інтернет речей: проблеми безпеки та основні засади її забезпечення

Марія Диха[21]

Інтернет речей (Internet of Things, IoT) – «концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку» (Інтернет речей, n.d.).

Аналізуючи підходи до визначення IoT вважаємо, що Інтернет речей – це взаємодія пристроїв й інших предметів в мережі, які збирають, обробляють, обмінюються даними завдяки електроніці, програмному забезпеченню з метою виконання визначених завдань та реалізації певних функцій.У найбільш поширеному розумінні IoT дозволяє фізичним об'єктам (речам), здійснювати взаємодію між собою або з зовнішнім світом, частково або повністю без участі людини.

Запровадив термін «інтернет речей» Кевін Ештон у своїй доповіді «Інтернет Речей» для «Procter & Gamble» в 1999 р. з ідеєю впровадження радіочастотної ідентифікації

[21] Професор кафедри економіки підприємства і підприємництва, доктор економічних наук, професор, Хмельницький національний університет, Україна

(RFID) в ланцюг поставок виробничих товарів чим привернув увагу до самої ідеї підключення до мережі нових типів пристроїв. На сьогодні розробками в сфері досліджень і стандартизації інтернету речей займаються багато країн як на рівні національних ініціатив, наприклад ANSI (США), BSI (Великобританія), так і на інтернаціональному рівні: ETSI, ITU, ISO, IEC.

Інтернет речей вже сьогодні приносить великі зміни у повсякденному житті. А за прогнозами Gartner, «до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпеченнята послуг становитиме 1,9 трлн дол» (Gartner says the Internet of Things, 2013).

Інтернет речей з'єднує мільярди нових пристроїв з інтернетом, але це також розширює можливості кібератак хакерів проти мереж та інформації. Широке включення «розумних» пристроїв у повсякденні об'єкти призводить до появи нових вразливих місць як в інфраструктурі, яку вони підтримують, на яку вони покладаються, так і на процеси, якими воникерують.

Кібератак зазнають державні інституції, бізнес структури, окремі сектори економіки (наприклад, енергетична мережа), а також і окремі особи.

Дослідники з безпеки продовжують розкривати вразливі місця у функціонуванні міжнародних і державних інституцій, у різних сферах ведення бізнесу і життєдіяльності людей. Зокрема, у промислових та комерційних програмах можемо навести такі приклади (Fisher, E. A., Liu, E. C., Rollins, J. W., Theohary, C. A., 2014; National Vulnerability Database, n.d.):

1) кібернападники атакували підприємство з метою отримання доступу до його ділової мережі. Кіберзловмис-

ники вразили металургійний комбінат у Німеччині, маніпулюючи та руйнуючи системи управління та запобігаючи зупиненню доменної печі регульованим способом, що призвело до «масових пошкоджень».

2) комерційна посудомийна машина, яка може бути підключена до інтернету, включає в себе вбудований веб-сервер, який «прослуховує порт 80 і схильний до атаки переходу по каталогу. Отже, зловмисник може використати цю проблему для доступу до конфіденційної інформації для атак» (National Vulnerability Database, n.d.).

Щоб протистояти загрозам IoT варто розуміти їх природу та технології їх поширення. В цьому контексті варто звернути увагу на доповідь дослідницьких служб (CRS) від 2014 року до Конгресу США, в якій визначено п'ять типів кіберзловмисників:

1. Кібертерористи: транснаціональні терористичні організації, бойовики та джихадисти, які використовують інтернет як інструмент планування атак, форму війни, радикалізації та вербування, метод розповсюдження пропаганди та засіб комунікації.

   Експеримент DHS Aurora передбачав комп'ютерну атаку на систему управління генератором енергії, яка призвела до припинення операцій та знищення обладнання.

2. Кібершпигуни: особи, які викрадають секретну або конфіденційну інформацію, якою користуються уряди або приватні корпорації, щоб отримати конкурентну стратегічну, безпечну, фінансову чи політичну перевагу. Зокрема, у звіті ФБР за 2011 рік зазначено: «Компанія стала жертвою вторгнення та втратила за добу 1 мільярд доларів досліджень і розробок, які розроблялися 10 років».

3. Кіберзахоплення: особи, які займаються незаконними кібератаками для отримання грошової вигоди. Важко оцінити, але щорічні глобальні витрати для приватних осіб складають сотні мільярдів доларів (і втрата довіри-клієнтів).

4. Кіберагенти: це агенти або квазіагенти національних держав, які розвивають свої можливості та здійснюють кібератаки для підтримки стратегічних цілей країни. У серпні 2012 року серія кібер-атак була спрямована проти Саудівської фірми Арамко, найбільшого у світі виробника нафтогазової промисловості. Напади спричинили спустошення 30 тисяч комп'ютерів компанії, а сам програмний код вірусу, мабуть, покликаний порушити або зупинити виробництво нафти. Деякі співробітники служби безпеки заявляють, що Іран, можливо, підтримав цю атаку.

5. Кіберг-активісти: особи, які виконують кібер-атаки для задоволення, або за філософськими чи іншими не грошовими міркуваннями.

Серед основних загроз та недоліків IoTвважаємо за доцільне звернути увагу на такі:

1. Відсутність єдиної системи. Проблема інтеграції IoT – у відсутності загальних правил і стандартів. Поки не буде розуміння загальної картини, складно впровадити універсальне рішення.

2. Енерговитратність. Для повноцінної роботи IoT потрібно домогтися автономності мережі і отримувати енергію з навколишнього середовища.

3. Питання безпеки та приватності. Основний ризик – у відкритій базі даних. У шахраїв з'явиться можливість

зламувати не тільки рахунки і комп'ютери, але навіть холодильники.

4. Вартість. Техніка дорога, незважаючи на те, що її використання окупиться в майбутньому: система «розумний дім» допоможе заощадити на електриці і водопостачанні, обладнання на виробництві завчасно сповістить про ризик поломки, кухонна техніка дозволить уникнути псування продуктів.

Аналізуючи технологічний прогрес останніх десятиліть, можна впевнено сказати, що людство рухається до впровадження концепції IoT в життя.

Отже, необхідно проектувати системи для забезпечення безпеки. В цьому контексті важливо збалансувати витрати на захист та час на його забезпечення.

Захист рішень на базі IoT від тих, хто планує завдати шкоди, буде мати вирішальне значення для зростання IoT, а також для особистої та ділової безпеки.

Серед основних засад забезпечення безпеки вважаємо за необхідне виділити такі:

1. Комунікаційні технології. Шифрування – складний процес, має наслідки від апаратного забезпечення до ключового управління, але є ефективним рішенням для безпечного IoT.

2. Послуги, мови та інструменти. Слабкі сторони програмного забезпечення у системі та коді призводять до вразливої роботи IoT. Мова, стандарти дизайну та кодування, а також інструменти, які їх підтримують, утримання служб, пов'язаних із безпекою – потребують фінансування, але економія на таких складових може призведе до серйозних порушень, яких можна було б запобігти.

3. Сертифікація. Сертифікація безпеки може вимагатись для певного напрямку діяльності. Навіть якщо це не потрібно зараз, усвідомлюючи вимоги щодо сертифікації та включення корисних елементів у практику розробки, вже зараз потрібно створювати безпечні продукти та потенційно підготувати їх до вимог сертифікації в майбутньому.

4. Промислова кооперація. Боротьба з хакерами – це асиметрична війна. Співпраця щодо виявлення дефектів, відстеження та спільного використання розробок, навіть конкурентів, стала прийнятною практикою. Так NIST Cybersecurity Framework призвела до розробки основ для організації зусиль щодо впровадження та адаптації практик безпеки в організації.

Отже, для інтернету речей характерні ще більш складні проблеми забезпечення безпеки в порівнянні з тими, які властиві для мереж зв'язку. До них додаються можливі проблеми масштабованості мережі, викликані мало передбачуваним обсягом передачі даних від великого числа вузлів, ненадійність програмного забезпечення, тощо.

Широке застосування інтернету речей є результатом інтеграції комп'ютерних технологій, технологій зв'язку і різних областей промислових галузей. Крім порушення інформаційної безпеки традиційних мереж зв'язку (в результаті ризику підслуховування, спотворення інформації, розкриття інформації) пристрої та мережі інтернету речей стикаються з додатковими проблемами безпеки на прикладному рівні – при використанні хмарних обчисленнях, обробці інформації, забезпеченні прав на інтелектуальну власність, захист приватності тощо.

У найближчому майбутньому середовище IoT буде безпосередньо причетне до життя простих людей та до бізнесу

і державної діяльності. Отже, таку складну структуру необхідно будувати з урахуванням сучасних вимог до інформаційної безпеки. До питання забезпечення захищеності інформації в межах IoT необхідно підходити комплексно і особливо приділяти уваги таким аспектам як безпека кінцевих інформаційних систем і безпека їх взаємодії.

Список використаних джерел

Fisher, E. A., Liu, E. C., Rollins, J. W., Theohary, C. A. (Dec. 15, 2014). The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R42984.pdf

Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. (Dec 13, 2013). In Finyear. Retrieved from https://www.finyear.com/Gartner-Says-the-Internet-of-Things-Installed-Base-Will-Grow-to-26-Billion-Units-By-2020_a27901.html

National Vulnerability Database (n.d.). National Institute of Standards and Technology. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2017-7240

Інтернет речей. (n.d.). Вікіпедія. Retrieved June 1, 2019 from https://uk.wikipedia.org/wiki/Інтернет_речей

DOI 10.34054/bdc010

Зростання поширення Інтернету речей та проблеми безпеки в часи кібератак

Тетяна Головач[22]

У статті (Бугера, 2018) дається наступне визначення терміну «Інтернет речей»: «Інтернет речей (англ. Internet of Things, IoT) – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані передавачі, а також програмне забезпечення, що дозволяє здійснювати передачу й обмін даними між фізичним світом і комп'ютерними системами за допомогою використання стандартних протоколів зв'язку». Натепер набуває поширення також термін всеохоплюючий або всеосяжний Інтернет (Internet of Everything, IoE).

Згідно з більшістю прогнозів, «Інтернет речей» продовжить зростання по всьому світу. Розумних пристроїв стане більше. Значно зросте їх функціонал. Прогноз обсягу Інтернету речей у світі та у Росії наведено в таблиці 1.

За прогнозами, в 2022 році європейська галузь Інтернету речей покаже результат в 241 млрд. дол. Найбільшими сегментами IoT залишатимуться виробництво, комунальні служби, роздрібна торгівля, транспорт. У поточному році лідером на європейському ринку Інтернету речей

[22] Старший викладач кафедри економіки підприємства і підприємництва, Хмельницький національний університет, Україна

Таблиця 1.

Прогноз обсягу Інтернету речей (TAdviser, 2019)

Показник	Значення				
	2018	2019	2020	2021	2022
1. Оптимістичний прогноз обсягу Інтернету речей у світі, млрд. дол	215,6	273,9	347,9	441,8	561
2. Прогноз обсягу Інтернету речей у Росії, млрд. руб:					
– оптимістичний	149,8	211,2	297,9	420	592,2
– песимістичний	129	151,8	174,6	197,4	220,2

буде Німеччина з результатом в 35 млрд. дол. Далі підуть Франція та Великобританія з витратами понад 25 млрд. дол. А ось Італія покаже результат на рівні 19 млрд. дол (Finance.ua, 15.02.2019).

Російський ринок IoT ділиться на споживчий (B2C) та корпоративний (B2B). Між ними є принципова різниця: B2B Інтернет речей націлений на заробляння коштів або їх економію, а B2C – на витрачання коштів; тут важливо, яку суму користувач готовий платити в обмін на комфорт або на задоволення. Частка фірм Росії, які сьогодні використовують у роботі цифрові системи управління відносин із клієнтами (CRM), в середньому по країні не перевищує 10,3 % (ICT Moscow, 2019). Такою ж є ситуація із впровадженням системи планування ресурсів підприємства (ERP): середній показник по Росії – 12,2% від загальної кількості досліджуваних (ICT Moscow, 2019).

17 січня 2018 року Кабінет Міністрів України схвалив Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердив план заходів з

її реалізації (Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації, 2018). За оцінками аналітиків, виконання усіх пунктів Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки сприятиме зростанню внутрішнього споживання цифрових та інформаційно-комунікаційних технологій бізнесом у 5-6 разів: з 700 млн дол. у 2017 році до 3,5-4 млрд дол. у 2021. Кількість створених робочих місць орієнтовно збільшиться на 200-300 тис. дол до 2021 року. Очікується, що до 2021 року 95% установ обслуговування громадян: від транспорту до салонів краси надаватимуть громадянам можливості безготівкових розрахунків. 99,9% громадян України будуть мати електронний цифровий підпис, інтегрований в паспорт (ID карту) або SIM-карту (MobileID). Натепер є окремі проекти, рішення і технології, над якими працює Уряд, держагенства, представники окремих організацій та компаній: 4G, ProZorro, «розумні-міста», електронна митниця, електронна медкарта (e-Health), електронне урядування тощо. Для успішного «цифрового» стрибка в Україні необхідно забезпечити доступ до швидкісного Інтернету, до якого натепер мають доступ лише 5,5 млн громадян. У планах Уряду до 2020 року збільшити покриття широкосмуговим Інтернетом понад 70 – 80 % території України. Такий крок дозволить досягти 3 млрд дол. щорічного об'єму приватних інвестицій у сферу цифрової інфраструктури включно до 2021 року. Після створення необхідного законодавчого та регуляторного поля понад 80% бізнес процесів перейдуть у «цифру». Це в свою чергу сприятиме зростанню частки високотехнологічного експорту у випуску промислової продукції та кількості винаходів (Мінфін, 2019).

За кількісним зростанням Інтернету речей й організаційно-технологічною трансформацією виробництва стоять важливі якісні зміни в економіці. Так дані, які раніше були недоступні, із зростанням вбудованих пристроїв є цінною інформацію про характер використання продукту й устаткування для всіх учасників виробничого циклу, є основою формування нових бізнес-моделей та забезпечують додатковий дохід від пропозиції нових послуг. Віртуалізація виробничих функцій супроводжується формуванням «економіки спільного використання» (shared economy), яка характеризується істотно більш високою ефективністю і продуктивністю за рахунок підвищення використання наявних ресурсів, зміни функціоналу пристроїв без внесення змін до фізичних об'єктів, шляхом зміни технологій управління ними. Моделювання технологічних процесів, наскрізне проектування дозволяють виготовляти штучний або малосерійний продукт за мінімальною ціною для замовника та з прибутком для виробника. Еталонна архітектура, стандартизовані мережі дозволяють зробити спільну виробничу інфраструктуру доступною для середнього та малого бізнесу, що полегшує їх зусилля з управління виробництвом, дозволяє прискорити реагування на вимоги ринку і скорочення життєвого циклу продукції, та тягне за собою розробку й появу нових додатків і сервісів.

Проте надалі варто очікувати посилення систем безпеки в IoT, так як не слід забувати про різноманітні віруси, ботнети й кібератаки у цій сфері (Борисов, 2017). За попередніми прогнозами, в 2021 році витрати на безпеку зростуть майже в тричі порівняно з 2017 роком (IQusion, 2019). Експерти Frost & Sullivan відзначають, що підвищення ризиків призводить до знаходження загальних підходів до забезпечення кібербезпеки. Слід відзначити, що ринок послуг промислової кібербезпеки знаходить-

ся на піку свого життєвого циклу. Свою роль відіграють посилення регулятивної ролі урядів країн світу в області ІБ й збільшення обізнаності про проблему як на «зрілих» ринках, так і на «молодих». Серед послуг ринку промислової кібербезпеки перспективними, згідно звіту Frost & Sullivan, є такі:

– розробка інтегрованих платформ, які забезпечують високий рівень безпеки кінцевих користувачів;

– паралельне впровадження кращих практик забезпечення ІБ;

– використання автоматизованих сервісів управління та розширеної аналітики для розробки комплексного портфеля послуг, який може бути адаптований для всіх типів кінцевих користувачів;

– гнучкі моделі ціноутворення й підхід С SaaS (Cybersecurity-as-a-Service – «кібербезпека як послуга»).

Існуючі проблеми безпеки IoT-пристроїв можна вирішувати за допомогою сертифікації. Сьогодні питаннями сертифікації займаються кілька приватних компаній. Зокрема, компанія Online Trust Alliance (OTA), незалежний підрозділ компанії Verizon - ICSA Labs, компанія UL Cybersecurity Assurance (CAP). Безпека Інтернету речей стала однією з перших сфер використання блокчейн-технології. Завдяки технології розподіленого реєстру з'явилася можливість забезпечувати високий рівень безпеки IoT-пристроїв в мережі та усунути існуючі обмеження і ризики для IoT, що пов'язані з централізацією. Блокчейн дозволяє швидко і безпечно зберігати протоколи обміну й результати взаємодії різних IoT-пристроїв в децентралізованій системі. Провідні компанії Cisco, BNY Mellon, Bosch, Foxconn утворили консорціум, мета якого знаходи-

ти рішення по використанню блокчейна для збільшення безпеки і поліпшення взаємодії IoT-продуктів. Сьогодні блокчейн може використовуватися при управлінні аутентифікацією, перевірці працездатності різних сервісів, забезпечення неподільності інформації тощо. DHS США почало використовувати технологію блокчейн для захисту, передачі і зберігання даних, які збираються відомством з камер відео спостереження і різних датчиків контролю. Технологію також тестує і DARPA - підрозділ Міноборони США, що займається питаннями розробки нових технологій для армії (Крон,2018).

Для підвищення безпеки та стабільності цифрової інфраструктури України та майбутнього зростання IT-індустрії необхідним є прогнозоване та зрозуміле регуляторне середовище та захист іноземних інвестицій, включаючи права інтелектуальної власності та комерційні таємниці. Основними труднощами (проблемами) у цій сфері натепер є:

– загальна невизначеність у сталості політичного / економічного розвитку України;

– залежність української IT-індустрії від правового режиму регулювання приватних підприємців;

– висока конкуренція для кваліфікованих фахівців у сфері IT як на місцевому, так і на міжнародному рівнях;

– складні процедури отримання дозволів на працевлаштування для іноземних фахівців з інформаційних технологій;

– великий розрив між рівнем кваліфікації, що надається IT-освітою, та потребами галузі;

– дії правоохоронних органів, які передбачають втручання у звичайну господарську діяльність та арешти обладнання;

– недостатній захист і дотримання прав інтелектуальної власності та комерційної таємниці;

– низький рівень захисту персональних даних і відсутність рішення про адекватність ЄС;

– непрозорий механізм збору та розподілу авторських винагород (насамперед через Організації колективного управління);

– відсутність дієвого механізму для боротьби з патентним тролінгом;

– низька інтенсивність проведених реформ у сфері інтелектуальної власності і корпоративного управління;

– відсутність реальної та дієвої відповідальності порушників прав інтелектуальної власності (Американська торговельна палата в Україні, 2018).

Розглянувши рекомендації дослідників загроз у сфері безпеки IoT-пристроїв, виокремимо основні заходи щодо зниження ризиків та забезпечення єдності виробничої діяльності у різних підрозділах організацій:

– необхідним є запровадження політики, яка суворо обмежує використання промислових систем управління, допускаючи їх використання тільки для необхідних операцій. Знизити доступність робочих станцій і моніторів промислових систем управління з доступом до зовнішнього Інтернет через браузер;

– потрібно проводити перевірку постачальників й систем, контролювати своєчасну установку всіх виправлень та оновлень. Скоротити використання карт пам'яті USB та дисків DVD;

– необхідно ізолювати промислові системи управління від ІТ-мереж, не допускати прямі з'єднання між цими двома інфраструктурами (це відноситься до мережевих з'єднань й підключень ноутбуків та карт пам'яті);

– потрібно встановлювати використання паролів за замовчуванням у виробничій мережі та замінювати ці паролі. Використовувати двох факторну аутентифікацію всюди, де це можливо;

– доцільно перевіряти плани аварійного відновлення після масштабної кібератаки.

Можливими напрямками подолання труднощів в ІТ-індустрії України є:

– аутсорсинг програмного забезпечення;

– прийняття законів, які обмежать повноваження правоохоронних органів на вилучення обладнання;

– гармонізація українського законодавства у сфері інтелектуальної власності із законодавством Європейського Союзу відповідно до Угоди про Асоціацію Україна-ЄС;

– модернізація законодавства у сфері промислової власності;

– реформування системи організацій колективного управління з урахуванням найкращих світових практик;

– створення Національного органу з питань інтелектуальної власності;

– утворення і функціонування Вищого суду з питань інтелектуальної власності (Американська торговельна палата в Україні, 2018).

Зауважимо, що IT тенденції неможливо розвивати без якісної глобальної інфраструктури. Сьогодні така інфраструктура представлена великими дата-центрами. Їх кількість у світі щорічно зростає. У першу чергу це пов'язано з розвитком більшості напрямків IT, які збільшують у свою чергу обсяги глобального трафіку, кількість даних та вимагають великих обчислювальних та пропускних потужностей (IQusion, 2019).

Виходячи з проведеного дослідження рахуємо, що найбільш затребуваними в 2019 році будуть автоматизація, безпека, блокчейн, IoT, ЦОДи. Ці основні напрямки будуть сприяти розвитку інших більш досконалих засобів обробки, передачі, введення даних тощо.

Список використаних джерел

Finance.ua (15.02.2019). *IDC: рынок Интернета вещей в Европе в 2019 году покажет значительный рост*. Доступ через https://news.finance.ua/ru/news/-/443966/idc-rynok-interneta-veshhej-v-evrope-v-2019-godu-pokazhet-znachitelnyj-rost

ICT Moscow (2019). Платформа. «Цифровая воронка» потребления: особенности и перспективы российского рынка IoT. Доступ через https://ict.moscow/research/cifrovaya-voronka-potrebleniya-osobennosti-i-perspektivy-rossiyskogo-rynka-iot/

IQusion (2019). *Тренди 2018 року, що залишаються популярними в 2019 році*. Доступ через https://iqusion.com/2019/03/11/

TAdviser (07.07.2019). ИТ. *IIoT Industrial Internet of Things - Промышленный интернет вещей)*. Доступ через http://www.tadviser.ru/index.php

index.php/Статья:IIoT_-_Industrial_Internet_of_Things_(Промышленный_интернет_вещей)

Американська торговельна палата в Україні. (2018). *Огляд економіки України*. Доступ через www.chamber.ua/Content/Documents/-1635684409Country_Profile_2018_UA.pdf

Борисов, М. (2017). Проблемы реализации промышленных приложений Интернета вещей. *Открытые системы, 4*. Доступ через https://www.osp.ru/os/2017/04/13053376/

Бугера, О. (2018). Інтернет речей та запобігання злочинності. *Підприємництво, господарство і право. 6*. 295-298. Доступ через http://pgp-journal.kiev.ua/archive/2018/6/54.pdf

Крон, А. (2018). IoT и проблемы безопасности. [Blogpost]. *Unet*. Доступ через https://habr.com/ru/company/unet/blog/410849/

Мінфін. (2019). *Цифрова економіка. Що чекає Україну в найближчі три роки*. Доступ через https://minfin.com.ua/ua/2018/01/30/32121695

Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. Кабінет міністрів України. № 67-2018-р. від 18 січня 2018. Доступ через https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

Current elections campaigns in Europe and Ukraine are undoubtedly due to show us the real scale of the Russian cyber threat. The European continent has turned out to be a digital battlefield where hackers, in particular state-sponsored ones, test and improve their skills. Cyber-attacks such as Not-Petya showed that Ukraine and Europe are closely interconnected and the common plan of actions is needed to resist the cyber threat, be it through public, private or civil society sphere.

Being a civil society organization Promote Ukraine with support of the partners organized the conference "Behind the digital curtain. Civil society vs state sponsored attacks".

Sponsors and partners of the conference

Djannet.com
East West Mentor
DigitYser
CyberDesk
Institute of Innovative Governance
БізнесWoman
Хмельницький національний університет
Львівський національний університет ім. І. Франка
Київський національний економічний університет
ім. В. Гетьмана

promoteukraine

promoteukraine

promoteukraine

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.