**DOI:** https://doi.org/10.17721/ISTS.2020.1.3-8
UDC 004.56.5

# ANALYSIS OF THE PRIMARY TRENDS IN CYBERSECURITY

**Oksiiuk Oleksandr [1]**
**orcid.org/0000-0001-9797-6015**
**Zerko Andriy [2]**
**orcid.org/0000-0003-2000-7835**
**Fesenko Andriy [3]**
**orcid.org/0000-0001-5154-5324**

[1] Kyiv, Taras Shevchenko National University of Kyiv, oksiuk@ukr.net
[2] Kyiv, Taras Shevchenko National University of Kyiv, a.l.zerko@ukr.net
[3]Kiev, Kiev National Taras Shevchenko University, aafesenko88@gmail.com

**Article history:**
Received by the editor 04.01.2020
Accepted 12.01.2020

**Key words:**
cybersecurity;
cyberspace;
information protection;
cyber-attacks;
threats

**Abstract:** Open and free cyberspace increases the freedom of people and social communications, in such conditions it becomes especially important to search for new possibilities of ensuring the state security in view of the formation of a new confrontation field - cyberspace. It is important to analyze the actual problems of information security, actions of the world governments and world organizations for identifying the current state of modern trends in the cybersecurity field. Cybersecurity incidents affect the lives of consumers of informational and many other services, and cyberattacks targeting various objects of electronic communications infrastructure or process management. This article covers in detail the factors that influence the state of cybersecurity in the country, its cyberspace and the protection of information objects. The rapid development of malicious software in the world and the lines of action by famous hacker groups are analyzed. The tendencies of active legislative updates in the cybersecurity field of the world's leading countries, such as creating new structural groups, increasing the number of existing ones and increasing their funding, are identified. The reasons for attackers concentrating their efforts on the search for assets vulnerabilities and the development of a unique multifunctional malware and technologies for unauthorized assets are considered. Structured information about the status of modern trends in the field of cybersecurity and information protection is presented in this article. The situation that has evolved to date with cybercrime requires continuous improvement of cybercrime fighting methods, development of information systems and methods aimed at ensuring the country's cybersecurity. Therefore, the issue of cyberspace security, cybercrime fighting is relevant internationally as well as at the national level and therefore needs further consideration.

**Анотація:** Відкритий та вільний кіберпростір збільшує свободу людей та соціальну комунікацію, в таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору. Важливо проаналізувати актуальні проблеми інформаційної безпеки, дії урядів світу та світових організацій для виявлення сучасного стану сучасних тенденцій у сфері кібербезпеки. Інциденти в сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг та кібератаки, націлені на різноманітні об'єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами. У цій статті детально розглядаються фактори, що впливають на положення кібербезпеки країни, її кіберпростір та захист інформаційних об'єктів. Проаналізовано стрімкий розвиток шкідливого програмного забезпечення у світі та напрямок дій відомих хакерських угрупувань. Виявлено тенденції активних оновлень законодавства у сфері кібербезпеки провідних країн світу шляхом створення нових структурних груп, збільшення кількості існуючих та збільшення їх фінансування. Розглянуто причини концентрації зусиль зловмисників на пошуку вразливості активів та розробці унікальної багатофункціональної зловмисної програми та технологій для несанкціонованих активів. Структурована інформація про стан сучасних тенденцій у сфері кібербезпеки та захисту інформації представлена в цій

статті. Ситуація, яка склалася на сьогоднішній день з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни. Отже, питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

## 1. INTRODUCTION

The rapid development of information technology (IT) is transforming the world. An open and free cyberspace increases people`s freedom and social communications, makes relationships between them easier and creates a new global interactive place for many ideas, researches and innovations.

At the same time, access to cyberspace created because of compatible communication systems and electronic communications that are using the Internet or other global data networks, is allowing to gain advantage in the political, economic, military, social, scientific, technological and other spheres.

New technologies and new users will reshape cyber-risks in 2020. The emergence of 5G networks in 2020 will result in substantially broader access for both devices and people. Greater and more convenient broadband at higher speeds will encourage the development and deployment of everything from connected devices and ubiquitous computing to virtual as well as augmented reality and artificial intelligence.

The number of national and municipal laws and regulations addressing cybersecurity – through either new proposals or updates to existing measures – will also increase. While calls for greater alignment across regulatory regimes will continue to grow, there will be little change on this front in the near term owing to the pace and complexities of law-making process and continued debate about the underlying cybersecurity requirements. Continued volatility across the geopolitical landscape will also add to this delay and cybersecurity threats will evolve to exploit the ever-changing environment.

However, the advantages of modern digital world and the growth of information technology led to the emergence of new national and international security threats. Besides natural incidents, there is also an increase in the number and power of threats that benefit individual states, groups or individuals. Depending on their intentions and motivation, these threats can include:

- Collection and theft of information resources for further use or sale;
- Industrial espionage and diversion;
- Hacking networks in order to gain access to their information and use them to implement cyber-attacks;
- Violation of network processes with cyber-attacks or malicious software;
- Attacking or exploiting important infrastructure objects;
- Personal data theft.

## 2. ACTIONS IN THE CYBERSPACE OF THE WORLD`S COUNTRIES

The leading countries of the world are focusing on the creation and improvement of legislations in the cybersecurity sphere in order to increase the level of digital information protection.

At the same time, the continued aggression in cyberspace from Russian Federation was the reason for several incidents and other changes in the protected external and internal environment of the world`s leading countries.

Let us analyze some actual examples of actions in cyberspace of the countries in the world that deserve attention:

1. USA.

In December 18, 2017, the updated US National Security Strategy has been published; it included directives that might increase the level of country’s protection against cyber threats.

2. EU.

The Research Center of the European Parliament reported that one of the main directions of EU policy in 2018 is to increase the cybersecurity because of the threat from Russia.

3. Great Britain.

The British Cabinet has produced a transitional national science and technology strategy in the cyber security sphere aimed at ensuring the UK`s technological capacities’ resistance to cyber-threats.

4. France.

In February, 2018, the Government of France has approved the Strategic Review of Cybersecurity (Review) containing the country`s strategic tasks in the sphere of digital and information technology taking into consideration the current geopolitical state, as well as improving the new instruments of warfare.

In order to adhere to the standard of the country`s cybersecurity, a consecutive increase of personnel in the Cyber Command (CYBERCOM) of the General Staff of the Armed Forces of France is in order: to 3200 people by 2019 and to 4K people by 2025.

5. Germany.

The government of Germany is considering the possibility of introducing corrections to the country`s constitution regarding the problem of hacker`s attacks aimed at private computer networks. The Germany's Ministry of International Affairs delegate stated that the relevant reforms were to be completed in 2018. The experts think that the possible methods of protection from hackers include the probability of disabling servers used by attackers in offensive.

6. Japan.

During the second quarter of 2018, the Japanese government intended to develop criteria for the danger of cyberattacks on critical infrastructure of the country (this includes railways, electricity, financial institutions and so on). This will help the government use appropriate measures to fight crisis.

The concrete ways of government`s response to a cyberattack will change depending on the six-level scale of threats.

7. Georgia.

At the end of November 2017, the Government of Georgia has announced about additional $35 million to fund the creation of the Innovations Center and Cybersecurity Training.

The results of the analysis show the tendency of active legislative updates in the cybersecurity sphere of the leading countries of the world, the increase of cybersecurity level achieved by the creation of new structural divisions and increased amount of funding, mainly because of the threat from Russia.

## 3. ACTIONS OF INTERNATIONAL ORGANIZATIONS AND LEADING COMPANIES IN THE CYBERSECURITY SPHERE

International organizations and leading companies in the cybersecurity sphere are actively exploring the cyberspace usage to increase the protection level of the vital interests of citizens, society and state, as well as to protect their assets by creating cyber security systems, cyber security centers, cyber defense hardware and software complexes.

The following actual examples of international organizations' and leading cyber-security companies' actions are given for the analysis:

UN Secretary General Antonio Guterres at The Munich Security Conference during his speech said that our world needs determination in responding to cyber-attacks on the international field.

He proposed to start a discussion on that matter at the UN General Assembly residency.

As part of reforming the NATO command structure, they are reevaluating cyber capabilities of the Alliance for strategic cybersecurity.

On February 14 – 15, 2018 at the meeting at the NATO Headquarters in Brussels, the North Atlantic Council at the level of defense ministers of NATO`s member states decided to create a NATO Center for Cyber Operations (Cyber Operations Center). This Center will be integrated with Headquarters of the NATO Operations Command (SHAPE) in Mons, Belgium.

The Press Service of the Cybersecurity Center of the NATO Center (CCD COE), based in Estonia reported on January 30, 2018 that the Center is starting to identify the need for training new specialists in the field of cybersecurity and coordinating their education.

Experts from American Network Protection "FireEye" have discovered a new Triton (Trisis) malware family with status of rare malicious electronic medium, which runs often in the Middle East.

The main object of this wrecker is to prevent the work of industrial defense systems that are protecting workers' lives.

Hackers can use Triton in the system to create a dangerous situation, even dealing physical damage.

The cybersecurity researchers from the American company Cisco Talos were able to detect the SPO that was used to attack the sites of the 2018 Olympics.

"During the attack, hackers interrupted the work of digital interactive television at the main Press Center of the Winter Olympics in Pyeongchang, South Korea, and caused a crash in the Wi-Fi network at the stadium".

Software called "Olympic Destroyer" is a malicious program for operation systems based on Windows that can complete a lot of hacker`s tasks, especially infecting a device with multiple files that steal stored passwords from Internet Explorer, Firefox and Chrome browsers, as well as computer system passwords.

The National Institute of Standards and Technology of the USA (NIST) has published a document project "The Status of International Cybersecurity Standardization for IoT", that can help in developing security standards for IoT.

NIST proposes to divide IoT into five functional areas:

- Device connection;
- IoT of the consumer class;
- Medical equipment and devices used in health care area;
- "Smart" homes;
- "Smart" production (including ACS);

Standards should be developed for each area, taking into account its specifics.

Taking into consideration all of the above and according to the results of the analysis, it can be

noted that international organizations and leading companies in the field of cybersecurity are taking active measures protecting the vital interests of citizens, society and state in cyberspace.

## 4. ACTUAL THREATS IN CYBERSPACE AND ASSETS VULNERABILITY

Attackers are developing new computer viruses and malware to gain access to assets owned by a person, organization or state.

The following cyber threats and vulnerable assets that deserve attention are given for analysis.

**GandCrab malware**

Experts of the company "Malwarebytes" reported about new ransomware that is spreading in a very unusual way – with the help of two sets of exploits.

The activity of ransomware "GandCrab" was first recorded on January 26, 2018. This malware was distributed by two separate exploits – RIG and GrandSoft.

The RIG contains exploits for vulnerabilities in Internet Explorer and Flash Player to execute JavaScript, Flash or VBscript attacks. The RIG is probably distributing GandCrab through malicious advertisements on compromised sites.

The second set of GandCrab`s exploits, GandSoft, exploits vulnerabilities in the Java Runtime Environment, which allows to remotely execute the code.

After installing it into the system, GandCrab works like most of ransomware – encrypting files that are stored on the computer using RSA algorithm, adding GDCB extension to them and then demanding a payment for the recovery tool. However, unlike most cryptographers, GandCrab requires payment not in Bitcoin, but in the cryptocurrency Dash. This fact is another proof that cybercriminals are ceasing the use of Bitcoin little by little in favor of other cryptocurrencies.

**Coinhive malware**

On February 11, 2018, thousands of government websites in the UK and Australia were attacked by the Coinhive malware, which exploited the potential of infected computers to demand cryptocurrency. With this, the National Cybersecurity Center of the United Kingdom (NCSC) published a tutorial that describes attacks using third-party JavaScript archives and gives advice for website administrators and community agents to counter the attack.

The experts of the center note that hackers are focusing on discrediting additional computer systems, since this allows them to initiate a much more complicated criminal operation.

**Dridex malware**

Security researchers from Forcepoint reported about a new fishing campaign, in which attackers use discredited FTP resources to spread the banking trojan, Dridex.

This trojan spreads by phishing emails and by deceptive offers to download and execute malicious macros that are hidden in Microsoft Office documents. Once in the system, Dridex steals credentials for online banking, which attackers can then use for stealing money from the victim's bank account.

This campaign has begun on January 17, 2018. Phishing letters were sent mainly to top level domains, such as .com, .fr, and .co.uk. The highest number of victims was recorded in France, the United Kingdom and Australia.

According to experts, the Dridex campaign uses two types of documents: an XLS file with malicious macros that downloads trojan on the device, and a DOC file that exploits a vulnerability in Dynamic Data Exchange (DDE) to execute attacker`s commands.

**Cisco ASA firewall software vulnerability (CVE-2018-0101)**

Cisco Company informed their clients without going into details that the attackers are actively exploiting the critical vulnerability CVE-2018-0101, which affects Cisco Adaptive Security Appliance (ASA) an operating system run by the Cisco ASA family of firewalls. This vulnerability allows a remote unauthorized hacker to execute any code or evoke a denial of service.

Hacker groups continue to actively search for vulnerabilities in assets and control systems in order to realize new cyber threats.

The actions of hacker groups that deserve attention can be determined:

**A cyber espionage group Fancy Bear (APT28)**

The cybersecurity researchers from ESET have reported about appearance of a new Xagent malware feature – one of the main tools in the Fancy Bear hacker group (APT28).

They also noted that the main objects of this group`s attack are still government agencies and embassies around the world, and especially in Eastern Europe.

The "Talos Group" has exposed a new criminal cyberattack from hacker group APT28. The document created by this group is the leaflet of the CyCon U.S. Conference, organized with the Cyber Institute of the US Military Academy and the CCD COE (7 – 8 November 2017, Washington). The leaflet does not contain malicious software, but activates the execution of a malicious code inside a fake document when it`s opened.

**Hackers group Dark Caracal**

This hacker group, which is allegedly related with the Lebanese government, has stolen hundreds of gigabytes of information from thousands of

victims around the world using only phishing emails and simple malware. This is stated in the common report of the human rights organization Electronic Frontier Foundation and cybersecurity company Lookout.

## 5. CYBERCRIME

Cybercriminals continue to realize socially dangerous attacks in cyberspace.

The Council of Economic Advisers under the President of the United States created a list of "hacker states", which included:

- Russia;
- China;
- Iran;
- The DPRK.

This was reported in the 62-page report of the Council "Cost of Malicious Cyber Activity to the U.S. Economy".

In the report, economists identified six categories of cybercriminals depending on their targets:

The first category includes Russia, Iran, China and the DPRK, whose state hackers have political, economic, technological, and military targets.

The second category includes corporations who wish to acquire their competitors' industrial secrets and intellectual property. Many of them are funded by the state.

The third category is "Hacktivists", whose activity in the cyberspace is a protest action. Their actions have a propagandistic nature, and they cause losses for organizations for ideological reasons.

The fourth category includes organized cybercrime groups that carry out targeted attacks for the purposes of acquiring profit.

Next are the "Opportunists" – unprofessional hackers who want popularity. In their attacks, they use widely available techniques and codes.

The last category consists of insiders – present or former employees of companies, prompted by revenge or profit.

Considering all of the above, it can be noted that cybercriminals of different categories are actively searching for vulnerabilities in assets and management systems to reach their political, economic, technological, military and other objectives.

## 6. Conclusion

According to the results of the analysis, the main trends in the cybersecurity sphere are the following:

The leading countries of the world and foreign companies are actively researching the aggressive actions from RF in cyberspace and note that such cyberattacks lead to losses in the political, economic, technological and military spheres (USA, UK, Australia, Canada and New Zealand are blaming Russia for organizing a cyberattack using NotPetya malware in the summer of 2017. Estonia has published an annual report that analyzes Russia`s cyberbullying activities).

The leading countries of the world continue the process of legislative consolidation in the sphere of cybersecurity (France approved the Strategic Review on cybersecurity; in Poland the bill about nation system of cybersecurity was developed).

The leading countries increase their operational capabilities in order to raise the level of cybersecurity, create new structural units and increase the number of existing ones (NATO has provided the yearly cyber training "Crossed Swords", the USA`s Ministry of energy created a new unit for cybersecurity, energy security and emergency responding. France plans to increase the number of those units up to 4,000 by 2025. The Australian Defense Forces have created a cyber-command).

The leading countries of the world are concentrating attention on the interactions with state bodies and with private organizations to increase the protection level of critical infrastructure objects (France is planning a full engagement of private companies to the common process of the securing cyberspace).

Attackers are focused on finding vulnerabilities in assets (control systems) and developing multifunctional malware with unique properties and technologies for unauthorized access to assets (attackers focus on discrediting additional computer systems, allowing them to gain access to the main asset in the future; the ransomware from GandCrab is spread by unusual way – with two sets of exploits).

Russian-oriented hacker groups continue to carry out cyberattacks on the assets of the Ukrainian segment of the Internet and on assets of the Ukraine-oriented countries of the world, foreign companies, institutions, organizations. Notably, for some of the hacker groups the targets of their attacks are the same as actions of the Russian government policy (for example, interference by hacker groups ATP28 and ATR29 in the US election process).

The leading countries of the world are researching to determine the legal status of cryptocurrencies and legal regulation of transactions with them. At the same time, attackers are actively searching for vulnerabilities in assets and control systems to use their resources to get the cryptocurrency or steal it.

Cyber defense is the only thing that can prevent the loss of information and the interference of some countries into the security of others. The analysis identified the main areas of protection against cyber threats, protection of sovereignty of cyberspace and

national security in the leading countries of the world.

## 7. References


[1] Cybersecurity Trends Report 2019 // elevenpaths. – 2019. – URL: https://www.elevenpaths.com/ cybersecurity- trends-report-2019/index.html. The Hacker News — Online Cyber Security News & Analysis. URL: https://thehackernews.com/.

[2] North Atlantic Treaty Organization official website. URL: https://www.nato.int/.

[3] United Nations official website. URL: http://www.un.org/.

[4] FireEye, Threat Research Blog. URL: https://www.fireeye.com/blog/threat-research.html.

[5] Cyber Security Essentials. James Graham, Ryan Olson, Rick Howard. N.Y.: CRC Press, 2010.

[6] Michelle Nichols. North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report / Michelle Nichols // reuters – URL: https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

[7] State of Cybersecurity Report 2018 // wipro. – 2018. – URL: https://www.wipro.com/ content/dam/nexus /en/service-lines/ applications/latest-thinking/state-of-cybersecurity-report-2018.pdf..

[8] State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development // isaca. – 2019. – URL: https://www.isaca.org/ bookstore/bookstore-wht_ papers-digital/whpsc191..

[9] Bernard Marr. The 5 Biggest Cybersecurity Trends In 2020 Everyone Should Know About / Bernard Marr // www.forbes.com. – 2020. – URL: https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone -should-know-about/#4e86a2857ecc

[10] Cybersecurity Trends for 2019 // cisecurity.org. – 2018. – URL: https://www.cisecurity.org/blog/ cybersecurity-trends-for-2019/.

[11] Elias chachak. Top 10 Countries Best Prepared Against Cyber Attacks / ELIAS CHACHAK // cyberdb.co. – 2019. – URL: https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/.



***Oksiiuk Oleksandr***
*Dr.Sc., Professor, Head of Cybersecurity and Information Protection Department, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.*
*Interests: theory and practice of developing automated systems and conducting expert assessments, models and methods of building integrated information security.*



***Zerko Andriy***
*Graduate student of Cybersecurity and Information Protection Department, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.*
*Interests: information security, information technology*



***Fesenko Andriy***
*PhD., Assistant Professor of Cybersecurity and Information Protection Department, Faculty of Information Technology, Kiev National Taras Shevchenko University*
*Interests: information security, cybersecurity*