UDC 327.7

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION

Исаева Аяжан Байжанкызы, Бакибаева Дамеля Ардаковна
E-mail: damelya2002@mail.ru, E-mail: issayeva.ayazhan@mail.ru
Студентки 1 курса кафедры международных отношений, ЕНУ им.Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Кенжалина Г.Ж.

In an informational age, the importance of cybersecurity is growing due to various incidents in a cyberspace. The European Union is an organization of a group of European countries that act together in political and economic matters, also made an effort to strengthen cybersecurity in Europe. As it is written on the official website of European Council and Council of European Union: Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies

depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring. For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognize its leading role. Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems [1, p. 2].

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. […] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."[2]

The European Commission and the High Representative have proposed a wide range of concrete measures that will further strengthen the EU's cybersecurity structures and capabilities with more cooperation between the Member States and the different EU structures concerned. These measures will ensure that the EU is better prepared to face the ever-increasing cybersecurity challenges.

Europeans believe that digital technologies have a positive impact on our economy (75%), our society (64%), our quality of life (67%). 86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing. Sectors like transport, energy, health and finance have become increasingly dependent on network and information systems to run their core businesses. Sectors like transport, energy, health and finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things (IoT) is already a reality. There will be tens of billions of connected digital devices in the EU by 2020.

For the last years cyber incidents and attacks are on the rise:

- +4,000 ransomware attacks per day in 2016.
- In some Member States 50% of all crimes committed are cybercrimes.
- Security incidents across all industries rose by 38% in 2015 – the biggest increase in the past 12 years.
- +150 countries and +230,000 systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including hospitals and ambulance services.
- 80% of European companies experienced at least one cybersecurity incident last year.

The scale of the problem makes it necessary to act at the European level. Recent figures show that digital threats are evolving fast: ransomware attacks have increased by 300% since 2015. According to several studies, the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further rise by a factor of four by 2019. Evidence suggests that people from around the world identify cyber-attacks from other countries among the leading threats to national security. Furthermore, in the aftermath of the "Wannacry" and "(Non)Petya attacks", a recent report has estimated that a serious cyber-attack could cost the global economy more than €100 billion.

According to the statistics of EU, despite the growing threat, awareness and knowledge of cybersecurity issues is still insufficient.

69% of companies have no or basic understanding of their exposure to cyber risks.

60% of companies have never estimated the potential financial losses from a major cyber-attack.

51% of European citizens feel not at all or not well informed about cyber threats.

The EU needs more robust and effective structures to ensure strong cyber resilience, promote cybersecurity and to respond to cyber-attacks aimed at the Member States and at the EU's own institutions, agencies and bodies. It also needs strong cybersecurity for its Single Market, major advances in the EU's technological capability and a broader understanding of everybody's role in countering cyber threats. In response, the Joint Communication suggests new initiatives to further improve EU cyber resilience and response in three key areas:

- Building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity;
- Creating an effective criminal law response;
- Strengthening global stability through international cooperation.

The Commission and the High Representative are therefore proposing to reinforce the EU's resilience, deterrence and response to cyber-attacks by:

- Establishing a stronger European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks.
- Creating an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world.
- A Blueprint for how to respond quickly, operationally and in unison when a large scale cyber-attack strikes.
- A network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.
- A new Directive on the combatting of fraud and counterfeiting of non-cash means of payment to provide for a more efficient criminal law response to cyber crime.
- A Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.
- The EU aims at driving high-end skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a cyber defence training and education platform[3].

On 18 October 2018, the European Council called for measures to build strong cybersecurity in the European Union.

EU leaders referred in particular to restrictive measures able to **respond to and deter cyber-attacks.** The basis for the renewed EU commitment to tackle cyber threats is a European Commission **reform package** on cybersecurity tabled in September 2017.

This reform aims to build on the measures put in place by the cybersecurity strategy and its main pillar, the directive on security of network and information systems - the **NIS directive.**

The proposal sets out new initiatives such as:

- building a stronger EU cybersecurity agency
- introducing an EU-wide cybersecurity certification scheme
- swiftly implementing the NIS directive

EU leaders regard cybersecurity reform as one of the main ongoing aspects on the road to completing the EU digital single market.

The Commission also proposed to build a stronger EU cybersecurity agency on the structures of the existing European Union Agency for Network and Information Security (ENISA). The new agency's role would be to help member states, EU institutions and businesses deal with cyber-attacks[4].

Taking into account the measures and problems of cybersecurity The European Council adopted conclusions on internal security, following the Leaders' Agenda thematic debate in Salzburg on 20 September 2018. To ensure a high level of network and information security EU is implementing the adoption of Passenger Name Records. The EU will strengthen actions against to the cyber-attack carried out against the Organisation for the Prohibition of Chemical Weapons (OPCW). The European Council also calls for measures to combat cyber-enabled illegal and malicious activities.The Commission of the European Public Prosecutor's Office examine cross-border terrorist crimes which helps to reduce effective spread of radicalisation and terrorism. Finally, heads of state or government will also address the need for adequate resource for Europol to face new challenges posed by technological developments, the need for improvements in theinteroperability of information systems and databases as well as the need to strengthen the EU's crisis management capacity, mainly through the proposed EU civil protection mechanism [5].

Cybersecurity package (2017) built on the review of 2013 Cybersecurity Strategy

The European Commission and the High Representative have proposed a wide range of concrete measures that will further strengthen the EU's cybersecurity structures and capabilities with more cooperation between the Member States and the different EU structures. The revised Cybersecurity strategy called : Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Building EU Resilience has 3 main objectives: Implementation of NIS Directive which proposed cybersecurity certification Framework, Reinforce and restructure ENISA to support Member States, EU institutions and businesses in key areas and the last one rapid emergency response and crisis management (reinforced tools and a new emergency fund).Creating effective EU cyber deterrence includes identifying malicious actors, strenghtening the law enforcement response (cybercrimers effective investigation and prosecution, cross border access to electronic evidence, traceability and attribution, an improved forensic capability of Europol, role of encyption) and stepping up the public private cooperation against cybercrime (e.g. between financial institutions and law enforcement bodies against online frauds).Strengthening international cooperation on cybersecurity fueled with the EU core values and fundamental rights (freedom of expression, right to privacy and protection of personal data, promotion of the open, free, stable and secure cyberspace). Also contains cybersecurity in external relations (prevention and deterrence of cyber attacks, strategic framework for conflict prevention and stability in cyberspace) [6].

Digital Europe programme 2021-2027

It contains 5 key policy areas: High-performance Computing, Cybersecurity, Artificial Intelligence, Advanced Digital Skills and best use of Digital Capacities and Interoperability.EU's cybersecurity capacity is going to be reinforced to gain the necessary capacities to protect its citizens and businesses from cyber threats. Consumers will be protected when using connected products that can be hacked and their safety compromised. Trust is a prerequisite for the Digital Single Market to work well. Cybersecurity technologiessuch as digital identities, cryptography or intrusion detection, and their application in areas such as finance, industry 4.0, energy, transportation, healthcare, or e-government are essential to safeguard the security and trust of online activity and transactions by both citizens, public administrations and companies.Wide deployment of the latest effective state of the art cybersecurity solutions including advanced cybersecurity equipment, tools and data infrastructures will be supported according to this programme [7].

EU company on 4 February,2019 adapted new law to the digital era

The presidency of the EU Council reached a provisional agreement with European Parliament's representatives on a draft directive that will facilitate the use of online solutions in a company's contacts with public authorities through digital tools. The draft directive provides that the companies are able to registir branches online and make available for cross-border users and fees charged for the online registration of companies do not exceed the overall costs incurred by the member state.Documents submitted by companies are stored and exchanged by national registers in machine-readable and searchable formats. The EU Council marked that the draft directive provides for safeguards against fraud and abuse in online procedures, including the control of the identity and

legal personality of a person setting up a company, and the possibility of requiring physical presence before the competent regulatory authority [8].

Conclusion

The European Union is seriously concerned about cyber security. The cyber strategies of the EU emphasize the need for joint efforts of the state, society, business and all citizens in the fight against cyber threats.The EU has made a lot of progress under the 2017 EU Cybersecurity Strategy. It has created a comprehensive regulatory to increase cyber resilience across the Union. The EU is on the right track, but with digitalisation progressing at full speed and the evolving of cyber threats, the EU should embed cybersecurity principles in all relevant policies, such as the (Digital) Single Market (e.g. online platforms, and the data, collaborative, and app economy), education (knowledge, skills, and life-long learning), industry, innovation, investment, as well as in defence cooperation.

Literature

1. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions, Brussels, 7.2.2013 // https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
2. European Commission President Jean-Claude Juncker, State of the Union Address, 13 September 2017
3. PWC, Global State of Information Security Survey, 2016 // https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf
4. Reform of cybersecurity in Europe, European Council, Council of the European Union // https://www.consilium.europa.eu/en/policies/cyber-security/
5. European Council conclusions, 18 October 2018 // https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/
6. Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017 // https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf
7. Digital Europe programme - Coreper confirms common understanding reached with Parliament // https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/digital-europe-programme-coreper-confirms-common-understanding-reached-with-parliament/
8. EU company law adapted to the digital era // https://www.consilium.europa.eu/en/press/press-releases/2019/02/04/eu-company-law-adapted-to-the-digital-era/