Cybersecurity – An Instrument of Influence and Meddling in the Decision-making Process of "Partner" Countries

In 2018, Black Friday sales totalized $6.22 billion in online sales a 23.6% jump from last year with over $1 billion in sales from smartphones[1]. In UK, online transactions were up 47% compared to last year[2].

Mihaela-Adriana Pădureanu[3]

Abstract

As is the case with new domains in which the economic activity takes a turn for the better, the huge increase in internet usage and access to the network have more than tripled in the last two decades (in 2005, 16% of the world population had access to the internet, while in 2017 48% of the world population had access to internet). Therefore, this new sector has attracted the attention of policymakers that started to see the opportunities through which they could gain access to different groups and people and capitalize the gains or try to obtain different advantages for them or their country.

In this paper, we will present the evolution of the cyber sector in Europe's Eastern Neighbourhood and the main threats posed by the threats in this area, for states and non-states actors. Also, we will describe and analyse the main steps taken at international and European levels to respond to these activities. Because most of the clashes between states and non-states actors that took place in cyberspace involved European parts, we consider the topic and the chosen methods as highly relevant for the discussion about cybersecurity.

[1] Thomas, Lauren. „Black Friday pulled in a record $6.22 billion in online sales: Adobe Analytics"(28.11.2018), CNBC https://www.cnbc.com/2018/11/24/black-friday-pulled-in-a-record-6point22-billion-in-online-sales-adobe.html (29.11.2019). The numbers are for US.

[2] BBC News, „Black Friday shoppers 'spending less', (23.11.2018)", https://www.bbc.com/news/business-46320551 (29.11.2019).

[3] Mihaela-Adriana Pădureanu PhD, vice president of the Experts for Security and Global Affairs Association (ESGA), Bucharest, Romania. This policy paper is elaborated within the project "Understanding the Eastern Neighborhood. A unique platform for comprehensive debates and analysis on Russian affairs", implemented by ESGA between February 2018 –January 2019. All the views and opinions belong to the author and do not necessarily represent those of the ESGA Partners.

Introduction

Today, Eastern Europe comprises Ukraine, Belarus, and Republic of Moldova, countries united by certain political, economic and social features[4]. This year, EU's Eastern Partnership initiative will celebrate its 10th anniversary in a regional context very different from the one that existed in 2009. Without a doubt, the situation in Ukraine is by far the most complicated part of this puzzle and it looks like many policymakers lack the instruments and tools necessary to understand the problems in the region and act accordingly. Europe's Eastern Neighbourhood can be seen as a region characterized by an imbalance of power – material, as well as social. Two main actors – the EU and the Russian Federation are willing to provide resources in order to influence the evolution of the region. From the six member countries of Eastern Partnership, three have signed an Association Agreement with EU, which will allow them to deepen their relationship with it and hopefully, provide more stable and prosperous societies to their citizens. However, with the notable exception of Georgia, which managed to maintain the reform process after the signing of the Association Agreement, all the countries in the region are having difficulties on the political, as well as the economic fields when it comes reforms and changes that need to be implemented. The Republic of Moldova has been in a dramatic decline in the last two years and Ukraine is involved in a dangerous and, as far as can be seen, long-term conflict with the Russian Federation. Therefore, the appetite for reform-implementation and domestic strong democracy consolidation is rather low.

In this context, activities in the cyberspace are just another way in which certain parties and groups can influence the outcome of political negotiations – including the evolution and role of different leaders. As is the case with other regions around the world, internet access in Eastern Europe has grown considerably in the last decade. For example, in 2016, 53% of Ukraine's population had access to internet compared to just 17.9% in 2009; in Moldova, the number of people with access to internet increased from 27.5% in 2009 to 71% in 2016; and in Georgia from 20.07% in 2009 to 60.49% in 2016[5]. In the Russian Federation, the increase has

[4] See for example: Radio Free Europe Radio Liberty countries in the section East Europe https://www.rferl.org/ (29.11.2019).

[5] The World Bank, "Individuals using the Internet (% of population) Ukraine" https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=UA (30.11.2018).

been from 29% in 2009 to 76% in 2017. Therefore, the number of participants to this space has increased constantly and some of the actors want to influence what is happening there, in the cyberspace. This new "space" just like what is happening due to the Arctic sea ice decline brings into discussion the necessity to formulate rules for the interaction that takes place there. The states started to understand that this space needs to be protected, because it can be attacked by different groups who can use the date for several reasons – for example, some can just sell on the black market. In this paper, we are interested to see how different actors in Eastern Europe influence and act in this "space", especially after 2013. Most of the time, cybersecurity is associated with or considered part of *hybrid threats* or *hybrid war*. The use of term hybrid in relation to defence or security topics increased after US involvement in Afghanistan and Iraq[6] and today is used as *a catch-all* phrase describing almost all the threats and actions found in 21st-century conflicts[7].

Cyber defence, cybersecurity and main actors involved in regulating the cybersecurity domain in Euro-Atlantic space

Defending the cyberspace went from being discussed between countries' representatives to one of the main subjects in official documents and strategies, especially in the last decade. In today's plethora of information finding a definition for *cyber*-related problems proves to be a difficult task. We have terms such as cyber defence, cyberspace defence and cybersecurity with definitions at the national levels – with different states formulating particular definitions for it – and professional definition - from specialized organizations like International Organization for Standardization. These two types of actors that aim to describe the term also show two different possible paths that can be followed when it comes to the topic of *cyberspace*. First, we have the political approach – meaning the way in which policymakers define the

[6] Hoffman, Frank G. (2009). „Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict", *Strategic Forum* no. 240, April 2009 https://s3.amazonaws.com/academia.edu.documents/43436887/SF240.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1546541148&Signature=lCeozZcSQruZfCvYSehv%2BSvvhrc%3D&response-content-disposition=inline%3B%20filename%3DHybrid_Threats_Reconceptualizing_the_Evo.pdf (02.12.2018).

[7] Pawlak, Patryk (2017). „Countering hybrid threats: EU-NATO cooperation", European Parliament, European Parliamentary Research Service, pp. 2-3, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf (02.12.2018).

possible threats and vulnerabilities to the cyberspace and which tools can be used to answer these threats. Second, we can discuss cybersecurity from the point of view of experts in technical fields like engineers, IT experts, etc. In this paper, we will explore the first approach.

Before discussing the role of different actors in this area, we should offer some working definitions for the main terms used in this paper. As this study only aims to present and describe certain interactions between actors in Eastern Europe after 2013, competing for different aims in cyberspace, we will not present all the terms related to cyber defence, but only cybersecurity and cyber threats[8]. The first important term is cybersecurity. Many states opted for their own definition of cybersecurity (Australia, France, Germany etc.). However, we chose to use EU's definition of cybersecurity because it is more comprehensible:

> "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[9]

Another important term is cyberspace. Tallinn Manual 2.0 defines the cyberspace as:

> "the environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks."[10]

As is the case with other topics – such as climate change, the domain of cybersecurity cannot be tackled only by states and a multilateral approach should be encouraged in order to offer a coherent response to these problems. In the Euro-Atlantic space, along with centres from different universities, a few international bodies or organizations have been very active in

[8] This problem has also been mentioned here: Trimintzios, P., Chatzichristos, G. *et al.* "Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU", European Parliamentary Research Service, Study EPRS/STOA/SER/16/214N p. 11 http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf (02.12.2018).
[9] NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, Resources https://ccdcoe.org/cyber-definitions.html (01.12.2018).
[10] *Ibid.*

analysing the subject of cybersecurity: United Nations (UN), NATO, Council of Europe and EU are the main actors involved offering information to the citizens about what is happening in the cyber space. We think it is useful to also offer an overview of what is happening at the international level in cyberspace. That is because most actions taken by states at regional and national levels should also apply the principles and norms agreed on at the international level.

UN, through its agency International Telecommunication Union (ITU) launched in 2007 the ITU Global Cybersecurity Agenda – a framework aiming to encourage countries' cooperation in the information society. The Agenda is based on five pillars:

1. Legal measures;
2. Technical and procedural measures;
3. Organizational structures;
4. Capacity building;
5. International cooperation[11].

The agency also collects data for the Global Cybersecurity Index which measures how states are prepared to respond to cybersecurity threats. The latest edition of the Index is from 2017 and found that the highest-ranking countries in Europe are Estonia, France and Norway[12] with Georgia and the Russian Federation ranking first and second in the CIS[13]. At the Global level, the most active countries in fighting cyber threats are Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada (Russia ranked 11th)[14]. The Index also found that almost half of the world countries did not prepare a national response to cyber threats. It is not difficult to understand why European countries the ones are leading the pack – in April 2007 Estonia became one of the first and most well-known victims of cyber-attacks in history.

Following into the steps of UN, NATO stressed the increased role of cyber threats in the early 2000s. Between 2002, when the topic of cybersecurity first emerged on NATO's

[11] International Telecommunication Union, „Global Cybersecurity Agenda (GCA)", https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (01.12.2018).
[12] International Telecommunication Union, „Global Cybersecurity Index (GCI) 2017", p. 36 https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (01.12.2018).
[13] *Ibid.*, p. 34.
[14] UN News, "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports" (5 July 2017) https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports (01.12.2018).

agenda at Prague Summit and 2018 at Brussels Summit 2018, the alliance took several measures that tackled the problems related to cyberspace. At NATO's Wales Summit in September 2014 and NATO's Warsaw Summit in 2016 member states decided to deepen their cooperation on cyber defence. At Wales Summit a new policy and action plan were presented and supported by the member states and in February 2017 the Alliance decided that cyber defence is part of the collective defence and that international law should also cover this area. At Warsaw Summit, the member states agreed that they should consider cyberspace one of the areas in which they should defend themselves just as they do in the air, on land and at sea[15]. The alliance has a few Centres that work in fields related to cybersecurity such as:

- NATO Computer Incident Response Capability (NCIRC) based at SHAPE, Mons, Belgium;

- NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia;

- NATO Communications and Information Systems School (NCISS) in Latina, Italy provides training to personnel from Allied (as well as non-NATO) nations (soon to the relocated in Portugal;

- NATO School in Oberammergau, Germany which works in fields related to education, and training to support Alliance operations, strategy, policy, doctrine and procedures.

- NATO Defense College in Rome, Italy emphasise the importance of research in strategic thinking[16].

After the illegal annexation of Crimea, the European countries and NATO countries became more worried about the cyber topic. That is why after the Wales Summit, NATO decided to create the Trust Fund on Cyber Defence for Ukraine. Again, an Eastern Europe country had been the target of cyber-attacks and used to test different instruments of cyberwar. This is one of the six funds created for Ukraine. In December 2014 the Fund is declared operational and works to provide Ukraine with the defensive capabilities in order to respond to different cybersecurity threats. Romania strongly supports the NATO Industry Cyber

[15] NATO, Cyber defence https://www.nato.int/cps/en/natohq/topics_78170.htm (01.12.2018).
[16] *Ibid.*

Partnership and is the lead nation in NATO Trust Fund on cyber defence for Ukraine, through the Romanian Intelligence Service[17].

Council of Europe

In 2001, Council of Europe initiated what had become the Council of Europe Convention on Cybercrime, or the Budapest Convention on Cybercrime, the first international treaty aimed to increase cooperation between national governments in order to respond to cyber threats. This step makes the Council one of the strongest bodies in the world that has expertise in this field. The Project PGG 2018: Cybercrime@EAP is a joint initiative of European Union and Council of Europe Partnership for Good Governance in the Eastern Partnership region, implemented in all EaP member countries. The project aims to strengthen their capacity to respond to cybercrimes such as theft of personal data, or fraud[18]. This comes to strengthen the societies' capacity to respond to these new threats in economic (the increased access to the internet for the citizens of these countries as well as the boost in online shopping) and political areas (attacks on public institutions). Because the economies of these countries are also growing and becoming more complex, they also need to respond to different problems and possible attacks including form different state actors, as was the case for Ukraine. Therefore, this project increases the resilience of these countries.

The Role of the European Union

As we have seen, European Union cooperates with NATO and Council of Europe in order to respond to different cyber threats. As the aim of the paper is not to present an in-depth analysis of these relations, we will only briefly present the main dimensions followed by EU in this area and the most important actions that took place in the last years regarding cybersecurity. Probably, the most effective official step was the fact that EU adopted in 2013 a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace guide by the main idea

[17] NATO, „Ukraine Cyber Defence" https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf (22.08.2018).
[18] Council of Europe, „PGG 2018: Cybercrime@EAP – International and public/private cooperation" https://www.coe.int/en/web/cybercrime/cybercrime-eap-2018 (02.12.2018).

that principles followed offline should also guide action online[19]. This framework helps boost the activities in the EU countries that have not yet developed a very comprehensive approach to cybersecurity and in the same time ensures certain coordination between different national procedures.

However, in terms of content exchange and cooperation, EU has its strongest partner in NATO. In July 2016 the EU-NATO joint declaration stressed the fact that it was necessary for both entities to cooperate in order to respond more efficiently to the "the unprecedented challenges emanating from the South and East"[20] in order to ensure their citizens' security. This shows that North America and Europe are the frontrunners in problems of cyberspace – NATO as the strongest defensive alliance and EU as the biggest single market in the world this is also because they have the capacities – human and financial to respond to these problems.

Cybersecurity is likewise one of PESCO's dimensions. Initiated in December 2017, PESCO is EU's latest try to develop closer cooperation in defense and security areas. During 2018, the Council adopted more projects in the area of cyber defense. The updated list of PESCO projects funded seven initiatives for cybersecurity and C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance)[21]. This step will offer the member states that decided to join in, the possibility to better coordinate their efforts in this domain, in which no state can work alone.

Further, different subnational actors are active in Europe in the area of cyber research. For example, The European Centre of Excellence for Countering Hybrid Threats launched in April 2017 is a think tank that works to provide the member states with the tools to understand better cyber threats and to respond more effectively to them. Currently, the Centre has 19 members – and is open for membership to EU and NATO countries[22].

---

[19] European Commission (2013),"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (02.12.2018).
[20] European Council (2016). „Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg"https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf (02.12.2018).
[21] European Council (2018). „Defence cooperation: Council launches 17 new PESCO projects", pp. 8-10, https://www.consilium.europa.eu/media/37315/table-pesco-projects-updated.pdf (02.12.2018). PESCO https://pesco.europa.eu/ (02.12.2018).
[22] Council of Europe, Hybrid CoE, „What is Hybrid CoE?" https://www.hybridcoe.fi/what-is-hybridcoe/ (04.12.2018).

Another initiative is *e-Governance Academy* a think tank based in Estonia, found in their National Cyber Security Index 2018 that five European countries France, Germany Estonia Slovakia and Finland ranked first in the world in terms of capacities to respond to cyber threats and good practices in this area[23]. The fact that the most well-prepared countries to respond to cyber threats are from Europe, confirms how important this topic is in Europe, but also that these countries were or are more prone to be victims of a cyber-attack. Ukraine experienced many of the instruments of this type of confrontation from little green man to cyber-attacks. In December 2015, a power grid cyberattack that affected 225,000 people took place in Ukraine. This is considered the first successful attack on utilities[24] or critical infrastructure[25]. Other incidents followed in Ukraine, which linked the country to the set of different activities that can be considered part of a *hybrid war,* as we mentioned in the beginning of the article.

By using different methods – including the fact that rather a state actor can have the resources to support this type of behavior - most of the experts and researchers that work in this field consider Russia as the main suspect behind these operations, an activity that has started in 1986 before the end of the Cold War[26]. The authors argue that after using these methods in domestic politics, Russia is now exporting them to the international arena. This means that Russia has the experience, resources and willingness to continue to engage in these projects. However, Russia is very active at global level in talks about regulating the cyber space and has proposed together with China and some Central Asia countries an "international code of conduct for information security"[27]. As long as the countries negotiated and debate different

[23] Rikk, Raul (2018). „National Cyber Security Index 2018" e-Governance Academy, https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (02.12.2018).
[24] BBC News, "Hackers behind Ukraine power cuts, says US report"(26.02.2016) https://www.bbc.com/news/technology-35667989 (03.12.2018).
[25] Trimintzios, P., Chatzichristos, G. et al. "Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU", European Parliamentary Research Service, Study EPRS/STOA/SER/16/214N pp. 41-2 http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf (02.12.2018). Department of Homeland Security, US-CERT, „Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure" (25.02.2016) https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (04.12.2018).
[26] Popescu, Nicu. Secrieru, Stanislav. „Introduction: Russia's cyber prowess – where, how and what for?" in Popescu, Nicu. Secrieru, Stanislav (ed.) (2018). Hacks, leaks and disruptions.Russian cyber strategies Chaillot papers no 148, Eurorean Union Istitute for Security Studies, pp. 6-7, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (10.12.2018).
[27] Capacity-building and confidence-building are also presented here: United Nations, (2015). „Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the

tools to respond to these 21st-century threats there is a chance to also increase transparency and confidence between participants. However, more debates are needed in this field.

As a complementary dimension for what is happening in the cyberspace, but not with a meaning as strong as cyberwar is the concept of *LikeWar* [28]. This type of activity is related to the huge rise of social media and how citizens' attention has become the new battlefield for different parties that aim to influence decisions and behaviours all over the world. Everyone who has an account on social media can become a target for a group that wants to influence his or her opinion. In this type of war, information is not censored or forbid but it is distorted in a kind of *smoke&mirrors* approach. Everything is mixed and presented in an ambiguous way, by anonymous with the aim to misguide and confuse the public. Singer and Emerson consider Russia to be the country that developed this kind of behaviour, in order to compensate for its declining military power[29]. Of course, Russia is not the only country with this kind of behaviour, but the fact that it was once *very* important, a superpower and today is just a great power strengthens this argument – it has more reasons to behave in this way.

Conclusions

At the global level, states – including European ones – were rather unprepared to respond in a fast and coherent manner to the evolution of the cyber area. Due to the fact that with the spread of internet access – made possible including by a decrease of price services – the cyber sector started to attract different types of actors and interests. This made viable the speed up process in deciding how to deal with the cyber domain and the cyber threats to state's security. The actors involved in defining and answering to different cyber threats are first the states and international organizations and on the second place, private non-state actors such as multinational companies, whose activity is taking place mostly online (as a matter of fact more

Context of International Security A/70/174", https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf (05.12.2018).

[28] Singer P. W. Brooking, Emerson T. (2018). „What Clausewitz Can Teach Us About War on Social Media Military Tactics in the Age of Facebook", *Foreign Affairs*, October 4, 2018, https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media (04.12.2018). See also: https://www.likewarbook.com/.

[29] *Ibid.*

and more of the companies) and citizens. One of the main problems in cyber-related incidents is the fact that is very difficult to have the proofs linking to the aggressors.

Recommendations

Because in May 2019 we will have new elections for the European Parliament probably there will increase the number of incidents in the cyberspace and will decrease the attention and resources for other regions of the world. Therefore, using the current resources in an efficient way is indeed necessary. The further recommendations are not unique and overlap with other points of view mentioned in different documents. However, we will also propose specific steps for countries in Eastern Europe. First of all, there needs to be a clearer understanding of terms – what do we mean when we discuss these terms – but keep in mind the differences between countries because these attacks use each state's vulnerabilities[30]. Then it is important to increase capacity-building starting with providing the relevant legal framework and continuing with learning technical skills in order to expand the possible counter-measures against different attacks. Another step can be confidence-building including between partners and avoiding duplicating the activities[31]. Cooperation and confidence- building can be developed by organizing workshops, seminars, exercises, stimulations and debates with different experts from countries affected by cyber threats and from states with a more advanced set of regulations and capabilities in this sector.

In order to enhance cybersecurity, states should keep in mind that they are the most responsible and legitimate actors to take actions and at the same time address the role of citizens in this mechanism. In the same time, it is necessary to educate the average citizens about the possible dangers and pitfalls of cyberspace in through different communication campaigns.

[30] Hagelstam, Axel. Narinen, Kirsti (2018). „Cooperating to counter hybrid threats" (23.11.2018), *NATO Review* https://www.nato.int/docu/review/2018/also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm (04.12.2018).

[31] Capacity-building and confidence-building are also presented here: United Nations, (2015). „Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174", http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (05.12.2018).

Bibliography

BBC News, "Hackers behind Ukraine power cuts, says US report"(26.02.2016) https://www.bbc.com/news/technology-35667989.
BBC News, „Ukraine power cut 'was cyber-attack' (11.01.2017) https://www.bbc.com/news/technology-38573074.
BBC News, „Black Friday shoppers 'spending less', (23.11.2018), https://www.bbc.com/news/business-46320551.
Council of Europe, „PGG 2018: Cybercrime@EAP – International and public/private cooperation", https://www.coe.int/en/web/cybercrime/cybercrime-eap-2018.
Concil of Europe, Hybrid CoE, „What is Hybrid CoE?" https://www.hybridcoe.fi/what-is-hybridcoe/.
Department of Homeland Security, US-CERT „Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure (25.02.2016)" https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
European Commission (2013),"Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
European Council (2016). „Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg"https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf.
European Council (2018). „Defence cooperation: Council launches 17 new PESCO projects", https://www.consilium.europa.eu/media/37315/table-pesco-projects-updated.pdf (02.12.2018). PESCO https://pesco.europa.eu/.
Hagelstam, Axel. Narinen, Kirsti (2018). „Cooperating to counter hybrid threats" (23.11.2018), *NATO Review* https://www.nato.int/docu/review/2018/also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm.
Hoffman, Frank G. (2009). „Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict", Strategic Forum no. 240, April 2009 https://s3.amazonaws.com/academia.edu.documents/43436887/SF240.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1546541148&Signature=lCeozZcSQruZfCvYSehv%2BSvvhrc%3D&response-content-disposition=inline%3B%20filename%3DHybrid_Threats_Reconceptualizing_the_Evo.pdf
International Telecommunication Union, Global Cybersecurity Agenda (GCA) https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.
International Telecommunication Union, „Global Cybersecurity Index (GCI) 2017", https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf.
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, Resources https://ccdcoe.org/cyber-definitions.html.
NATO, Cyber defence https://www.nato.int/cps/en/natohq/topics_78170.htm.
NATO, „Ukraine Cyber Defence" https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf.

Popescu, Nicu. Secrieru, Stanislav. (2018) „Introduction: Russia's cyber prowess – where, how and what for?" in Popescu, Nicu. Secrieru, Stanislav (ed.) „Hacks, leaks and disruptions.Russian cyber strategies", Chaillot papers no 148, Eurorean Union Istitute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.
Pawlak, Patryk (2017). „Countering hybrid threats: EU-NATO cooperation", European Parliament, European Parliamentary Research Service, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf.
Pawlak Patryk (2018). „Operational Guidance for the EU's international cooperation on cyber capacity building" European Union Institute for Security Studies, Luxembourg: Publications Office of the European Union https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.
Radio Free Europe Radio Liberty https://www.rferl.org/.
Rikk, Raul (2018). „National Cyber Security Index 2018" e-Governance Academy, https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf.
Trimintzios Panagiotis, Chatzichristos Georgios, Portesi Silvia, Drogkaris Prokopios, Palkmets Lauri, Liveri Dimitra and Andrea Dufkova. (2017), "Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU", European Parliamentary Research Service, Study EPRS/STOA/SER/16/214N, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf.
UN News, "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports" (5 July 2017) https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports.
United Nations, (2015). „Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174", https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf.
World Bank, „The World Bank Individuals using the Internet (% of population) Ukraine" https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=UA.
Thomas, Lauren. „Black Friday pulled in a record $6.22 billion in online sales: Adobe Analytics"(28.11.2018), *CNBC* https://www.cnbc.com/2018/11/24/black-friday-pulled-in-a-record-6point22-billion-in-online-sales-adobe.html.
Singer P. W. Brooking, Emerson T. (2018). „What Clausewitz Can Teach Us About War on Social Media Military Tactics in the Age of Facebook", *Foreign Affairs*, October 4, 2018, https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media.
https://www.likewarbook.com/.
http://www.ocsc.com.au/.
https://www.oxfordmartin.ox.ac.uk/cybersecurity.
https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front.

Bucharest, Romania

2019

www.esga.ro

Diaconu Coresi Str., nr. 53, Bucharest, Romania
Web: www.esga.ro, E-mail: contact@esga.ro