CYBERSECURITY IN THE EUROPEAN UNION

Andreas Düll, Anja Schoch and Matthias Straub[1]

DOI: 10.24989/ocg.v331.26

Abstract
The coordinated Denial of Service attacks in Estonia 2007, the successful hacker attacks against the German Bundestag 2015 and the increasing number of cyber-crimes challenge the European Union (EU). In order to overcome these challenges the EU initiated a cyber security strategy in 2013. This paper follows up the question, whether the measures of this strategy are adequate in order to tackle the challenges of the cyberspace in modern times and which improvements can be done. The focus will rely on the analysis of the EU's cyber security strategy 2013 as well as its advancement of 2017. The three issues 'cyber resilience', 'reducing cybercrime' and 'cyber defence policy and capabilities' shall be analyzed. The unlimited sphere of the cyberspace, the invisible and barely identifiable opponents and the focus on national regulations seem to be an unsolved dilemma in the EU. After analyzing the current state, the paper shall formulate future recommendations for action to postulate an improved 'pooling and sharing' as well as the coordination and involvement of existing member states' cyber capabilities. The devolution of responsibilities regarding cyber security to the EU stage is desirable in order to increase the European potency, because a divided EU will have great difficulties enforcing its interests over attacking opponents.

1. Introduction

Our world in its globalization process is in constant and ongoing change, which can lead to positive and negative outcomes. Never before has it been so easy to share knowledge and interact online on a global basis. Each smartphone owner in the EU produces and consumes data. The interconnectivity of Europeans grows constantly. Due to digitalization processes everything is more and more linked, from cars via military equipment over to power plants. This connectivity allows a fast and excessive exchange of data, leading to a higher living standard and prosperous economy. However, the growing amount of digital information transactions and the transformation of the virtual world not only lead to more options but to more challenges worldwide. [1] The coordinated Denial of Service attacks in Estonia 2007, the successful hacker attacks against the German Bundestag 2015 and the increasing number of cyber-crimes, challenge the European Union (EU). Due to the growing cyber-threat within the EU member states the European Commission was determined to outline a Cybersecurity Strategy (CSS) in 2013 with the main objective to guarantee the values, norms and principles of the EU on an online level. These premises also maintain in the updated version of 2017. Considering the cyber-threats this paper follows up the question, whether the measures of the CSS are adequate in order to tackle the challenges of the cyberspace in the 21th century and which improvements can be done. Therefore the CSS`s three main focuses, 'cyber resilience', 'reducing cybercrime' and 'cyber defence policy and capabilities' shall be analyzed. After dissecting the strategy regarding the immanent cyber-threats, the paper shall formulate future recommendations for action to increase the European repercussiveness.

[1] Andrássy University Budapest, Pollack Mihály tér 3, H-1088 Budapest; duell.andreas@gmail.com/ anja_schoch@web.de/ matt-straub@gmx.de

2. European Measures and Challenges

The EU's most issued discrepancy is to grant fundamental rights of expression and participation of individuals and countries on one side and at the same time to ensure national security. The combination of protecting states, businesses and citizens without invading into their freedom of rights is the most grievous defiance of cybersecurity on EU level. [2] In order to provide security without violating the freedom of rights, the EU focuses on a defensive alignment in its CSS and waives offensive measures as "hack backs" against cyber-aggressors.

In the following section the measures and goals of the European CSS regarding the cyber defence policy and capability shall be outlined. In another step the question whether the European measures are sufficient to tackle the most important challenges of cyber-threats shall be answered.

2.1. Cyber Resilience

Potential targets of hybrid attacks are the vital functions of a state. These include the economy, precisely those sectors where dependencies exist, the information and communication systems, in particular the cyberspace and the critical infrastructures in the field of finance, energy, health and logistics. Thus, the question of whether one's own systems and structures are sufficiently adaptable and resistant is becoming increasingly important for all states. The security and full availability of critical infrastructures such as water and energy supply is not only a precondition for prosperity, but for life and survival at all. [3]

In the security discourse, resilience refers to societies and political systems. Resilience is therefore the ability of a community or society to cope, adapt, and recover dangers to which it is exposed and its consequences in a timely and effective manner, thus preserving or rapidly restoring vital basic structures and basic functions. This means that resilience must be constantly maintained and re-acquired. [3] In the EU cybersecurity is taken as a cross-sectional task, both in terms of content and institution, and lies at the interface of civil and military cooperation as well as internal and external security, especially in times of crisis. [4]

The European Commission published a report evaluating the European Network and Information Security Agency (ENISA) and a proposal for a regulation establishing an enlarged EU cybersecurity agency. [5] The mandate of ENISA under Regulation (EU) 526/2010 expires on 19.06.2020. [6] In particular, ENISA assists member states in implementing NIS-Directive (EU) 2016/1148 [7] on measures to ensure a high common level of security of network and information systems in the Union. The evaluation identified the resource shortage of ENISA as a key challenge. For effective coordination of the various actors in the EU, ENISA should therefore be developed into an enlarged EU cybersecurity agency with a permanent mandate, a future 125 staff and an annual budget of around € 23 million. [8] In addition, the Commission proposed the introduction of a European cyber security certification system for digital products and services. In doing so, uniform quality labels comparable to the labeling of foodstuffs should contribute to the trustworthiness and safety of consumers. However, according to the Commission's proposal these should initially be distributed only on a voluntary basis. [5] Furthermore the aim is to develop a cybersecurity crisis response mechanism. This should be regularly tested in the form of cyber and crisis management exercises in the member states. In addition, a European cyber security research and competence center will be established to support the development and use of cyber-defence technologies. A pilot center is to be built in 2018. [9] Finally, a Cyber Security Emergency Fund will be set up in the future to support those member states that have properly implemented all

cybersecurity measures required by EU law. The emergency response could be made available to the affected member states similar to the EU Civil Protection Mechanism. [10] However, the Commission's proposals appear vague and sometimes less substantive. The following problems can be identified against this background: In recent years it has become increasingly clear that radically decentralized structures and voluntary cooperation are insufficient to effectively protect critical infrastructure against cyberattacks. Cybersecurity is increasingly understood as a public good that can only be guaranteed through binding legislation. In order to strike a balance between decentralized multi-stakeholder approaches and effective legal protection, a precision of the understanding of resilience would have been required. The Commission's strategy does not contain any comprehensible criteria that could shed light on which instruments should be used in which scenarios and why. There is a risk that member states, under the guise of the new CSS, could hide negligence on their national responsibilities, on domestic coordination and on the provision of financial resources. [11]

While the General Affairs Council, in its November 2017 conclusions on improving cybersecurity in Europe [12] welcomed the Commission's proposals, it also pointed out that the main responsibility remained with the member states. The Council only assigned a coordinating role to the European level and emphasized the need for the complementarity of EU action. This shows that the Commission has indeed given promising ideas in its strategy, but without possessing the relevant competences in the appropriate fields, it is to be feared that the member states will only take note of the ideas without working substantially on needed reforms.

Moreover, institutional fragmentation in cybersecurity still appears to be an unsolved problem. The upgrading and expansion of ENISA's role can contribute to the improved standardization and security of the cyber infrastructure. Nevertheless, the EU is still a long way from bundling all the measures in a single cybersecurity agency: So far, even the role of ENISA vis-à-vis national cyber security agencies in the member states has not been sufficiently clarified. In this context, institutional fragmentation also means that staff and financial resources are not yet sufficiently bundled. In particular, given that IT professionals are difficult to recruit, especially for the public sector, it is crucial for cyber resilience that all member states also provide the proposed measures with sufficient funding, including the financing of the new network of excellence. [11]

Furthermore, the legal harmonization, which would be essential for increased resilience to cyberattacks, is still awaited. [11] The stricter certification of IT products and the verification of the private sector by ENISA are in themselves very useful and important. These measures continue to be based on the principle of voluntariness. This leaves major structural hurdles in the provision and reporting of cyber-attacks. However, with NIS Directive (EU) 2016/1148, significant progress has been made in requiring critical infrastructure providers and operators, such as banks, power plants, hospitals, water or the Internet, to adopt cybersecurity reforms and related investments. In addition, member states are now obliged to set up national reporting systems. [7] The proposal by the Commission to introduce product certification only on a voluntary basis does not appear to be effective in this context. This could undermine the NIS policy and make new threats easy to play due to the lack of legal liability.

2.2. Reducing cybercrime

The increasing information and communication technology, the expanded use of the internet, the ability of using mobile devices have not only led to benefits but to an increasing vulnerability within the European member states. [13] [10]

Referring to the CSS of 2013 "cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target." [10] It includes 'traditional' violations as fraud or identity theft, content-related offenses such as child pornography or racial hatred and attacks towards computers or information systems. Cybercrime activities as stealing critical data, economic espionage or hacking into state-owned information systems became a new threat to all governments and economies worldwide. [10] According to the Center for Strategic and International Studies (2014) cybercrime is stated as one of the top four economic crimes worldwide. [14] In recent years these activities enlarged and are now a growing and profitable industry. [1] Trends flourishing this new industry result from crimes of terrorist actors, ransomware, banking and data gains, fraud, manipulation of payments and virtual currencies. [15] With this in mind it seems impossible to ensure the needed security level in the private and public sector. Member states still play the most important role in maintaining national security and protecting individual rights, but to fight cybercrime they cannot act effectively alone. Therefore the importance of cooperation is unavoidable. [13] [1]

As the CSS states cybercrimes are increasingly dangerous because they result in high profits and mostly have low risks, therefore "cybercrime is a growth industry" [14] which makes it very attractive to use for threatening infrastructure, government institutions or individual data security. The sources of activities mostly result from criminal, politically motivated, terroristic or state-sponsored attacks and focus on vulnerable harming in knowledge societies. [15] Invisible and barely identifiable enemies are becoming more and more dangerous and raise the difficulties of back tracing. [16] [10] The European Cybercrime Centre (EC3) provided an update (2016) on recent threats resulting from cybercrime incidents and the Internet Organized Crime Threat Assessment (IOCTA) highlights the biggest concerns being ransomware, information-stealing malware and banking trojans for EU law enforcement. Cryptocurrencies like Bitcoin have been the main choice to use for cybercrime activities and services. Furthermore increasing attacks against information systems or phishing campaigns can be reported by EU member states, aiming high value targets as key threat against law enforcement and the private sector. Incidents like the Stuxnet worm, Flame or the Distributed Denial-of-Service (DDoS) attacks against several Estonian national websites show that critical infrastructure can be targeted by viruses and valuable information can be collected. In recent years a large number of malware infections within air-gapped control system networks, combined with the exploitation of zero-day or security vulnerabilities in software programs, got reported across Europe. [17]

The main challenges within the EU are the division of tasks between civil defence, military defence and police, the defence against cyberattacks on critical infrastructures, the quantitative detection of security threats and how deep state security measures can interfere with individual freedom. [15] As one of the main priorities the CSS states the drastic reduction of cybercrime, since there is a high need for the right tools to tackle cybercrime actors and networks. In order to reduce cybercrime the EU suggests a strong and effective legislation in the EU member states, therefore the Budapest Convention[2] as a binding international treaty evolved as a framework for the adoption of guidelines on national level. Since not all member states have the same abilities to tackle cybercrime with effective response, the EU suggests national units as a necessity. Supporting the member states, the European Commission identifies gaps and strengthens capabilities to investigate and combat cybercrime. Connections shall be drawn between the private sector, research institutions and law enforcement to share best practices, new techniques and policy approaches. To reduce cybercrime,

[2] The Budapest Convention of Cybercrime was opened for signature in 2001 and is the most important document on cybercrime and electronic evidence.

the EU has implemented the CSS to focus on legislation and support borderless cooperation. Actions are the facilitation of cross-border access to electronic evidence for criminal investigations and legislative activities. It provides analysis, helps with investigations, creates channels for information sharing and "serves as a voice for the law enforcement community" [10] for all relevant stakeholders fighting against cybercrime. [15] The European Police College (CEPOL) organizes e-learning and training courses in cooperation with Europol to standardize knowledge and set a framework for European exchange. [10] Eurojust intends to assist cooperation at the judicial level between legal systems of the EU member states and with third states.

Offline or online, the EU is willing to follow its core principles and values regarding the rule of law and fundamental rights. It is difficult to distinguish between transparency, awareness-raising, empowerment of individuals and tackling cybercrime acts. [2] [11] To analyze the effectiveness of the EU's policies regarding cybercrime the improvements of the 2017 renewed CSS, institutional settings and cooperation between member states on EU level shall be identified. Progress was made in the adoption of measures by the member states to combat sexual abuse and exploitation of children and child pornography with the amendment of criminal codes, procedures and sectoral legislation, coordination of national actors was able to improve. Interpol's International Child Sexual Exploitation (ICSE) database for illegal images is constantly expanding. The cooperation of member states became closer with the implementation of the Directive on Attacks against information systems and 14 additional states ratified the Budapest Convention since 2013. The EC3 became the focal point in the fight against cybercrime in which staff and resources rose. In cooperation with the EU member states' law enforcement difficult cases were able to be solved more easily. The so called *No More Ransom* project of the EC3 was adopted to raise awareness and enabled citizens to decrypt their ransomed devices for free. Furthermore the cooperation between Eurojust and Europol improved since 2013. [18]

The CSS has so far not been effectively enough in increasing online accountability due to lack of publicly available and accurate data on registrants of domain names which creates opportunities for criminals to hide their activities. Further remaining gaps are mostly in the establishment of prevention programs, infrastructure and investment. The number of child sexual abuse images and number of traffickers in child pornography have increased (81%), thus, more effective measures are required. The EC3 is a good approach for effective cooperation, monitoring and investigations; still it lacks staff and resources to be effectively in high-profile cases. [18]

2.3. Cyber Defence Policy and Capabilities

The CSS 2013, the advanced version of 2017 and the Reflection Paper on the Future of European Defence acknowledge that the vulnerability of the supply of essential services as healthcare and water has risen due to the interconnectedness of the cyberspace. Furthermore the EU stresses the fact, that foreign governments outside of the EU abuse cyberspace for surveillance and manipulation. In order to tackle the unintended as well as intendent threats to the European cybersecurity the CSS focuses on detection, response and recovery. It seeks to improve the "synergies between civilian and military approaches in protecting critical cyber assets". [10] The CSS 2013 also gives priority to the information exchange between the EU and the member states as well as the risk assessment, awareness raising and the establishment of the cybersecurity. In addition, the industry and academia shall be fostered in order to develop and coordinate new solutions to reduce the cyber threats. One of the most important measures of the CSS 2013 is the use of the "network of NIS competent authorities […] to share information and support. This would enable preservation and/or restoration of affected networks and services." [10] Besides that, the EU

mentions that “it is predominantly the task of member states to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance.” [10] In order to tackle the threat of cyber-attacks as efficient as possible the EU aims to avoid duplications and strains to strengthen the international cooperation within the EU-US Working group as well as NATO, OECD, UN and further international organizations. The CSS also seeks to deter cyberattacks. Consequently, a foreign cyber-attack could lead to the invocation of the EU Solidarity Clause, Article 222 of the Treaty on the Functioning of the EU. [10]

The CSS 2017 refines the previous CSS and strengthens the deterrence approach. Thus, in the case of a cyber-attack the public authorities are supposed to response fast and effective in order to build confidence in the ability to avert a cyber-attack. A deterrence comprises a successful attribution, i.e. the detection of a cyber-attack as well as the assignment of it to the aggressor. Therefore, the CSS 2017 aims to improve the attribution of a cyber-attack with the implementation of IPv6, which shall allow an improved identification of a single user and raise the likelihood to detect the aggressor. The effectiveness of IPv6 is, however, doubtful, because despite of a wholesale adoption of IPv6 potential aggressor still would be able to use anonymous proxy servers or TOR browsers to obscure their attacks. Moreover, a cross-border cooperation within the EU as well as the establishment of an electronic platform to exchange information will accelerate the attribution. In order to tackle the fast-evolving cyber threats the CSS also claims the need for an efficiently functioning Computer Emergency Response Team. Therefore an EU Cyber Capacity Building Network will have to be established, which comprises the EEAS, member states‘ cyber authorities, EU agencies, Commission services, academia and civil society. Another aim of the EU is to strengthen the CSDP’s ability to tackle cyber threats within the framework of PESCO and the EDF. Apart from that, the CSS 2017 also refers to the Reflection Paper on the Future of European Defence. [19] The Reflection paper contains three possible kinds of defence integration between the member states. The first kind of integration comprises an exchange of information on cyber-threats and attacks, the second one aims at a stronger cooperation and the third one seeks a better coordination on cybersecurity within the member states. [20]

There are several challenges to the maintenance and development of European cyber security, which are mainly addressed by the CSS. The most important challenge of cyber-threat is the attribution of attacks. There are further challenges like the protection of less protected critical infrastructure on the municipal stage. These challenges shall not be outlined, as the CSS mainly concentrates on deterrence. An important condition for a credible deterrence is to detect and attribute the aggressor. Without an attribution the enforcement of laws or regulations would be unrealistic. [21] The attribution problem can be outlined in an attack against the Iranian nuclear enrichment facilities in Natanz, which has suffered the what is probably the most harmful cyber-attack by the malware Stuxnet. [22] At first the Iranian scientist assumed that the incident was an accident. After several weeks the accident was declared as a cyber-attack. By now it is not clear whether the USA or Israel was the aggressor. This example shows, how problematic a proper and fast attribution is. The detection of a cyber-attack takes averagely 150 – 200 days, the attribution itself can take months or even years. An exact attribution requires more information and time, than a less accurate attribution. The right for self defence according the UN Charta Article 51, however, demands an immediate reaction. Considering the long timeframe of the attribution the delayed retaliation measure could be seen as a new aggression. Otherwise a fast and less accurate attribution could lead to take measures against the wrong state, which could lead to a political escalation. [23] Hereby it is also noteworthy, that the complexity of attribution ease false flag attacks. [21] Thus, a credible deterrence requires a fast and proper attribution. Therefore the European decision to implement IPv6 is the right step to improve the ability to attribute, but it is also necessary to set up

– as the EU also intends – a platform, which fosters data exchange on cyber-threat incidents. This platform should seek to provide the actors with data mining techniques and statistical analysis. These elements could deliver further information about the aggressor, which raise the degree of certainty. Yet, the positive effects of an information exchange, which was prioritized by the CSS 2013, could be diminished by several problems. Firstly, if a member state shares its information about a cyber aggressor, other member states will also postulate further information about the way how data was collected and who received it. The receiving member state requires this accurate information in order to ensure an exact attribution, but it is very unlikely that the sharing member state will provide all these information. [21] Thus, the European member states do not receive all required information in order to establish an EU-wide security network as well as grant an effective attribution. [4] Secondly, a contextual understanding of the shared data is necessary. The gathered information is only useful, if the cyber intelligence experts of a member states are sufficient trained to interpret the information as well as the linked digital forensic traits and geo-political factors. Finally, it is very expensive to take part in the information gathering. It requires new hardware, software and training of new processes. [21] Considering the hard- and software‘s life cycle of two to three years, the public sector will always have to be always up to date in order to guarantee a successful attribution and deterrence. That means, that the current life cycle of public procured devices of five to ten years will have to be reduced. [24]

Unfortunately the EU neither stresses these problems nor suggests possible concrete solutions to it. That is why, some recommendations shall be proposed in the next section of this essay.

3. Recommendations for actions

Cyber resilience

The objectives of resilience should be defined more precisely: Is it 'just' about the ability to fend off attacks, endure and repair damage, or is there an additional need to build structures such as second strike capabilities or new forms of outer defense in order to already be able to reduce the occurrence of such attacks and damage? In this context, it would be useful for the Commission to devise a definition adapted to the real possibilities of action in form of an European White Paper on cyber resilience. With regard to the NIS Directive, which in principle goes in the ‘right’ direction, consideration should also be given to including digital SMEs and internet providers. This would mean that the definition of critical infrastructure would have to be revised. However, in view of the equally high vulnerability of smaller digital companies, they should also be required to provide security measures in the general interest. The certification of IT products should be legally binding, rather than voluntary, in order for the NIS Directive to be fully effective. In addition, a liability for hardware and software manufacturers should be considered. It should also be mentioned that the issues arising, such as the required protection profile and the scope of liability, should be discussed broadly and openly with all relevant stakeholders. The newly created certification and liability framework could put pressure on the world market by compelling non-EU manufacturers to implement European regulations in the context of market access. This in turn could lead to competitive advantages for European companies in a growing and sustainable industry. [11]

Cybercrime

Since cybercrime is crossing nations and effective law enforcement cannot be limited within state borders, the collaboration and cooperation between member states and the EU is essential to increase private and public safety “to make the EU's online environment the safest in the world.”

[10] To be highly effective in the reduction of cybercrime it is important to avoid institutional overlaps, focus on a clear distinction of resources and experts and ensure an appropriate investment in infrastructure and capacities. The EC3 shall remain the focal point in order to have a highly qualified contact institution for all member states in the field of prevention and investigation. The more trust of people and states in political processes of the EU are ensured, the more the system can be effective to combat cybercrime. The harmonization and qualification of tools, instruments and authorities is therefore essential. [13] To ensure the reduction of cybercrime in the EU, voluntary guidelines are not effective enough and it should be in the interest of all member states to cooperate and embed recommended guidelines into national law. To avoid monitoring incidents the cooperation of law enforcement regarding cybercrime reduction needs binding rules. Further needed is the increase in cooperation between Eurojust and Europol to identify challenges and possible solutions. [11] There have been proactive progresses in collaboration regarding the Budapest Convention. To make measures internationally more effective it would be progressive if additionally large countries as Russia, China or India would ratify the Convention. Supplementary the Budapest Convention, from 2001, needs to be modernized regarding today's needs. [25]

Cyber Defence Policy and Capabilities

The EU has to raise awareness for the problems linked to the attribution. The sharing of member states' experiences with the EU would be very helpful to identify cyber-attacks and to attribute them correctly. In the short term the EU could create incentives and financial support with the EDF in order to tackle the problems with the information sharing. [21] So, the task of the EDF could be expanded in order to support member states with a lower defence budget to afford the high expenses for hard- and software as well as the cyber-training program for intelligence staff. This would strengthen the cyber defence capability of every single member state and hence the defence capability of the EU. It would especially make it easier to gather information gathering and data analysis. Considering the importance of a comprehensive and profound information and data exchange, the EU should aim to build confidence between all member states' intelligence agencies and strengthen the interconnectivity of these agencies. In the long run it would be sensible to establish a well-equipped European center for cyber defence, which bundles all necessary competences and capabilities in order to fasten the attribution of broad cyberattacks and, in a second step, to avert them. Such a center would be especially auxiliary to defend small member states like the Baltics, which are not be able to defend themselves.

4. Conclusion

In summary, the European Commission, as part of its renewed CSS, has been fortunate enough to acknowledge that cybersecurity issues play an essential role in the security, freedom and prosperity of EU citizens in the 21st century. It is therefore to be welcomed when it is suggested to expand the public spending in education, training and cutting-edge research in order to be ready for the risks of the digital age. The expressed desire for increased European cooperation on cybercrime and cyber defence issues is urgently needed. On a positive note, the Commission recognizes that only a multidimensional approach involving business and civil society can ensure a sustainable balance between security and freedom. In a world that is becoming increasingly complicated, it is crucial for the future of Europe to speak with one voice on all crucial issues of internal and external security while making the most of the (digital) single market.

At the same time, however, this paper shows that the EU is still a long way from a system of standardized procedures, automatic data reconciliation and equivalent cyber resilience rules across

all member states. The national governments are still firmly in the grip of action in the central areas of foreign and security policy, on the one hand, and domestic and justice policy on the other. There is a risk that larger and economically more potent member states will work alone and strengthen their cyber resilience and cyber defence capabilities, while smaller and weaker member states lag behind. It must be remembered that the EU has a high degree of interdependence due to its single market and open borders, so risk assessment is never just about how well one's own country is set up, but about keeping the EU as a whole in mind. As a result, the EU is only as resilient as its least resilient member state.

In order for the Commission's efforts to be fruitful, the European treaties would need to be amended so that the ordinary legislative procedure is applied to CFSP and CSDP. Finally, the EU would be more than just a coordinating layer of diverse national regulations, and could indeed provide for a significantly increased level of cyber resilience, a more effective fight against cybercrime and a common cyber defence policy with substance.

5. References

[1] BARTH, J. D. / SCHLEGELMILCH, W.: Cyber Democracy: The Future of Democracy?, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber- Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice, Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 195-206.

[2] MITTERLEHNER, B.: Cyber-Democracy and Cybercrime: Two Sides of the Same Coin, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber-Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice. Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 207-230.

[3] TAMMINGA, O.: Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie, SWP-Aktuell 2015/A 92, November 2015, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2015A92_tga.pdf, 11/2015, p. 2f. (Accessed on January 14, 2018).

[4] BENDIEK, A.: Das neue >>Europa der Sicherheit<<. Elemente für ein europäisches Weißbuch zur Sicherheit und Verteidigung, in: SWP-Aktuell 2017/A 37, Berlin 2017, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2017A37_bdk.pdf, p. 5. (Accessed on February 2, 2018).

[5] EUROPEAN COMMISSION (2017): Proposal for a regulation – COM(2017) 477/947932

[6] EUROPEAN UNION: Regulation (EU) 2013/526

[7] EUROPEAN UNION: Directive (EU) 2016/1148

[8] EUROPEAN COMMISSION: Cybersecurity - EU Agency and Certification Framework, available online: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-eu-cybersecurity-agency-and-eu-framework-cybersecurity-certification, 2017. (Accessed on January 18, 2018).

[9] EUROPEAN COMMISSION: Commission Recommendation (EU) 2017/1584

[10] EUROPEAN COMMISSION: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

[11] BENDIEK, A./ BOSSONG, R./ SCHULZE, M.: Die erneuerte Strategie der EU zur Cybersicherheit. Halbherziger Fortschritt angesichts weitreichender Herausforderungen. SWP-Aktuell 2017/A 72, October 2017, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2017A72_bdk_etal.pdf, 2017, p. 2-4; 4f. (Accessed on January 08, 2018).

[12] COUNCIL OF THE EUROPEAN UNION: Draft Council conclusions on the Joint Communication to the EP and the Council: Resilience, Deterrence and defence: Building strong cybersecurity for the EU, 14435/17, available online: http://www.consilium.europa.eu/media/31666/st14435en17.pdf, 2017. (Accessed on January 21, 2018).

[13] PETRATOS, P.: Cybersecurity in Europe: Cooperation and Investment, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber-Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice, Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 279-302.

[14] CSIS- CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES: Net losses estimating the global cost of Cybercrime. Economic impact of cybercrime II, Report, available online: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf, 2014, p. 20. (Accessed on January 09, 2018).

[15] EUROPOL: The relentless growth of cybercrime, available online: https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime, 2016. (Accessed on January 09, 2018).

[16] BENDIEK, A.: Europäische Cybersicherheitspolitik. SWP-Studie, available online: https://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf, Berlin, 2012. (Accessed on January 12, 2018).

[17] EUROPOL IOCTA: Internet Organized Crime Threat Assessment, available online: www.europol.europa.eu, 2016, p. 7f.; 40. (Accessed on February 02, 2018).

[18] EUROPEAN COMMISSION: Commission Staff Working Document. Assessment of the EU 2013 Cybersecurity Strategy, available online: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF, 2017, p. 36-41. (Accessed on February 01, 2018).

[19] EUROPEAN COMMISSION: Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 2017, p. 12-14.

[20] EUROPEAN COMMISSION: Reflection Paper on the Future of European Defence, available online:https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf, Brussels, 2017, p.12-14. (Accessed on February 01, 2018).

[21] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE: Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks, Pihelgas M. (ed.), available online: https://ccdcoe.org/sites/default/files/multimedia/pdf/False-flag%20and%20no-flag%20-%2020052015.pdf, Tallinn, 2015, p. 8; 21. (Accessed on February 01, 2018).

[22] TABANSKY, L.: Cyber Security Challenges: The Israeli Water Sector Example, in: Clark, M. R./ Hakim, S. (ed.), Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level, Philadelphia, 2017, p. 205-221.

[23] REINHOLD, T. / SCHULZE, M.: Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von „hack backs“, in: SWP, available online: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf, Hamburg, 2017, p. 8f. (Accessed on February 02, 2018).

[24] MATTHEWS, E. D./ ARATA III, H. J./ HALE, B. L.: Cyber Situational Awareness, in: Connolly, C. (ed.), The Cyber Defence Review. A dynamic multidisciplinary dialogue, New York, 2016, p. 35-48.

[25] CHATHAM HOUSE: Building a Stronger International Legal Framework on Cybercrime https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime, 2017. (Accessed on February 01, 2018).