DOI: 10.62897/COS2023.1-1.31

SUSTAINABILITY OF ELECTION SECURITY FROM A MULTIDISCIPLINARY APPROACH

Roland Kelemen[a,*], Ádám Farkas[a], Richárd Németh[b]

[a]Széchenyi István University, Faculty of Law and Political Sciences, Győr, Hungary
[b]Széchenyi István University, Faculty of Mechanical Engineering, Informatics and Electrical Engineering, Győr, Hungary
kelemen.roland@ga.sze.hu

The study discusses the importance of election security in modern information age and its impact on democracy. It emphasizes that elections are crucial for democratic functioning, and any threats to their integrity undermine public confidence in the political system. With the increasing digitisation of the electoral process and the reliance on social media for election campaigns, the risks of interference and misinformation have escalated. The paper explores the relationship between national security and sustainability in today's security environment, highlighting the complexity and totality of security challenges. It argues that sustainability is essential to safeguard security interests in the long term, encompassing not only material aspects but also cognitive and societal resilience. The study delves into the cyber vulnerabilities of electoral systems, such as attacks on e-voting systems and attempts to manipulate related information. It underlines the importance of network and internet security in protecting election-related systems and data and also addresses the role of social media in spreading misinformation and disinformation during elections, as well as the need to enhance security awareness and resilience among the public and election officials. It presents EU and national legislation and practices in this area and then identifies areas where progress is needed in both regulation and best practice to achieve sustainability, based on these and on the experience of recent years.

1. Introduction

The election of members of the legislature is a cornerstone of democracy, a crucial opportunity for voters to participate, at least indirectly, in the political process and in shaping the laws that affect their lives and their everyday lives. The processes leading up to elections, the organisation and conduct of elections and the declaration and publication of results are, therefore, extremely sensitive points in the democratic functioning of a state. Maintaining a high level of public confidence in these systems is essential to ensure that the legitimacy of the branch of power, and ultimately of the entire attribute of state power, is beyond reproach in society. However, in the current geopolitical context of the information age, the threat to elections and attempts to influence them have been greatly enhanced.

In many countries today, the electoral process, or its certain elements, is being implemented digitally. In addition, the success of election campaigns is strongly linked to cyberspace, especially social media (Kwak et al., 2022). This has led to a renewed focus in recent years on interference by one party in the democratic processes of the other and, on the other hand, on more effective defences against attempts at influence and delegitimisation. Ensuring the sustainability of electoral legitimacy is an aspect that has a major impact on voters' faith and trust in democracy – a fact that is also highly vulnerable to misinformation, disinformation and fake news from cyberspace.

Election security can be approached from both a network security and a cognitive security perspective. Electronic voting systems are a part of critical government infrastructure. In recent years, many countries have experienced cyber-attacks on electoral information systems, with the perpetrators gaining access to large amounts of personal data. In addition to network security, the increasing number of foreign information operations over the past decade has posed a particular threat to the integrity of elections.

In this paper, we use the tools and scientific methods of military and legal science to investigate the links between sustainable security and electoral security. In doing so, it will examine how the transformed and totalising security environment of today’s military science experience and the high level of digitalisation of states and societies affect the security of elections. How election security can be segmented. It will also examine the regulatory and practical responses of individual states and the European Union to this issue. The lessons learned will be summarised and conclusions drawn on the areas where progress is needed to enable democratic states to achieve sustainability in the area of election security.

2. The relationship between national security and sustainability and election security in today’s security environment

The complexity of security is now a fundamental principle (Dannreuther, 2013) in thinking about the functioning of national and international communities. Security in its essence, can be interpreted in all areas of life, with its individual sectors. Beyond traditional military security and public security, if we take food security, economic security, transport security, energy security or information security as examples, it goes without saying that security permeates the functioning of our societies in both horizontal and vertical senses. From this perspective, security is not only complex but also totality in the 21st century, as are the dynamically changing challenges, as they can affect all aspects of life, are truly global and real-time, and can partly break away from spatial boundaries through technological development, especially cyberspace. The security medium is, if you like, ‘total’ because it has both horizontal – i.e. according to the multiplicity of types of challenges and threats – and vertical – i.e. according to the scope of each specific challenge/threat – extreme and partly unpredictable variability.

It also follows that sustainability has fundamental security linkages, as environmental change, consumer society’s exposure to different supply systems, economic stability and resources (Khanna, 2016) all bring with them the recognition that sustainability is a long-term strategic interest in safeguarding security. This insight is supported by work on the relationship between climate change and security (Moran, 2011) or resource-driven conflicts (Isaszegi, 2015), both in a specific military and broader geopolitical context (Dalby, 2020).

However, when it comes to security, we have a tendency to focus all our attention on the material links: the infrastructure, the services, and the resources. However, the problem of information warfare, disinformation and post-truth phenomena, as well as hybrid threats (Giannopoulos et al., 2021), have highlighted the need to strive for sustainability not only in material terms but also in cognitive, individual and societal psychological terms, in order to make our security sustainable. The human factor, and within it cognitive and mental resilience, is fundamental to the functioning of our societies and indeed to the safe operation of many of our technological systems, without which misinformation can create uncertainty that can have a significant impact on material security.

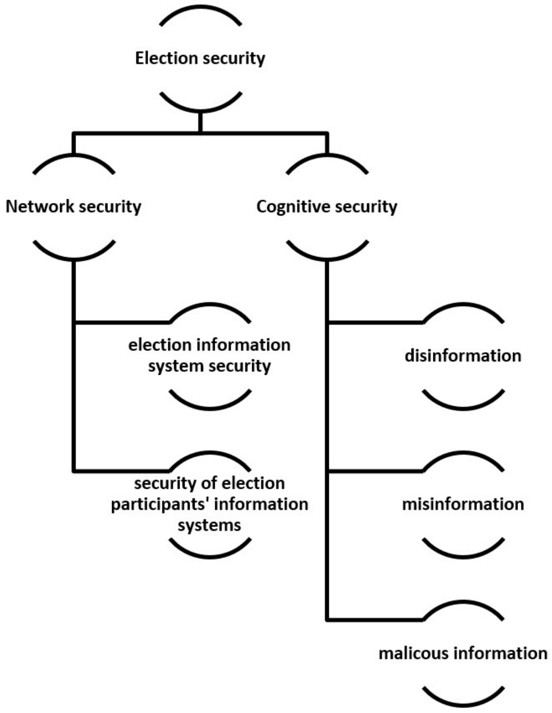
In the age of total security, therefore, sustainability is also understood in a complex way, and in this complexity, the reliability of information, our ability to process and control information, and our individual and societal cognitive resilience play a prominent role. Sustainability, if you like, is also a key issue for the functioning and culture of the information society and, therefore, for information security in a broader sense. The absence or dysfunction of these can result in security exposures that can lead to political-legitimacy disruptions and, in serious cases, to the erosion of physical security, for example, in the case of disinformation-based riots. In the age of total security, a political dimension must, therefore, be properly considered.

In 2015, the UN adopted the Framework for Sustainable Development, which states that “Sustainable development cannot be realised without peace and security” and thus includes peace among the sustainable development goals. To this end, the document argues that it is essential to reduce all forms of violence, support the rule of law and strengthen appropriate national institutions (Squillace et al., 2023). One such national institution is democratic elections, a pillar of the rule of law. In recent decades, however, with the proliferation of cyberspace and related technologies, this institution has come under attack from many sides. On the one hand, these attacks have targeted electronic systems associated with electoral processes, and on the other hand, they have attacked the integrity of democratic elections themselves.

The relationship between sustainable security and election security is rooted in the broader concept of ensuring the stability and well-being of a nation or community. Sustainable security focuses on long-term, comprehensive strategies that go beyond traditional military measures to safeguard a nation's interests. Election security, on the other hand, pertains to the protection of electoral processes and the integrity of democratic institutions during elections.

These two concepts intersect in several ways: (1) Democratic stability: Sustainable security relies on stable political systems. Secure and transparent elections are crucial for establishing and maintaining political stability, as legitimate leadership transitions reduce the risk of internal conflicts and violence. (2) Public trust: Sustainable security efforts benefit from a population that has trust in its government and political institutions. Ensuring election security by preventing fraud and interference fosters this trust, which is vital for national cohesion and resilience. (3) Foreign influence: Foreign interference in elections can undermine both election security and a nation's sustainable security. Hostile actors may seek to manipulate election outcomes to weaken a nation's stability, making it imperative to safeguard elections from external manipulation. (4) Rule of law: Sustainable security is closely tied to the rule of law, which includes the fair and equitable enforcement of electoral rules. Secure elections uphold the rule of law, bolstering a nation's legal and political systems. (5) Conflict Prevention: Secure elections reduce the risk of political disputes turning into violence. In this way, election security contributes to conflict prevention, a key aspect of sustainable security. (6) Resilience and adaptability: Sustainable security strategies must adapt to evolving threats and challenges. Election security also demands adaptability to address emerging threats like cyberattacks or disinformation campaigns, reflecting the shared need for resilience.

In summary, the relationship between sustainable security and election security is symbiotic. Secure and transparent elections support long-term national stability and well-being, while sustainable security strategies aim to create a conducive environment for such elections to take place. Both concepts are integral to maintaining a robust and resilient society.



Figire 1: Diagrammatic representation of electoral security

3. European Union and national practices and regulations on election security

In recent years, there have been a number of incidents involving electronic systems related to elections. For example, in autumn 2020, Iranian hackers attacked US election databases and gained access to large amounts of voter registration data, and actors close to the Chinese, Russian and Iranian governments significantly affected the security of US political organisations (JUSTICE.GOV, 2023). In Israel, the personal data of 6.5 million Israeli voters, virtually the entire eligible population, will have been exposed ahead of the 2021 general elections.

The security of election-related electronic systems is a priority for national security authorities in each country, as well as for the European Union. According to an annual cybersecurity report published by the security and counter-terrorism agency under the Ministry of Justice and Defence of the Netherlands, one of the main targets of cyber-attacks by states for geopolitical gain is attacks on systems that ensure the democratic process (NCTV, 2021).

The Cybersecurity & Infrastructure Security Agency (CISA), the main body responsible for election cybersecurity in the United States, classifies cyber threats relevant to elections into three groups: phishing, ransomware and distributed denial of service. To avoid these threats in the US, officials seeking to secure election infrastructure should carefully review each section to identify the tools and services that can address the primary risks. The services and tools used should all be consistent with the Protect and Detect functions of the NIST Cybersecurity Framework. Within this scope, Protect defines the precautions to ensure the provision of critical services and Detect defines the activities to identify when a cyber security event has occurred. (CISA, 2023a) In addition, election officials should have extensive oversight of technological, physical and procedural systems to reduce the likelihood of malicious cyber activity that could affect the integrity of the election, such as altering votes or otherwise disrupting or preventing voting. To this end, measures such as the use of provisional ballot papers and reserve ballot books are possible (CISA, 2023b).

In addition to the direct attack on electoral systems, a particular problem is the hacking of information systems of organisations or individuals involved in the election campaign and the extraction and leakage of data from these systems in order to influence the election results. Two of the most notorious of these are the cases of the presidential elections of Hillary Clinton and Emmanuel Macron. In these cases, the source of the threat was mainly inappropriate employee behaviour or inadequately designed data management rules and systems. Such cases make clear the need to develop the appropriate infrastructure and internal controls for such actors, in addition to awareness-raising activities tailored to their own organisations. (Tenove et al., 2018) Our surveys conducted during the COVID-19 pandemic showed that, in the case of Hungarian businesses, this type of preparedness was most prevalent among multinationals but that the cybersecurity awareness of employees was already highly contested among these actors. In the case of SMEs, however, it is clear that neither the business organisation nor the majority of employees had an adequate level of preparedness in these areas. What is also reflected in the 2022 Hungarian elections is that there were several data breaches of the organisations and their employees during the campaign period. (Németh, 2022)

The European Union's Regulation on restrictive measures against cyber-attacks that threaten the Union or its Member States includes attacks on public elections and the electoral process among those that threaten Member States. Accordingly, persons, entities and bodies to whom such attacks may be directed are subject to restrictive measures, including the freezing of their funds and economic resources (EU, 2019).

The network security of elections is based on a properly built, operated, monitored and improved information system and its well-functioning funding, as well as the training and preparation of election officials, but at least as important is the improvement of social resilience on the part of those involved in the election campaign, for whom it is necessary to develop and enhance security awareness, as all of these are essential to ensure the integrity of elections in the future.

Another interesting case of electoral security is cognitive security in elections, which also seeks to undermine the legitimacy of electoral institutions. Russia's actions against Ukraine have led the European Union to recognise the potential for the exposure of trust in the democratic functioning of Member States and EU institutions, mainly through Russian and Chinese disinformation scenarios. Therefore, in 2015, the East StratCom Task Force was set up to improve the EU's capabilities to anticipate, detect and respond to disinformation. In 2018, an action plan against misinformation was adopted. It provided for a split action between Member States and EU institutions. The coordinated response is based on four pillars: improving the capacity of EU institutions to detect, analyse and expose cases of misinformation; strengthening coordinated and joint responses to misinformation; mobilising the private sector to combat misinformation; raising awareness; and improving the resilience of society (EUROPA, 2018).

Some Member States have not been idle in this area. France has adopted a law to combat the spread of disinformation during election campaigns. The law allows the authorities to remove or block false information that could influence the electoral process and provides for transparency in the financing of online political advertising (Guillaume, 2019; Craufurd Smith, 2019). Spain adopted a law in 2018 aimed at protecting the electoral process from disinformation and interference. The law establishes measures to monitor and combat disinformation during electoral campaigns, focusing, among other things, on social media and online platforms. (Campos-Freire et. al., 2021) The Irish Elections (Amendment) Act 2021 focuses on political advertising and transparency. It requires online political advertisements to include information on who is responsible for the advertisement and whether it is a paid advertisement. (Kirk and Teeling, 2021; Lynch, 2020) Latvia introduced amendments to its Law on Electronic Mass Media in 2019 to address disinformation and the use of mass media for electoral interference. The aim is to regulate the publication of political advertising and funding sources (WIPO, 2023).

In December 2020, the European Commission presented an Action Plan for Democracy in Europe (EUROPA, 2020). The fourth point of the Action Plan is the fight against disinformation. It advocates closer cooperation with the private sector, civil society, academia and the EU's international partners, but still only to better understand hybridity. In other words, it is still just a promise to implement the code of conduct and develop a common methodological framework. In the case of the platforms, he criticised the opacity of the algorithms they use and their news practices, problems that were only identified during the evaluation of the Code of Conduct. The Commission believes that a stronger and clearer commitment from platform providers and an approach based on an appropriate monitoring mechanism are key to an effective fight against disinformation. The Commission remains of the view that one of the most important areas in the fight against disinformation is media literacy.

The Helsinki-based Hybrid Centre of Excellence has made recommendations to ensure smooth elections in 2020. It divided the pre-election period into three periods: beyond one year, within one year and within six months. One of the key tasks of the one-year period is to establish mechanisms for cooperation with other Member States, allowing best practices to be collected and integrated into the process. To this end, the European Union set up the Rapid Alert System in 2019 to facilitate the exchange of information and coordinate the action of Member States and EU institutions against disinformation. To this end, a network of twenty-seven national contact points has been set up to coordinate and share best practice. This division of responsibilities makes it difficult to solve problems, and the national toolbox remains (Makela, 2019). From a disinformation perspective, the last six months are still relevant, as it is here that issues that divide voters need to be mapped and targeted actions on these issues need to be monitored. These should then be communicated to policymakers, journalists and candidates, and the potential for escalation should be raised (Rosenstedt, 2021). Also central to this recommendation is the ability of individual public bodies to engage appropriately with platform providers. However, experience shows that no progress has been made. The Avaaz team's report points out exactly that. In 2019, there were 158 million views of political falsehoods about the upcoming presidential election monitored by Avaaz. That number is horrific in itself, but when you add in the 153 million voters registered for the 2018 mid-term elections, you can jump straight to the conclusion that at least one piece of fake news has reached every single voter (AVAAZ, 2020).

Following Russia's attack on 24 February 2022, the European Parliament reaffirmed its opposition to foreign interference in democratic processes in a resolution of 9 March 2022 (European Parliament, 2022). In this area, protests against interference in elections could not be ignored. The reason given for this was that the external aggressor was using the fundamental values of the Unison, namely openness and pluralism, the dangers of which and the weakening effect on social resilience are only increased by the use of new, modern technologies, which create doubt and uncertainty and delegitimise the entire electoral process. However, whether the EU and the Member States will have a real response and whether progress will be made in this area by the 2024 elections is still very much in question, as it is now quite clear that unless social media platforms are genuinely involved in this process, share their screening mechanisms and cooperate with public authorities, there is no real chance of effective action.

4. Conclusions

Given the complete transformation of the security environment in recent years, and the security challenges that are becoming total, a sustainable security environment can only be achieved in a resilient society. Election security is one of the components of this area, where, based on the above regulatory and practical experience, progress is needed in the following areas to enable the European Union and its Member States to respond adequately to the threats to election security from cyberspace in the coming years:

Increase international cooperation. In order to develop the necessary resilience, Member States and regions should increasingly rely on information sharing, exchange of best practices and coordinated responses to election-related threats. NATO and the European Union are of particular importance in this process in the Euro-Atlantic region.

The codification of appropriate cybersecurity legislation is a priority. The European Union has made significant progress in 2022-23 with the regulation of NIS2, DSA, and DORA, among others, but the rules on critical infrastructure in the Member States are far from uniform. For example, the Hungarian regulation and cybersecurity strategy is already ten years old, so law enforcement faces extreme difficulties in responding to today’s security challenges.

NATO’s overall approach to resilience must include educating and preparing voters against specific cyber threats, and thus, there is a need to raise voter awareness in the areas of network security and cognitive security. The need to do so was highlighted by the infodemic during the COVID-19 pandemic. The most vulnerable are those who do not speak foreign languages, have a low level of education and live in small communities. We have seen many examples of this during this period, both in the Central and Eastern European regions. Thus, the importance of cognitive awareness has been highlighted in several EU documents, but no progress has been made to date in the field of individual education. It would be necessary to channel the development of these skills into public education and also to develop awareness-raising programmes for older generations at the local community level.

Transparency and verifiability are also key issues for states. Transparency and verifiability are key elements in ensuring the integrity of elections in an increasingly digital and interconnected world. Transparency refers to the openness and accessibility of the electoral process, allowing stakeholders, including voters, to observe and understand each stage of the election. This transparency is essential for building trust in the electoral system by allowing for independent verification and validation. In the context of electoral security, transparency means making the process of casting, counting and tabulating votes as clear and understandable as possible. This may include measures such as publicly accessible electoral databases, clear guidelines on electoral procedures and open-source software for electronic voting systems. Confidence in these systems can be undermined by, among other things, over-regulation and excessive reliance on traditional solutions that are difficult to understand in a digital environment (e.g. the Hungarian postal voting system, which has suffered from a number of setbacks in recent years), over-control of the digital space or political ambitions to do so. Verification complements transparency by ensuring systematic and rigorous scrutiny of election results and processes. Audits are essential to verify that the results declared correspond to the votes actually cast, thus preventing fraud and ensuring the accuracy of results. Various forms of auditing can be used, including post-election paper ballot audits and risk-constrained audits. In these procedures, a statistically significant sample of paper ballots is examined to confirm the integrity of the results of the electronic voting system. The combination of transparency and verification enhances the credibility of the election process, assuring the public that their votes have been accurately recorded and counted, and providing a robust defence against potential cyber threats and manipulation.

References

- AVAAZ, 2020, Avaaz Report 5/11/2019. <secure.avaaz.org/campaign/en/disinfo_report_us_2020>, accessed 18.07.2023.
- Campos-Freire F., Rodríguez-Castro M., Gesto-Louro A., 2020, The reform of audiovisual legislation and electoral coverage in Spain. (in Hungarian), Revista Latina de Comunicación Social, 76, 143–161, DOI: 10.4185/RLCS-2020-1441.
- CISA, 2023a, Cybersecurity Toolkit and Resources to Protect Elections. <cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>, accessed 18.07.2023.
- CISA, 2023b, Malicious Cyber Activity Against Election Infrastructure Unlikely to Disrupt or Prevent Voting. <www.cisa.gov/sites/default/files/2023-01/psa_cyber-activity_508.pdf>, accessed 12.09.2023.
- Craufurd Smith R., 2019, Fake news, French Law and democratic legitimacy: lessons for the United Kingdom? Journal of Media Law, 11, 52–81, DOI: 10.1080/17577632.2019.1679424.
- Dalby S., 2020, Anthropocene Geopolitics: Globalization, Security, Sustainability. University of Ottawa Press, Ottawa, Canada.
- Dannreuther R., 2013, International Security: The Contemporary Agenda. 2nd Ed, Polity Press, Cambridge, United Kingdom, ISBN: 978-0-745-65377-8.
- EPIC, 2023, Election Security. <https://epic.org/issues/cybersecurity/election-security/>, accessed 20.07.2023.
- EU, 2019, Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, LI 129/1.
- EUROPA, 2018, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation, Join(2018)36. Final. <https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation>, accessed 17/12/2023.
- EUROPA, 2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan. COM(2020) 790 Final, 03.12.2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?amp;qid=1607079662423&amp;uri=COM:2020:790:FIN>, accessed 17/12/2023.
- European Parliament, 2022, European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)). <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html>, , accessed 17/12/2023
- Giannopoulos G., Smith H., Theocharidou M. (Eds.), 2021, The Landscape of Hybrid Threats. A Conceptual Model. Public Version. European Union and Hybrid CoE, Luxembourg.
- Guillaume M., 2019, Combating the manipulation of information – a French case. Hybrid CoE Strategic Analysis, 16, <https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf>, accessed 17/12/2023.
- Isaszegi J., 2015, The 21st century is a war of living space for land, water and food . (in Hungarian), létezésért! Gondolat kiadó, Budapest, Hungary.
- JUSTICE.GOV, 2023, Key Findings and Recommendations from the Joint Report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections, <https://www.justice.gov/opa/press-release/file/1376761/download>, accessed 17/12/2023.
- Khanna P., 2016, Connectography: Mapping the Future of Global Civilization, Random House, New York, United States.
- Kirk N., Teeling L., 2021, A review of political advertising online during the 2019 European Elections and establishing future regulatory requirements in Ireland, Irish Political Studies, 1, DOI: 10.1080/07907184.2021.1907888.

- Kwak J., Jo J., Ku D., Lee S., 2022, The Relationship between Green Transportation and Leisure Travel Based on Social Media Data, Chemical Engineering Transactions, 97, 115-120.
- Lynch C., 2021, The regulation of online political advertising Evaluating the Government's proposals. L&RS Note, <data.oireachtas.ie/ie/oireachtas/libraryResearch/2021/2021-02-08_l-rs-note-the-regulation-of-online-political-advertising-evaluating-the-government-s-proposals_en.pdf>, accessed 12.09.2023.
- Makela J., 2019, Countering Disinformation: News Media and Legal Resilience, Hybrid CoE Paper, No. 1, <https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf >, accessed 17/12/2023.
- Moran D. (ed.), 2011, Climate Change and National Security: A Country-Level Analysis. Georgetown University Press, Washington, United States.
- NCTV, 2021, Cyber Security Assessment Netherlands 2021. <https://english.nctv.nl/binaries/nctv-en/documenten/publications/2021/08/05/cyber-security-assessment-netherlands-2021/CSBN2021_EN_02.pdf>, accessed 17/12/2023.
- Németh R., 2022, The effect of home office work introduced due to the COVID-19 epidemic on working conditions and organizational communication in a large company environment. (in Hungarian), Jog Állam Politika, No. 4. 87-109.
- Rosenstedt L., 2021, Improving Cooperation with Social Media Companies to Counter Electoral Interference, Hybrid CoE Paper, No. 5, <https://www.hybridcoe.fi/wp-content/uploads/2021/02/07022021_HybridCoE-Paper-5_Public-private-Cooperation.pdf>, accessed 17/12/2023.
- Squillace J., Hozella Z., Cappella J., 2023, Maintaining a Secure Foundation of Cybersecurity Awareness while Reducing eWaste and Carbon Output through Ethical User Actions and Sustainable Green Computing. AI, Computer Science and Robotics Technology , 2, DOI: 10.5772/acrt.18.
- Tenove C., Buffie J., McKay S., Moscrop D., 2018., Digital Threats to Democratic Elections – How Foreign Actors Use Digital Techniques to Undermine Democracy. The University of British Columbia, Vancouver, Canada.
- WIPO, 2023, Amendments to the Electronic Mass Media Law (Latvia). <www.wipo.int/wipolex/en/text/582042>, accessed 12.09.2023.