Information Security During Electronic Voting: Threats and Mechanisms for Ensuring

Mykola Buchyn
Department of political science and international relations
Lviv Polytechnic National University
Lviv, Ukraine
buchyn@ukr.net

Anna Helesh
Lviv Polytechnic National University
Lviv, Ukraine
anna.v.gelesh@lpnu.ua

Bohdan Shubyn
Department of Automated Control Systems
Lviv Polytechnic National University
Lviv, Ukraine
boshubin@gmail.com

2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT) | 978-1-6654-0618-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/AICT52120.2021.9628971

***Abstract* — The essence and features of electronic voting have been revealed. The main threats to information security during electronic voting have been shown. The main mechanisms for neutralizing existing threats and ensuring information security of electronic voting have been proposed.**

Keywords — electronic voting, information security, information technologies, threats, electronic democracy, election.

I. Introduction

The era of globalization and development of the information society has actualized the problem of informatization of all spheres of public life, not to mention the political sphere. Therefore, at the present stage we can observe a clear trend to increase the share of processes and services that are implemented in whole or in part remotely by electronic means.

The coronavirus pandemic has significantly actualized the issue of informatization of the life of society and the international community. Practically all spheres of society began to actively use information and communication technologies, platforms of remote communication, etc. These include distance learning, online shopping, distance meetings, summits, virtual museums, online libraries, etc. Information and communication technologies are playing an increasing role in the functioning of the state and civil society.

One of the most important and large-scale political processes is the electoral one, which is an instrument of representative democracy and is, in fact, a mechanism for implementing people's power. The trend towards informatization of electoral relations has long been stable around the world and is manifested, in particular, in the introduction by governments of many countries of electronic state voter register, increasing use of electronic media during elections and campaigning, using the Internet to inform voters about the course and results of elections, etc.

According to many politicians and experts, digitalization of the final stage of the election process – electronic voting – should be a logical and consistent step that shall correspond to the mentioned tendencies. This seems even more evident in the context of a pandemic that has significantly affected the electoral practices of the world. Many states were forced to postpone elections, and in the same countries where voting did take place, a large number of citizens did not participate in the elections for fear of infection. Therefore, more and more people started talking about the need to implement electronic voting. The issue is also topical for our state, because with the victory of Volodymyr Zelenskyy in the 2019 elections, a course for digitalization and development of the "state in a smartphone" was announced.

Nowadays, two main groups of theories differently assess the importance of e-voting and the possibility of its practical implementation. Representatives of one scientific camp see e-voting as an important way to improve and develop democracy and the electoral process according to current information society trends. Their opponents have a negative view of e-voting, seeing it as a threat to democracy. They either reject e-voting altogether or allow it with strict security mechanisms.

Therefore, in our opinion it is important to consider that the development of information and communication technologies includes new risks and threats associated both with increasing opportunities for manipulation of the population and cyber-attacks, which can threaten democracy in general, and the result of the vote, in particular. The electoral practice of the world (proven facts of Russian interference in the US presidential elections and in the elections of a number of European countries) shows that the effectiveness and expediency of electronic voting is possible only if all threats are neutralized and information security is ensured during the expression of the will.

II. International Security Standards During Electronic Voting

In our opinion, the security of electronic voting should be understood as the state of protection of all components of electronic voting, due to which the electronic voting system is protected from outside influences and interference, operates autonomously and smoothly, and electronic voting results reflect the real will of voters.

Since electronic voting is a relatively new and unknown phenomenon for most countries of the world, international legal regulation of electronic expression of the will is important. When considering international documents governing electronic voting, reference should first be made to the Venice Commission's Code of Good Practice in Electoral Matters, adopted on 30 October 2002 [1], the

978-1-6654-0618-5/21/$31.00 ©2021 IEEE

Recommendation of the Committee of Ministers № R (2004) 11 on Legal, Organizational and Technical Aspects of E-Voting of 30 September 2004 [2], as well as the Recommendation of the Committee of Ministers on E-Voting Standards № CM / Rec (2017) 5 of 14 June 2017 [3].

The Code of Good Practice in Electoral Matters addresses the issue of electronic voting only in passing. However, this document, which is considered a benchmark for democratic election standards, emphasizes for the first time that electronic voting must be secure and reliable. Under the security of electronic voting, the legislator understands the ability of the electronic system to resist attempts to deliberate hacking. Reliability of electronic voting, according to the Code, implies the ability of the electronic system to function autonomously, regardless of failures in hardware and software [1].

In the second document (Recommendations of the Committee of Ministers of 2004), the legislator notes that as information technology has become increasingly used in everyday life, European countries shall take this into account in their democratic practice. At the same time, the document contains a recommendation to Member States: in case of introduction, electronic voting should be based on democratic principles of elections, be reliable and secure [2].

The legal act recommends following such rules, which should ensure the security of electronic voting:

- states should ensure the security and reliability of electronic voting systems;
- the electronic voting system should be inspected by an independent body before operation, as well as after changes in its operation;
- all necessary measures should be taken to prevent falsification of data and possible interference with the operation of the system throughout the electronic voting process;
- it is necessary to ensure the resilience of the electronic voting system to problems, failures or attempts to block access;
- only authorized persons should have access to the central infrastructure, servers and election data;
- regular testing of the efficiency and reliability of the electronic voting system should be carried out [2].

Considerable attention in the Recommendations of the Committee of Ministers is paid to the reliability and security of the electronic voting system. In particular, the legislator recommends complying with the following requirements:

- regular software updates and corrections of electronic voting software protection;
- availability of an emergency plan;
- compliance of backup electronic voting systems with the same standards and requirements as for the main system;
- availability of sufficient reserves to ensure the continuity of voting;
- regular receipt of data from the monitoring of the electronic voting system by the reserve services;
- verification of the electronic voting system for changes in its work after any technical work;
- placement of equipment for electronic voting in a safe area, where reliable protection will be provided throughout the period;
- availability of equipment evacuation plan in case of natural disaster;
- ensuring reliable storage of data remaining in the electronic system after voting [2].

Another above-mentioned international legal act regulating electronic voting standards (Recommendation of Committee of Ministers of 2017) contains a rule that the right to vote is an important element of democracy, hence any voting mechanisms (including electronic ones) shall comply with international democratic principles. At the same time, the legislator notes the awareness of the potential problems of security, reliability and transparency of electronic voting systems. Therefore, Member States are encouraged to assess and address risks through appropriate measures, in particular those inherent in electronic voting systems [3].

III. Main Security Threats During Electronic Voting

First of all, it should be noted that there are different models of electronic voting, the main of which are stationary (requires the presence of a voter at the polling station during voting, which is carried out using a special electronic machine), or remote (carried out via computer (smartphone) by voter remotely and does not require his or her presence at the polling station) [4]. It is clear that each type of electronic voting has its own specific security threats. Therefore, we would like to note that in our publication we will consider the main security threats inherent in remote electronic voting, as we consider it more promising and relevant to current trends in the world.

In addition, we will consider the security threats to electronic voting in the context of the reliability of electronic systems and their protection from interference. Therefore, the complex of problems and threats related to the need to ensure the democracy of electoral procedures during electronic voting will remain in our attention. Although we understand the importance of this aspect of electronic voting, because without democracy observance, even a completely reliable and secure electronic voting loses all meaning.

The main security threats to electronic voting, in our opinion, include the following:

- threat of falsification of voting results by the election administration;

- the threat of interference in the operation of electronic systems by outsiders (hacking attacks) both in order to distort the voting results and in order to hinder the operation of electronic systems;
- blocking voters' access to the electronic voting system;
- damage of personal electronic means of voters;
- failures in the electronic voting system as a result of internal problems or the influence of objective negative factors;
- problems with Internet connection both for individual voters and in the context of the functioning of the electronic voting system in general [5].

As already mentioned, one of the important threats to electronic voting is hacking attacks. Researchers distinguish the following main types of hacking attacks on electronic voting, depending on the goals set by hackers:

- hacking attacks aimed at overloading a website where electronic voting takes place and the voter's loss of connection to the site;
- hacking attacks aimed at obtaining personal data of voters (in this case, the voter is redirected to an identical or similar to the official website);
- hacking attacks in which a voter is redirected to a duplicate site in order to adjust the election results;
- hacking attacks aimed at delaying information transmitted during electronic voting [6].

IV. Mechanisms of Neutralization of Security Threats of Electronic Voting

A number of mechanisms are considered appropriate to neutralize the security threats to electronic voting:

- ensuring the autonomy of electronic voting, in particular through the use of cryptographic protection;
- increasing the level of computer literacy of voters as a component of increasing the level of protection of personal computers and smartphones during electronic voting;
- conducting periodic audits of electronic voting systems. Such an audit should be both preliminary (performed before the start of electronic voting to identify malfunctions) and operational (performed after each change introduced in the electronic voting system, to verify the functional reliability of the updated parliaments and the absence of signs of outside interference in the electoral system);
- implementation of international certification of electronic voting systems;
- ensuring mutual control of persons responsible for the functioning of the electronic voting system;
- installation of equipment that provides uninterrupted power supply for electronic voting systems;
- availability of a contingency plan in case of force majeure during electronic voting, including the availability of a backup electronic system that meets the parameters of reliability and security;
- ensuring reliable round-the-clock protection of equipment used for electronic voting, in order to prevent access to it by unauthorized persons [2; 5].

The existing threats of electronic voting and possible mechanisms for their neutralization are shown in the Fig. 1

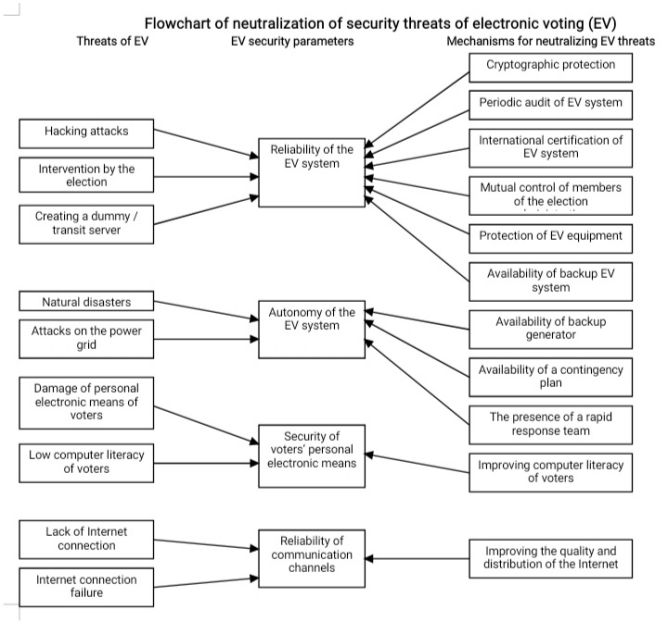

Fig. 1. Threats of electronic voting and possible mechanisms for their neutralization.

As already mentioned, the strategy of introduction electronic voting can be implemented only if the existing threats of information security are neutralized (see Fig. 2).

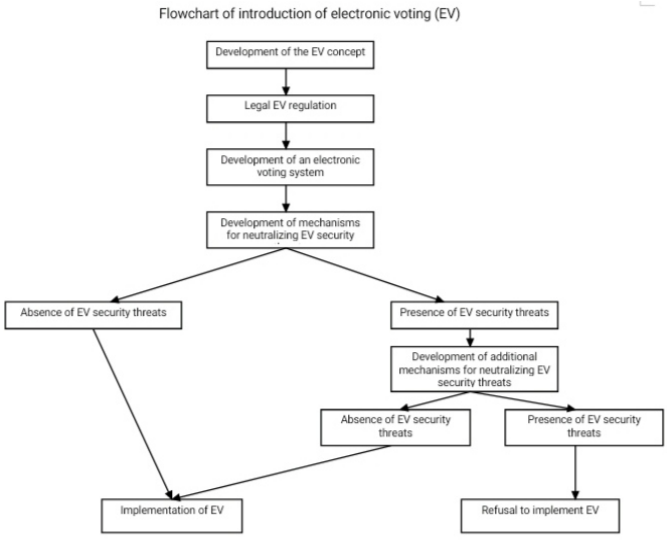

Fig. 2. The mechanism of neutralization of existing threats of information security in the context of the introduction of electronic voting

V. Use of Blockchain Technology and Smart Contract to Ensure Information Security of Electronic Voting and Anonymity of Elections

Nowadays, new technologies are developing very fast, which have a strong impact on our daily life. An example of a technology that can affect the electronic voting process is Blockchain [7,8]. We can see how fast the Blockchain and cryptocurrency in general are evolving. Blockchain, as a rule, is now commonly used by banks and the financial services industry to move money quickly, efficiently, safely and reliably. However, the features of Blockchain can be used not only to transfer funds or purchase goods, but also to conduct safe and anonymous electronic voting [8].

To conduct an effective vote, we suggest using Smart Contract, which is deployed on a Blockchain to ensure the use of a feedback mechanism. In general, a Smart Contract is a collection of code and data that is stored at a specific address on a blockchain. Creating a Smart Contract to vote on the Blockchain can increase the efficiency of the voting process.

In general, the electronic voting system implements the electoral process through the support of software and hardware. The election process, as a rule, includes registration, certification, voting, statistics and other stages.

In general, the electronic voting process will be carried out in four steps:

- In the Blockchain voting system, the voting initiator records the voting information in the Smart Contract and publishes it on the Blockchain before the official voting. Then voters can find out information about voting in a Smart Contract.
- The process of registering and logging in to a Blockchain-based voting system is usually completed when users log in to the Blockchain.
- The voting process takes the form of sending a transaction to a Smart Contract account.
- After that, the initiator of the vote can get the results.

The general process of electronic voting in the Blockchain is presented in the Fig. 3.

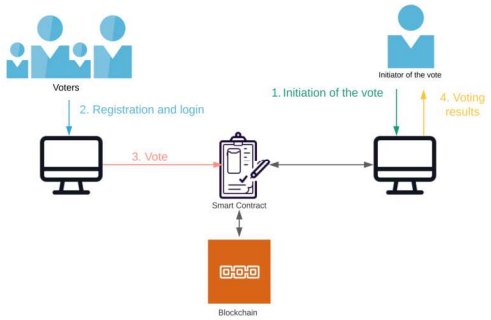

Fig. 3. Voting process in the Blockchain

The use of such a voting system has many advantages over conventional voting systems. The electronic voting system requires less time, energy and expense than conventional voting systems. This system eliminates the possibility of false or dubious votes, which allows to get the most accurate results. This system is also very environmentally friendly, as it saves many trees that would be used to produce ballots. The electronic voting system can also prevent the manipulation or sale and purchase of votes, which is often encountered in polling stations. The electronic voting system not only modernizes the electoral process, but can also potentially enhance interaction between citizens and the government through platforms based on information and communication technology (ICT).

VI. Conclusions

As we can see, the use of electronic voting carries a number of security threats, without the neutralization of which it is impossible to ensure the democratic nature of the voters' expression of the will. The electoral practice of both foreign countries and our country testifies to the reality of such security threats, which significantly undermines the potential value of electronic voting. At the same time, in our opinion, when considering the expediency and possibility of introducing electronic voting, we should act in the direction of neutralizing security threats, and not abandoning electronic voting. This is due to the fact that the introduction of electronic voting in the information age is in line with modern trends in human development, so provided that the existing security threats are neutralized, it can significantly contribute to the development of democracy in the world.

References

[1] «Code of Good Practice in Electoral Matters», European Commission for Democracy Through Law (Venice Commision), 2002, https://rm.coe.int/090000168092af01

[2] Recommendation Rec (2004) 11 of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting, 2014, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dbef8

[3] Recommendation CM/Rec (2017)5 of the Committee of Ministers to member States on standards for e-voting, 2017, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016807726f6f

[4] N. Melnykova, M. Buchyn, S. Albota, S. Fedushko, S. Kashuba, «The Special Ways for Processing Personalized Data During Voting in Elections», in International Conference on Computer Science and Information Technology, 2019, pp. 781-791.

[5] O. Y. Peskova, S. V Fateeva, «Risks and e-voting issues», in Informative counteraction to the threats of terrorism, № 23, 2014, pp. 152-164.

[6] I. Irhin, «Voting via the Internet: to the Issue of the Prospects and Problems of Adaptation of Foreign Experience in the Russian Federation», in Legal Bulletin of the Kuban State University, № 3 (24), 2015, pp. 18-24.

[7] T. Maksymyuk, J. Gazda, L. Han and M. Jo, "Blockchain-based intelligent network management for 5G and beyond," IEEE International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 36-39.

[8] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 1 July 2018, doi: 10.1109/TKDE.2017.2781227.