TECHNIUM

Technium Vol. 3, Issue 2 pp.42-66 (2021)
ISSN: 2668-778X
www.techniumscience.com

CONTRIBUTIONS ON IMPROVING THE CYBER SECURITY OF THE AUTHORITY'S IT SYSTEM PERMANENT ELECTIONS

Adrian-Viorel Dragomir
Phd. University Politehnica of Bucharest

ABSTRACT . In order to respond effectively to the desire to constantly improve the electoral process, the Permanent Electoral Authority has undergone a series of administrative and regulatory change processes, in line with new trends in public administration management, namely simplification, dematerialization, digitization, staff professionalization, debriocracy and decision transparency. The research report analyzes the institution's most important cyber security reforms in line with the new public sector models, and proposes a new security solution that is suitable to be integrated into the AEP's it system.

KEYWORDS cybersecurity, innovation, defense against attacks, security measures

INTRODUCTION

Election processes are the basis for the functioning of representative democracy in any country, and compromises of any kind on this chapter can delegate an entire political system. At the same time, we see that elections are often becoming an increasingly frequent target in the modern digital age, which is being attacked around the globe. Therefore, cyber attacks, most probably combined with information operations and other hybrid threats, are a reality in terms of choices and need to be reflected in careful defense planning and risk management.

As far as electoral processes are concerned, a successful campaign of discredit can be carried out through successful cyber attacks, which can lead from the deterioration of results to the compromise of the entire electoral process. These actions could impact both on the legitimacy of the state's management and on the trust of other countries and companies that want to run their business internally.

From the point of view of the citizens, electoral processes must respect constitutional principles, i.e. be free, open, fair and based on the principle of secret voting, and technology cannot be introduced in elections at the cost of compromising any of the principles set out above.

Digital solutions, or electoral technology in itself, are no more or less secure than traditional paper voting solutions. These technologies need to be introduced with caution, with the prior assurance that they comply with the same legal and technical requirements as traditional options. Over time technology has shown that it can ensure that these requirements are met in order to ensure the legitimacy of the election results.

Over the last 15 years, cyber attacks on it&C infrastructures used in the elections have been seen to be backed by shadow States, often accompanied by intelligence and oriented toward the

sowing of discrediting, doubts and discord with the most likely objective of disrupting or influencing democratic processes. Even electoral systems that rely exclusively on pen and paper in the whole electoral process, take advantage of digital tools and services for drawing up and managing electoral registers, registering candidates or centralizing and communicating election results.

There is no ground to say that the digital solutions developed recently, which are used in elections, are not less secure than paper-based voting solutions, but rather we stress that new technologies must be carefully introduced in the electoral processes, while verifying that they are implemented according to the same legal requirements and security levels as traditional solutions.

While the activities or electoral processes themselves, the registration of voters and candidates, the counting and centralizing of votes and the communication of turnout and election results, are by no means impenetrable in the event of cyber attacks, recent events highlight the acute need to also defend ancillary computer systems or which are used as support for electoral activities, for example computer applications used by political parties or those who verify the results of elections, including the media that ensures respect for democratic rules.

As a result, electoral management institutions and cyber security organizations must take measures to protect against hybrid attacks, by pro-active surveillance of information systems to ensure a secure environment for the technology used in the elections.

In order to be effective, cyber security measures specific to electoral processes need to be reviewed as often as possible, as regards:

- registration of voters and candidates in databases;
- electronic tools used for counting and centralizing votes;
- digital tools that count, transmit and process votes;
- systems for publishing or communicating the results of elections;
- relevant ancillary systems and services.

In recent years, the international security environment has changed dramatically and cyber security institutions have expressed concern about the motivation and increased capacity of States and non-state actors to pursue their objectives by engaging in malicious cyber activities[1], integrated with other operations or campaigns. These cyber attacks targeting the basic functions of electoral management institutions undermine their legitimacy and void the guarantees they offer to participants in the democratic process. Therefore, a robust defense against cyber attacks on the technology being used in the elections must not under any circumstances be overestimated.

Cyber attackers who are often politically motivated, including by state entities, are constantly seeking opportunities and attack targets, and for that they acquire or have sufficient resources, which are usually renewable and strategic, because they combine cyber sabotage with economic and political espionage. These malicious actors have often attacked the it systems of electoral management entities to destabilize the election processes in order to delegate targets or gain awareness of what may also bring with it a potential geopolitical influence.

For example, in France, data and information from the presidential candidate Emmanuel Macron's campaign were ex-filtered shortly before the May 2017 elections. Security company Trend Micro announced in May 2016 that German Chancellor Angela Merkel's party was the victim of cyber attacks, Fact is, that CDU employees received phishing emails that were connecting to an authentication page similar to that of the genuine web mail service where the attacker retrieved the authentication data of those who entered it on the "take" page. The same year, information appeared that the US national Democratic Committee's servers were victims of a large number of cyber attacks, resulting in the theft and unauthorized publication of politically sensitive materials. According to the US intelligence services, the attacks, attributed to a state-supported actor, were part of a campaign aimed at influencing the US presidential elections in 2016.

[1] council conclusions on cyber activities,https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/ro/pdf , website consulted on 20.09.2020

Such events are taking place across the board and highlight the dependence of electoral processes on technology, leading to the urgent need for measures to strengthen cyber security in the whole electoral technology.

It is more than obvious that elections are a national prerogative, but nevertheless, cyber threats tend to become globalized and attackers can be part of multinational groups with different criminal profiles and transnational interests. This leads to the conclusion that exchanges of experiences between States in the field of cyber security, in terms of IT&C electoral infrastructures, are beneficial because attack vectors or cyber attackers can often be similar.

The electoral systems of EU Member States also have a strong international component, and the impact of cyber incidents and threats on any of the components of the information systems used in the elections can have EU-wide effect. The European Council was mandated by Member States to ensure the integrity of free and democratic societies in the digital age by protecting EU citizens' constitutional rights, freedoms and online security, as well as the integrity and legitimacy of democratic processes, in particular elections.

Similarly, the Secretary-General of the European Parliament wrote[2] to the Chair of the Cooperation Group established in the wake of NIS Directive (EU) No 1148/2016, in October 2017, asking him to put in place measures to increase cyber security in the elections, "Elections are a particularly sensitive process in a Union that has "democracy" as one of its founding values." The highest official of the European Parliament underlined in its letter that a cyber security incident during the elections "could create major disruptions in the functioning of any democratic state".

The electoral management institutions of the Member States should identify best practices in identifying, mitigating and managing risks in electoral processes from cyber attacks to disinformation/fake-news and facilitate the exchange of experience in these areas.

Therefore, A cyber-security workflow of technologies used in elections was created under the auspices of the Cooperation Group established by the NIS Directive at European Union level to share experiences and provide guidance on the development and implementation of the software being used in the elections, as well as an overview of tools, techniques and protocols to detect, prevent and mitigate these threats.

Furthermore, we stress that it is not only the central computer systems of electoral management bodies that are concerned by cyber crime, but also the ancillary or support computer systems used for elections, including other government computer networks and databases, the computer systems of candidates, parties and the media. Any of these it systems can be targeted by attacks, which can similarly undermine public results or trust in elections, as demonstrated in a multitude of electoral events or campaigns.

Checklists and case studies can provide important practical guidance for making cyber security measures more effective depending on the specific choices, including:

- Software development methodologies that are specific standards of development and implementation, sets of principles, systems of ideas, concepts, methods and tools that determine the style of software development.
- Cyber security principles applicable to electoral technology, which shall include testing of software applications and computer auditing;
- Implement and enforce software-specific security measures supporting all categories of electoral activities.

We conclude by saying that cyber attacks, most probably combined with information and other hybrid threats, i am part of today's realities in terms of elections and the response of electoral management institutions to these risks must be reflected in the diligent defense planning and responsible management of the risks associated with attacks.

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO, website: 20.09.2020

Technium Vol. 3, Issue 2 pp.42-66 (2021)
ISSN: 2668-778X
www.techniumscience.com

1. IT SYSTEMS MANAGED AT THE LEVEL OF THE PERMANENT ELECTORAL AUTHORITY

Public sector organizations need processes, structures, and applications to improve employee productivity. Given that there is a high momentum in public administrations in changing the paradigm in IT&C, for reasons of changes in government regulations or changes in information systems, they need to be designed flexibly and adaptable in order to integrate these changes easily.

There is a tendency at national level to introduce various information technologies in public administration, in particular it applications that have proved their effectiveness in the private sector first. Their failure to adapt to the specificities of the public sector, which is not committed to maximizing revenues and increasing profits, may lead to the failure of these initiatives.

In the public sector, the target must be to drastically cut red tape and the amount of office work that is done manually, which must become working procedures in relation to citizens and improved regulations. Public administration is not directly aimed at increasing competitiveness, but rather at meeting the needs of the public and those at the service of the affe1. Even though theory and means of implementation are much the same in the public as in the private environment, the objectives and methods of implementation are quite different, so the approach of it projects in public administration is substantially different.

It systems are combinations of equipment, programs, applications, databases, communications networks, policies and procedures that process, accumulate, find, and disseminate data and information. Organizations and their employees rely on modern it systems to communicate with each other, using a variety of devices or equipment, instructions and data processing procedures, communication channels and stored data. The term "it system" of the Permanent Electoral Authority defines it as the entire equipment, software applications or ICT licenses used in the performance of the activities of the institution.

The main purpose of AEP implementation of it systems is to move toward e-government services in the sense of using technologies and the Internet to provide information and services to citizens, officials and public institutions with which they interact. In addition to improving the way services are delivered, e-government makes AEP activities more efficient and allows citizens easier access to information and the possibility to interact electronically with local public authorities.

E-government is an ever-expanding phenomenon with a sustained pace of development with a strong influence on the activities provided to the public, which in the future calls for increased spending from the AEP budget for this purpose, In order to solve as many of the general problems of the public administration in Romania as possible in relation to citizens, among which we recall bureaucracy, lack of open data, lack of interconnected data sources between the public institutions in Romania.

At the beginning of the development of the concept of e-government at the level of the institution, it was manifested by the introduction of office applications, then of reporting and control information systems, and then of expert systems implemented for both internal activities and for the organization and conduct of electoral processes.

In addressing eGovernment as an information system, the following components can be found at AEP level: Equipment, programs (software), data and people. The system collects, processes, maintains data, obtains and communicates information, and manages knowledge. The existence of information systems within the institution was not conditioned by the use of information technologies, especially because in the public administration in Romania, a large part of the operations must be carried out manually or on paper for legal reasons. The use of information technologies does not define the information system of AEP but optimizes it.

The core of the information system of the Permanent Electoral Authority is first the data, information and knowledge, then the IT&C components, which support their collection, processing, storage and communication. And for eGovernment to be an information system within the AEP, a well-balanced mix of data, information and various technologies is added to the human resource, which gives the system a purpose and meaning, making organizational processes executed and carried out on the basis of a number of well-developed operational procedures.

Thus, the principle of e-government in AEP was considered as a "socio-economic and technological" concept, with a focus mainly on the social component (people), which is often insufficient or poorly managed in e-government projects and in secondary terms on the component of automated processes, major financial and human resources are allocated to the development and implementation of which.

Practice has shown that most of the failures in this area are due to the lack of education or trust in civil servants' information systems than to problems related to technology, which has required us to invest in vocational training and technological education, that leads the human resource to an understanding of automated organizational processes through specialized applications.

The e-government information system within the AEP is tailored to organizational structures, governance system, strategy, policies, technical-economic processes and available resources. In turn, the organization operates in an environment that presents various specific economic, political, legal, social-cultural and technical aspects, a wide context of laws and values, economic systems and technological innovations.

Some of the most common "check" lists, named in the computer system literature, ICPSODA, terminology derived from the acronyms of the terms (capture, input, processing, storage, output, decision-making, and action), have been used to create the information system on which the principle of e-government is based. what are the procedures that take place through the system.

The CIPODA checklist focuses on the activities of the information system, which involve working with data, information and knowledge. The classic data cycle includes the following activities:

- data collection/finding;
- entering the data into the system;
- data processing;
- the storage of data and processing results;
- to obtain the results in the desired form;
- the decision-making, supported by the information obtained through the processing of data;
- action to implement and implement the decision taken.
- communication of the decision taken, which is essential for the good conduct of all others.

To give meaning to the strategy for developing the principle of e-government within the institution and for its effective implementation, At the management level, the decision was taken by the restructuring of the activity and of the departments of the Permanent Electoral Authority, which was carried out by the decision no. 4/2020 of the Permanent offices of the Chamber of Deputies and the Senate, on the approval of the Regulation on the organization and functioning ofthe Permanent Electoral Authority. [3]

As part of this process, the it&C field was divided into two main categories, namely the it systems through which electoral processes forming the national Electoral information System (SIEN) are managed and the internal it systems providing support for the daily activities of the Authority's employees and its interface with the general public, We will continue to call the information system of the Permanent Electoral Authority (SIAEP).

[3] https://lege5.ro/App/Document/gm4dsobvhaya/regulamentul-de-organizare-si-functionare-a-autoritatii-electorale-permanente-din-26102020, website: 02.11.2020

1.1. NATIONAL ELECTORAL INFORMATION SYSTEM

At the level of the Permanent Electoral Authority, the Department of national electoral information system (DSIEN) is in direct coordination of the President of AEP and is in charge of managing applications of management and records of Romanian voters as well as of information systems that are used in elections to register candidates, registration of the turnout, verification of the voting rights of the citizens going to the polls, centralization of the voting results and application of the algorithms in the electoral laws for the purpose of holding mandates.

In accordance with Article 17 of judgment No 2/2019 on the approval of the Regulation on the organization and functioning of the Permanent Electoral Authority, he shall perform the following general tasks:

a) develop standards, strategies, policies and programs for the computerization of electoral processes and ensure their implementation;

B) carry out, coordinate and supervise the implementation of the Authority's process automation concept;

c) constitute the material basis specific to the national electoral information system by providing the necessary services, applications and it products;

d) certify, without change, the computer programs for centralizing the results of elections and referendums and make them available to the persons prescribed by law;

(e) draw up the plan for the acquisition of equipment for the development of the national electoral information system;

(f) monitor the performance of contracts within its field of activity and perform the reception of services or products, as appropriate;

G) issue instructions on security measures in connection with the management and use of the Register;

H) ensure audits of the security of the electoral registry and the other components of the national electoral information system, in accordance with the law;

i) administer, coordinate and carry out activities to update the Register of elections, according to the law;

J) establish the list of specialized staff, certified by the national Statistics Institute, who participate in the centralization, processing of data and observation of election and referendum results;

k) carry out the it system for monitoring turnout and preventing illegal voting, which is the responsibility of the Authority;

l) coordinate and methodologically guide persons authorized to operate in the electoral register;

M) ensure the exchange of data on Romanian and European voters with similar authorities in other EU Member States;

N) establish policies for cyber protection and security within the Authority's sphere of competence.

In accordance with the legal functions presented above, the entire arsenal of computer applications functions at the level of DSIEN, which are used as operational support for the smooth running of the electoral processes in Romania, and which we will present in detail.

1.1.1.IT SYSTEM ELECTORAL REGISTER

The computer system electoral register (SIRE) is a complex portal that was created in order to ensure a fair and transparent electoral process by accurately establishing the number of Romanian

voters, recording, updating, recording, recording, placing them on Romanian and foreign polling stations and for management, training and selection of computer operators and election experts who are part of the technical apparatus at all levels of the electoral constituencies in the country and abroad.

The electoral register is structured in counties, municipalities, towns, communes and manages the electoral record information of all Romanian citizens who turned 18 years old The mayor of each territorial administrative unit has the responsibility to operate, modify and update the information in this computer system in order to record and update the identification data of the voters and the information about their setting up on the polling stations.

The management component of the body of electoral experts and computer operators is managed, operated and kept up to date at the level of the Permanent Electoral Authority by all the county structures of the institution in charge of managing the persons who are part of the two electoral bodies.

Thus, by means of the electoral register, any situation in which the data recorded in the application on voters or election officials are wrong or there are people who have been left out of the electoral lists can be operationally solved, or misplaced on polling stations or identifying omitted persons on permanent electoral lists due to prohibition of electoral rights or death.

Another main feature of this system is the printing by mayors directly from the electoral register of permanent, special, supplementary and supplementary electoral lists, which include voters in polling stations by residence or residence, What are used in all types of electoral processes taking place in Romania.

The information system of the electoral register has been developed with two main sections, which have different principles and rules as regards the target audience to which it is addressed:

- The public section, aimed at giving all Romanian voters access to information intended for them;
- The private section, aimed at the public institutions in Romania that have functions in the electoral register, in accordance with the powers conferred by the laws in force.

By accessing the public section of the electoral register, Romanian citizens having the right to vote have the possibility to check the registration of their personal data in the electoral records and their correctness, without having to go to the premises of the town halls where they have their address of residence for this purpose. By accessing the web page found at www.registeralelections.ro and entering the NSP, the name and an automatic code to determine that the user of the software is a person or computer program, of the type of CAPCHA, Any Romanian voter can find the polling station in which he is held and all his location data, including a geo-localization module with a "go me to the station" function, which helps citizens reach the polling station location by using GPS coordinates.

Within the framework of the portal, a module is implemented to facilitate the communication of citizens with the mayor, which aims to facilitate the communication of citizens with the authorities involved in the electoral process in Romania, by developing a system of referrals/petitions by which citizens can notice the inappropriateness of their data, which are recorded in the electoral register. Through the application, citizens have the possibility to submit an online application requesting information from the mayor on their own data entered in the Electoral Register. The completed application online will be signed electronically with a qualified digital certificate and will be loaded into the portal. This module is called "citizens' communication with the Mayor" and is developed taking into account three different types of user profile, namely: Citizens authenticated on the Electoral Register portal, mayors or AEP staff.

From the Electoral Register portal (the Mayor profile) an offline application tool can be accessed and installed on the computers of the City Hall, for cases where the portal cannot be accessed to perform operations within the time limits stipulated by law. The application can be installed by users on their computers. Following installation, access will be allowed in both the online

and offline application (only if there is no internet connection). This module allows the entry of cancellations and residence voting requests in the electoral register.

Citizens holding a qualified digital certificate may have access to their own data from the electoral registry portal. After authentication in the portal, on the basis of the qualified digital certificate, the citizen will be able to access a dedicated graphical interface through which his or her personal data is presented, the polling station where he or she is held, the position on the electoral list has the possibility of downloading some certificates and other electoral records it needs.

Qualified digital certificate authentication is intended for both AEP users and public users enrolled in the electoral register portal.

Any inadequacies between the data provided by the electoral register and the real ones can be signaled by the voters, through the public portal, to the mayors and the representatives of the Permanent Electoral Authority. The voters also have the possibility to register through the portal with their residence address, under the conditions imposed by the electoral legislation, to communicate with the mayor and make requests for data or electoral documents.

The private section of the electoral register is the module by which the data that is managed by this application is updated by the mayors of all the territorial-administrative units in Romania. The data shall be kept up-to-date by:

- addition of 18 year old people to voters;
- adding citizens who have acquired romanian citizenship;
- addition of those who have ceased to suspend the exercise of electoral rights;
- the removal of deceased voters;
- the removal of those who have lost their romanian citizenship;
- the removal of those who have been banned from exercising electoral rights or banned by a court.

The electoral register allows the mayor to know at all times how many voters there are in the city, ensuring accuracy and timeliness in the generation of permanent electoral lists and the delimitation of polling stations.

The electoral register is an integrated information system, developed in the centralized architecture with access from web interfaces, which stores the data in a single database containing all persons over the age of 18 in Romania, A unique register of polling stations in Romania and information about the body of computer operators and the body of electoral experts. The it system is used by users in country-wide territorial administrative units specifically designated by mayors for this purpose, as well as by AEP users. The system ensures simultaneous access for multiple users, while allowing for the competitive use of the system by all the territorial administrative units in the country.

The it system the electoral register facilitates the Permanent Electoral Authority's role of arbitrator and mediator in the conduct of the electoral process, facilitates real-time information on polling stations and makes the process of reporting these data to the actors involved in the electoral processes more efficient.

In order to fulfill the legal and operational obligations of the AEP, which resulted from the latest legislative changes, the need for revision has been identified, updating and putting into service modules that were traditionally found in software tools for data processing and editing of reports needed to centralize voting results.

Thus, during 2020, the modules for registering applications and allocating mandates that were certified for change and used in the 2016 elections were integrated into the electoral register. These modules have been integrated into the electoral register infrastructure to ensure their interoperability with the register portal by consolidating them into a new version of the web application that has been installed and integrated into the web application of the existing infrastructure, develop information exchange services with the electoral register databases and ensure that end-users have access to these functionalities of the public web portal working interfaces.

The amendment of Law no. 370/2004 for the election of the Romanian president, republished since 2019, has been enacted the way to register citizens who want to vote abroad, at balloting stations created outside the country for this purpose or by correspondence.

In order to register in the electoral register as a voter abroad, a new portal called a foreign vote was developed at the level of the Permanent Electoral Authority, which can be accessed at https://www.votstrainatate.ro/, [4]And a component of the electoral register portal intended to communicate with citizens who wish to vote by mail or at the polling station, in accordance with the law.

The new component is called "Communication of citizens who wish to vote abroad and has been developed according to the types of user profiles that will use the portal, On the one hand, voters who will have access to the public section of the voting abroad portal and, on the other, users with a diaspora AEP profile who are employees of AEP and have a role in managing the information of the Electoral Register portal.

The basic functionalities of the voting abroad portal are:

- loading documents and registering citizens for voting at the section abroad
- loading of documents and registration for voting by correspondence from abroad
- the completion of forms with automatic field validation;
- upload your id copy and proof document Residence abroad and transmission to AEP of them and the data completed in the forms
- collect options to view / edit / cancel submitted request To AEP with authentication of the original application data
- how to view the requests that have been sent to AEP
- The way in which applications submitted to AEP are edited
- How to cancel a request submitted to AEP
- Contact details for citizens wishing to make a referral in connection with their requests, contact phone, contact mail address, address of AEP headquarters

Citizens have the possibility through the voting abroad portal to submit applications online through, requesting AEP to vote abroad in elections where citizens residing abroad have the right to vote by, at one of their voting options, by correspondence or at the polling station, under the law.

Online filled-in requests shall be displayed as entries in the system, in the diaspora AEP interfaces of the Electoral Register portal, depending on the actors involved and along with their status of resolution (status of the request).

From a logical point of view, the key to the services offered by AEP through the electoral register is to integrate them into a unified, user-friendly, user-friendly, intuitive interface that allows users to find useful information on-line in an easy, quick way, secure and confidential and allow for easy operation of everyday tasks.

The definition of the architectural solution of the electoral register has been achieved in order to achieve the following fundamental objectives:

- definition of reusable services divided into logical levels, each level having well defined functionalities;
- the modularity of the solution allowing the continued expansion of the services provided and the non-restriction of the number of public or authenticated users of the services provided;
- adaptability to legislative, administrative and technological changes;
- the scalability of the solution to easily accommodate increases in terms of number of users, throughput, or changes in the hardware infrastructure;
- architectural topology with central organization and distributed clients that can access the application using only a web browser;

[4]https://www.votstrainatate.ro/, website: 02.11.2020

- easy integration with external systems using open standards.

The logical architecture of the electoral register information system at AEP level contains the following components:

- The web server and application server component that provides the integration of all the components of the system.
- Portal component where part of business services are exposed to users in town halls and other institutions (Government to Government, G2G) or to voters (Government to citizen, G2C).
- Data component – represents the relational database used for the storage of all data handled within the information system
- The business intelligence component is used to extract information from existing applications and data sources within the electoral register and distribute it within the organization to optimize business processes, decisions and actions
- The external integration component used to expose AEP services in the form of WEB services to be called from applications of other institutions.
- Authentication server component used for user management and through which is used to authenticate users on the system
- Component to protect servers from computer attacks - antivirus.
- Server monitoring and protection to provide pro-active protection based on server behavior
- Virtualization component that enables efficient use of existing hardware resources and their dynamic allocation according to operational needs
- Client workstations from which end users access computer system services via A WEB browser.
- External systems accessing the web services exposed through the integration component.

The hardware infrastructure of the electoral registry information system is hosted in a mobile data center acting as the primary infrastructure and a disaster recovery and business continuity (DRBC) backup and recovery solution that is implemented in a low seismic risk area, The EC is designed to ensure the operation and access of SIRE-managed data regardless of the main data center's operational problems.

The DRBC data Center is built as a virtual environment for replicating the authentication and authorization components of the existing electoral register in the main data center. Replication solution provides data storage virtualization in the two data centers and ensures both replication and failover across all databases.

The replication solution ensures that the switch to the secondary site will be made without loss of data regardless of the reasons for the failure of the main site, and the maximum switching time from the primary to secondary database (passive) is 15 seconds.

1.1.2.IT SYSTEM FOR MONITORING TURNOUT, PREVENTING ILLEGAL VOTING AND CENTRALIZING ELECTION RESULTS

An important project implemented by the Permanent Electoral Authority for dematerialization and improvement of electoral processes by introducing information technology is the information system for monitoring turnout and preventing illegal voting (SIMPV).

SIMPV is an innovative project for the Romanian electoral system, which was put into practice for the first time in the 2016 local elections. The AEP is responsible for the development and implementation of this project, based on information from the electoral register and the register of polling stations, and is actively supported by the Special Telecommunications Service (STS).

The implementation of SIMPV shall aim to achieve the following objectives:

- facilitating the verification of compliance with the legal requirements for the exercise of the right to vote;

- The identification of the voters who are to vote is already recorded in the SIMPV;
- reporting of cases where persons submitting to the vote do not have the right to vote or are prohibited from exercising the right to vote;
- facilitating the exercise of the right to vote;
- ensuring that electoral registration is unique;
- an exhaustive presentation of turnout by automatic counting of the total number of voters present;
- ensuring the transmission of messages and information to electoral offices;

The computer system for monitoring turnout shall consist of the following main elements:

- the central information system;
- The it application for the verification of the voting rights, called the ADV;
- technical support center;
- communication infrastructure;
- tablet computer terminals at polling stations.

The central it system is a complex it-system composed of database servers, computer application servers, data communication equipment, cyber-incident protection equipment and administrator workstations provided by the Special Telecommunications Service. The central it system functions in the data center of the Special Telecommunications Service, in a special space for this purpose, to which the representatives of the Permanent Electoral Authority and the members of the Central Electoral Office have access.

The right-to-vote application is a computer software produced by the Special Telecommunications Service with its own resources, Which ensures that all voter identification data collected by computer operators on the day of the electoral event in the polling stations are processed and compared to the data already recorded in the databases, which were imported from the electoral register in advance.

The Technical support Center is an integrated communication center through which the Special Telecommunications Service, together the Permanent Electoral Authority, provides technical assistance to computer operators in polling stations, both on the day of the vote and in all tests that are carried out before the electoral event.

The communication infrastructure contains the following types of communication services and resources identified at polling stations and which can be used for the operation of the SIMPV:

- internet services in places where polling stations will be organized,
- data communication services on mobile operator networks;
- special telecommunications services, where the above services are not
- available.

The following computer equipment and means of communication shall be provided for the day the electoral process takes place in all the premises of the electoral offices of the polling station:

- a computer terminal with integrated mechanisms for the automatic and manual retrieval of identification data from the machine-readable zone with optically identifiable characters from identity cards and passports of voters who present themselves to the vote;
- Access to the Central information System through existing services at the polling station's electoral office or mobile operator networks, as appropriate.

Each computer terminal is uniquely identified in the SIMPV by the international identity number of the mobile equipment and the MAC physical address allocated to the network card and the unique identification of the two numbers, the ADV interface is accessed via the tablet.

SIMPV aims to monitor real-time voting turnout, to identify multiple voting attempts and to verify the conditions for exercising the legal right to vote. Voters can exercise their right to vote only

after they have been registered by a computer operator in the computer system for monitoring turnout and preventing illegal voting.

By registering all voters in the SIMPV, members of the branch of the electoral office may immediately discover the voter's position on the permanent or supplementary electoral lists, and if assigned to another polling station, if the right to vote is prohibited, whether he is a minor on the day of the elections or was previously registered in the system by another operator. The it system thus plays a key role in preventing, identifying and sanctioning this type of test.

On the day of the vote, after closing the polling stations at 21:00, using the tablet provided, the computer operator has a legal obligation to record the video of the vote counting process and the information is stored on the central server for a maximum period of 30 days, to prove possible deviations from the applicable electoral legislation.

One important component of SIMPV is the module of recording the voting results in the electronic minutes of the polling stations on the computer operators' tablets, which is called the computerized system for collecting the minutes (SICPV).

The central information system, the communication infrastructure and the computer terminals at the polling stations shall also allow electronic checking of the control keys in the minutes recording the voting results and their electronic transmission.

This computer application module shall be activated automatically, after 21.00, when the application to monitor voting presence and prevent illegal voting is closed at the end of the voting hours at the polling stations and the counting procedure is carried out, establishing the results and sending them to the upper election offices, with a view to centralizing the results of the elections and holding mandates. The main functions of this module are:

- ensuring uninterrupted video-audio recording of the operations carried out by members of the electoral offices of the polling stations;
- ensuring that the minutes on recording the voting results at the polling stations are drawn up electronically, as well as the correctness of the correlations, according to the approved validation and control keys, between the data to be recorded in the minutes on recording the voting results;
- Ensuring the electronic signature of electronic minutes by means of electronic signature certificates provided by the Special Telecommunications Service;
- Ensuring the transmission of electronic minutes to the Central information System (SCPV);
- ensuring that the minutes on recording the voting results are taken in paper form and that the photographs are sent to the central information system.
- At the level of each Electoral Bureau of Circumscription, of each Electoral Office related to Bucharest districts and of the Electoral Bureau of district for Romanian citizens residing or residing outside the country, of a database with the voting results found by the polling stations offices (48 databases);
- The export from the databases of the contents of each report - verbally with the results of voting recorded at the voting station level and their verification with the original minutes for the authentication of data in the databases by the President and members of the electoral Circumscription offices, President and members of the electoral offices of the Bucharest district of Bucharest;
- Centralization of the voting results at the electoral office level and automatic collection of the minutes with the results of the voting in each county, sector of Bucharest City and the electoral district office for abroad;
- The central data base with the voting results of the about 19.000 polling stations in the country and abroad and the results of the centralization at county, Bucharest district and the electoral district office for abroad;
- Centralization at country level of voting results from all 19.000 polling stations;

- Populating the storage medium with pictures taken with the tablets of the minutes for all 19.000 polling stations and dates collected by each computer operator in the stations, as well as providing a user-friendly system of direct access to these data, according to certain criteria: county, locality, number of polling station, etc. in order to verify the correctness of the results recorded in the minutes submitted to the upper election offices,
- The creation of a database storage medium at polling station level with all the information contained in the minutes and a system of access to this data, in the .csv and .xml structure, which will also contain all the statistical statements obtained from the centralization of the election results;
- Security of system data, by means of methods and procedures which should be proof of correctness in the receipt and processing of information, in accordance with the legislation in force;
- The traceability of the data in the system, allowing the retrieval of the history, use or location of the information, by means of recorded identifications;

After the minutes have been sent from the polling station and after they have been scanned and checked at the top level, that is to the county electoral office in which they belong, the data are sent to the application for centralizing the election results. After verification, all minutes are automatically sent for real-time viewing, consultation and download on https://prezenta.roaep.ro/[5].

After all the data from all polling stations have been centralized, the minutes on the result of the vote and the corresponding minutes are generated from the SICPV application.

This application shall be certified for no change by a certification committee nominated by the order of the President of the Permanent Electoral Authority. The members of the commission test the applications that are used by the Central Electoral Office to centralize the voting results, establish the elements of their uniqueness (such as control codes) and then conduct several tests on the functionality of computer programs according to the technical specifications of the implementation.

SIMPV hardware hosts virtualization platforms that have computer services installed to receive, process, and respond to computer messages from applications running on the terminals of polling stations' election offices. The stack of software installed on the virtualization platform, operating systems, web servers, application servers, database servers, relies entirely on open source technologies under general or similar public licenses.

At the service infrastructure level, the system is built with a three-tier modular architecture where, for security reasons, it communicates only adjacent ones, i.e. level one by two and level two by three. To ensure availability, each tier has an active-active or active-passive cluster structure.

The computer system for monitoring turnout and preventing illegal voting is hosted in the data center of the Special Telecommunications Service and serves as a primary infrastructure and is also implemented a "discovery and business continuity" backup and recovery solution - DRBC" which is located in the data center of the headquarters of the Permanent Electoral Authority.

Replication and load transfer systems enable switching from the primary to the secondary system without affecting users, with the application running with short interruptions and the maximum switching time from the primary to secondary data center is 10 minutes.

2. CONTRIBUTIONS ON THE SECURITY OF EC IT SYSTEMS ARE USED IN THE ELECTIONS

[5] https://prezenta.roaep.ro/ - website consulted on 17.10.2020

A number of initiatives have been launched since 2018 to secure elections at national level in line with the recommendations of the European Commission for Democracy through Law of the Council of Europe ("Venice Commission"). Working closely with the election Management institutions in its 61 Member States and also dedicated its annual conference in 2018 to cyber security of elections. The recommendations that followed a unified approach to the security of elections, in particular by focusing attention on distance voting with a view to strengthening citizens' participation in voting.

Bearing in mind that electoral processes throughout the country involving the use of it tools at all stages dedicated to preparing, recording, counting and/or centralizing results, it is necessary to raise the level of preparedness and security of these events so as not to jeopardize the integrity of the electoral processes as a whole.

The right of voters to participate in elections in a direct, free and secret universal suffrage means that they are not prevented from voting, that their votes are not falsified, the options are not disclosed prematurely and the electoral process is not cheated by cyber attacks or other information technology.

Cyber threats, sometimes combined with disinformation as well as other hybrid threats, can become a reality in electoral processes and thus need to be aware of and reflected in planning assumptions and risk management when designing and implementing it systems that will provide operational support in elections.

As with any new solution, IT&C technology used in the electoral process must be introduced with caution, while ensuring that the digital solutions to be used meet the same legal requirements for elections as the other traditional non-digitized solutions, i.e. free, open elections, correct and based on secret ballot. While respecting these fundamental principles, technology can make a beneficial contribution to elections by complying with the general democratic rules set out in constitutional or electoral law.

Trust in the electoral process is fundamental to ensuring the legitimacy of the results and to ensure compliance with this principle, the electoral management authority must take the following measures:

- public oversight, together with entities responsible for ensuring and maintaining cyber security;
- observation of elections, including training of observers in electoral technology;
- publishing documentation and allowing access to the technology used in the elections;
- viewing and publishing the results of the elections in a way that is accessible and understandable to the public;
- open communication of cyber security risks before and during elections.
- educating voters and building public confidence;
- involvement of key opinion leaders;
- relations with the media and the education of journalists;
- building trust among cyber security experts, raising awareness and involvement of experts in testing systems for use in elections.

The occurrence of cyber-security incidents during the elections could significantly disrupt the democratic process in general and also lead to a loss of credibility of the democratic electoral system, the Permanent Electoral Authority and parties conducting electoral campaigns. Major incidents or incidents that are most likely to happen may pose the following threats:

- Unauthorized access to and/or loss of legitimate access to their it infrastructure;
- manipulation/falsification of the registration process of voters/electoral commissions and/or the counting of votes;
- theft of data, including sensitive data.

In order to ensure the above principles, thorough cyber security checks are necessary to ensure the integrity of all software components or devices used, of which we recall:

- check the firmware to be updated;
- management of changes in technical configuration (traceability);
- Continuous and adequate monitoring of network trafficto provide a real-time analysis of security alerts generated by network applications and hardware, it is necessary to implement a comprehensive SIEM information solution to search for malicious activities, using their logs and send alarms to system administrators;
- Ensuring strong protection against DDoS - denial of service attacks are an important part of all attacks against electoral technology, in terms of protection of platforms used to collect electoral information or publish results. Denial of service is usually achieved by loading the target machine or resource with unnecessary requests in an attempt to prevent certain legitimate demands from being met;
- access control - identification and control of users who have access to data or system and application privileges;
- strong authentication based on the following principles: something that the user knows (passwords), what the user owns (token, mobile applications, smart-cards) or something that the user is (biometrics);
- checking data integrity and securing data transfer - data transfers are potential trade-offs, control amounts and digital signatures being useful tools to ensure data integrity;
- ensuring the segmentation of the network used for computer systems supporting electoral processes, which will ensure that processes that do not have to be accessible to the public, in particular centralization and counting of votes, can take place in an environment physically isolated from other public trials. Network segmentation can be achieved either by logical separation (VLAN) or by physical separation;
- provide back-up and recovery procedures from central systems that must be installed in secure locations where physical access will be verified and restricted.
- The provision of an alternative location that is available to enable business to continue in the event of a disruption of any kind, with adequate pre-reserved and ready-to-operate equipment at any time and complying with the same standards and requirements as the original system;
- duplication of secure communication channels.

In order to be ready to prevent cyber security crises, the Permanent election Authority has requested at government level and has obtained the creation of a working group with expertise in IT&C security and election technologies, the scopeis to develop instructions and methods for preparing elections and to ensure interinstitutional cooperation in this field.

The working group will have a 24/7 format support program during election periods, and the main tasks include coordinating cyber defense and managing crisis events. The working group will be composed of the technical staff responsible for cyber security nominated by the AEP leadership for this purpose, information Security Service personnel, as wellas national government teams acting as CSIRT-computer Security incident response team at our country level.

One of the main roles conferred on the working group was the testing and auditing of information systems and networks supporting electoral processes, which were considered as the cornerstones of network and information system security and the only means of achieving a practical assurance of functionality and security. Testing and auditing have therefore been adopted as comprehensive and multi-faceted approaches, with critical systems being tested by at least two independent teams, analyzing the connections between applications and conducting system penetration tests.

During election periods, the working group will carry out functionality tests, unit tests, and loading tests of it systems, which will focus on the answers the system gives, in terms of doing what it needs to do and giving the expected response from the data processing.

System security tests will be performed, which will focus on ensuring that systems cannot be compromised by forcing them to act in undesirable or altered ways. The problem with these

functional tests is that there is often an endless list of assets, conditions, and circumstances to test to see if the system is performing in a faulty way, limiting their effectiveness.

Another set of tests that the group will have to do is vulnerability scans, which are a specific and simplified form of security testing for "known" cyber vulnerabilities that are documented globally by all companies in the domain of cyber security. Vulnerability scans will be made with software specially developed for such activities that have the universal vulnerability libraries in place. These tests are generally useful for testing infrastructure security.

Penetration testing combined with organizational tests and audits and system tests will also take place. This type is one of the final security tests, which are done with experienced testers, allowed to try to attack network systems and computer systems that are used in electoral processes "by any means necessary".

In these extensive and creative tests, testes are trying to imitate real attackers using multiple combinations of attack methods. These penetration tests can be very useful to reveal the weaknesses of the system, in its entirety, in terms of system organization in general, system configuration, network connections and ancillary systems. Penetration testing results depend on the creativity and abilities of testing and their final penetration reports suggest solutions identified to reduce the number of vulnerabilities, especially those known.

In setting up the working group, the following principles have been taken into account, documented and disseminated to all actors involved in the conduct of the activities, through documents and procedures:

- providing a single point of contact at national level;
- creating a scale of crisis escalation detailing the type and level of criticism;
- creating a clear division of roles and responsibilities;
- creating secure means of communication;
- ensuring full documentation of the systems that are used as support for electoral processes;
- ensuring the flexible allocation of resources, both financial and human;
- an adequate training plan for all members of the group.

In the geo-political context of our country, cyber security in elections is considered with responsibility by the Permanent Electoral Authority, which is working to improve this area at all times. Thus for a better understanding and implementation of this concept, as well as for defense against this scourge, the institution has started and has ongoing long-standing partnerships with all the Romanian state institutions that play the role of operational centers for response to cyber security incidents, to monitor cybersecurity incidents, analyze the impact of cyber security incidents, respond to cyber security incidents and verify the level of cyber security for the products or information systems to be used in the networks used in the choices.

In addition to this, employees appointed by the management of the AEP to ensure the security of information systems, regularly participate in training in cyber security technologies, product or service presentation, colloquia and attack and defense simulations, in order to be aware of this highly dynamic area, given the real threats of cyber-terrorism to which the electoral field is exposed.

2.1. METHODS AND TECHNIQUES TO IMPROVE THE CYBER SECURITY OF SYSTEMS IT USED IN ELECTIONS

Under the legal provisions in force the Permanent Electoral Authority must provide the computer and communication applications and equipment necessary for the computer system to monitor turnout and prevent illegal voting, audio-video recording of the operations carried out by the members of the electoral offices of the polling stations for counting votes after the closure of the stations, the information system for the centralization of the minutes, as well as the photographing of

the minutes on recording the voting results, and the technical assistance necessary for all these systems, support and training for the entire set of election officials using this infrastructure.

In order to ensure cyber security of information systems containing the tools, procedures and technologies used in elections, technical measures should be adopted at each election event at the level of the Permanent Electoral Authority, the ec needs to be adapted to the legislation in this area that is then in force and implemented as appropriate, circumstances and needs.

In this sub-chapter, we will propose a set of cyber security measures, which may take the legal form of general instructions and be adopted at any electoral event, related to the administration, management and use of information systems to be used in elections, the ec will contain a set of rules and rules to be observed in order to ensure the real and correct results of the elections in general and the security of the information system in particular.

The generally valid rules that should guide the preparation of the instructions, as definitions of cyber security, will concern:

- prohibition of unauthorized persons' access to computer equipment or applications that are used as support for electoral processes;
- methods for securing computer applications;
- methods for securing databases to prevent unauthorized reading, copying, modification or deletion of data media;
- rules for the use of automated data-processing systems;
- logging of data-changing operations in systems used in elections;
- the methods of securing data communications serving information systems;
- the protection of personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and against any other unlawful form of processing.

In order to define the principles that will be used to draw up safety instructions, we define the following terms as the reference:

- Confidentiality - access to information associated with the information system is allowed only to authorized persons, applying the "need-to-know" principle;
- Integrity - ensures accuracy of information generated, processed, stored, archived or exported to/from information systems, and processing methods;
- Availability - the ability to provide authorized persons with access to system-related information, resources and services when requested;
- Identification - the ability to establish the identity of a person before any operation carried out on a computer system;
- Authentication – the ability to confirm the identity of a person in relation to the system;
- Authorization - the process of granting a person access to data, software or information systems.

The information system which the Permanent Electoral Authority together with the Special Telecommunications Service (SRI) make available to the Central Electoral Bureau (BEC) to be used as support for the electoral process is made up of:

- The central information system containing high-performance processing, storage and communication equipment that will operate in the AEP data center with redundancy in the STS data center;
- The web-based computer application for the verification of voting rights;
- The web-based computer application for the consolidation and verification of the minutes;
- Technical support center;
- The communication infrastructure which is a VPN network in a private, secure communications environment, to be used to access the information system by workstation operators in all electoral offices;
- Tablet-type computer terminals to be used in polling stations and in mail-voting bureaus,

- The work stations in all electoral offices dedicated to the verification and centralization of data and voting results.

The central it system shall collect, record, organize, store, delete and destroy all types of personal data and other categories of data and information falling within the following categories:

a) System input data:
- Permanent electoral lists in the country or abroad, depending on the type of elections taking place;
- The list of persons who have been prohibited from voting;
- The register of voting stations;
- The list of computer operators at all polling stations;
- Data taken from identity documents during the voting process;
- Data on the signatures of persons voting abroad as well as the signatures of the section presidents, depending on the type of elections being held;
- Data taken by scanning the barcode used on the envelope for mail voting;
- Audio-video recordings at all polling stations that are organized with the vote counting process;
- Data entered by computer operators at the polling stations in the correlation and verification key verification forms in the minutes of the observation of voting results;
- Pictures of the minutes, which have been drawn up on paper and which are sent for centralization;
- Calls made to the support Center;
- Monitoring data on the operational status of the communication infrastructure terminals and equipment;

b) Data stored on the system:
- CNP, surname, first name, ID of the polling station, county, number of the polling station, position of the person on the list and type of electoral list,
- audio-video recordings of the vote counting process at the polling station;
- the data from the correlation and verification keys form in the minutes to record the voting results;
- documents in .pdf format with data for electronic minutes and photographs of the minutes drawn up at the polling stations in paper format,
- operational data on turnout;
- data on operations by computer operators;
- Decisions amending the minutes of the presidents of electoral offices, scanned in PDF format;
- minutes signed by representatives of the electoral offices in their original and/or amended form;
- minutes with aggregated results per county;
- system generated reports containing in aggregate the history of the minutes entered into the system from the end of the vote until the validation by electronic signature of the qualified certificates of the presidents of the electoral offices;
- technical data: cyber security events/incidents, records and call logs to the technical support center, computer system access logs, data contained in notifications and tickets opened in the technical support center, web server and database logs serving notifications in the technical support center, logs of the maintenance processes carried out on the computer system components, logs of faulty or inoperative tablet replacement operations;
- data to monitor the operational status of the components of the information system;

c) System output data:
- statistics with turnout at the voting station level and centralized by territorial administrative units up to the country-wide level;
- data on the results of the vote for publication on the dedicated website;

- data on the minutes needed to enter the minutes of the centralization of the results of the vote;
- system generated reports containing in aggregate the history of the minutes entered into the system from the end of the vote until the validation by electronic signature of the qualified certificates of the presidents of the electoral offices;
- printed documents with the information sent from the polling stations' tablets, the correlation checking forms in the minutes concerning the establishment of voting results and the images of the paper minutes;
- data on audio-video recording at polling stations for storage;
- notifications made available to the Ministry of Internal Affairs on possible election fraud attempts,
- Other data and statistics requested by the Central Electoral Bureau.

A policy on roles and permissions in the information system will need to be strictly defined, allowing it system users to be strictly able to access the information needed to perform their duties. This will establish by rules the categories of users, responsible for implementing security measures, coordinating the implementation of operational procedures, training of staff in the order and checking the implementation of procedural measures, as well as the maintenance of all components of the it system within their area of competence.

The types and roles according to tasks and responsibilities to be defined are the following:

a) The it system coordinator, who will be responsible for coordinating all activities concerning the implementation and management of the it systems used in the elections;
b) The administrators of it systems that will provide operational support for elections, which will be in charge of drawing up internal procedures in accordance with the legal provisions and the instructions adopted by the Central Electoral Office, ensuring their implementation, as well as maintaining the components they manage. The categories of component administrators are:
   - Central information system administrators;
   - It system administrators for verifying the right to vote;
   - The administrators of the it system for collecting the minutes
   - Technical support Center administrators;
   - Data communication infrastructure managers;
   - It terminal managers, tablets, voting stations
c) The computer operators who are required to use the calculation technique and the equipment with which they are equipped, in accordance with their training and instructions received for this purpose, according to their technical duties and their area of responsibility, are:
   - Designated computer operator in the polling station or reserve operator;
   - Computer-operator Member at polling stations abroad, depending on the type of voting being held;
   - A user who will be granted to the employees of the national Statistics Institute who process data in the higher electoral offices;
   - President of the County Electoral Bureau or of the Central Electoral Bureau, who will be able to sign electronically the documents on the validation of the summary minutes and generate the final minutes;
   - Application Manager designated by AEP;
   - Operator in Technical support Center.
d) Technical managers, who will be responsible for activities aimed at maintaining computer terminals, tablets in polling stations, as follows:
   - Computer specialists who are staff proposed by local public authorities who are trained and evaluated to provide rapid intervention and technical support at polling stations;
   - Specialists of the Special Telecommunications Service who are designated at central and territorial level to operate in the technical support center.

e) It experts designated by the political groups under the conditions set by the decision of the Central Electoral Bureau (BEC), who are in charge of checking the integrity and correctness of the whole process, which is carried out through the information systems used for elections.

A series of security measures will need to be implemented across the it system to ensure that the objectives of confidentiality, integrity, availability, identification, authentication and authorization of all actions and transactions carried out through the systems are met, as follows:

a) Encryption, identification, authentication and authorization measures shall be implemented in order to ensure the confidentiality of data being traded or stored through the information system, structured into the following categories:
   - information resource management;
   - physical access control;
   - operations management;
   - communication and it resources management;
   - technical access control;
   - staff training;
   - audit.

b) In order to ensure the management of information resources associated with the information system, the following measures shall be implemented:
   - identification and inventory of all communication and information resources to be used for each component of the information system;
   - the establishment of all physical locations for the functioning of the it resources to be used;
   - the determination of a responsible person, holder or temporary delegate for each resource put into use, and their rights and responsibilities.

c) The following measures shall be implemented to ensure access to and control of physical access to the premises hosting the it system equipment:
   - In the spaces provided by the Special Telecommunications Service and the Central Electoral Bureau, internal rules on physical security will be applied and observed;
   - In the spaces provided by local public authorities, Ministry of Foreign Affairs, access control will be provided in accordance with legal provisions by the representatives of the Ministry of Internal Affairs;
   - the equipment that will be installed to provide data communication services, necessary for the polling stations, will be handed over on the basis of minutes to the staff designated by the legal officials of the premises where polling stations or higher election offices are organized. Their physical protection will be ensured through the care of the legal officers and representatives of the AEP;
   - The computer equipment of the information system will have access only to the staff authorized by the Special Telecommunications Service or by the Permanent Electoral Authority, to be appointed for this purpose;
   - The tablets in the polling stations will have access to computer operators, who will be trained and authorized by AEP for these operations;
   - other staff, within technical or emergency response structures, may only have access to the premises hosting it resources with appropriate approval, under permanent supervision and only after identification under the access permit. These persons will be kept in specific registers;
   - access to equipment, data and information generated, processed, stored, stored or transferred to unauthorized personnel by means of the information system shall be strictly prohibited.

d) The following operational measures will have to be implemented to ensure the management of operations carried out through the it system:
   - The provision of access to information in the information system for legal beneficiaries will be carried out in accordance with decisions or instructions to be adopted at the level of the Permanent Electoral Authority;

- Third-party external audits of the system will be able to be carried out in accordance with the regulations or decisions issued to that effect by the AEP and in compliance with the general security rules;
- Data on cyber security incidents will be transmitted to third parties in accordance with the rules established by the Central Electoral Bureau;
- data intended for authorized third parties will be encrypted, electronically signed and transported through removable storage media. The work will be mentioned in a handover/reception report.
- Data to be made available to authorized third parties over communications networks will be transmitted through secure channels such as IPSEC, SSL/TLS, HTTPS, etc.
- the use of unauthorized removable storage media in information systems shall be prohibited.

e) The following operational security measures will be implemented to ensure data management for the it resources to be used within the it system:
   - the communication infrastructure associated with the it system for the secure transport of tablet data from polling stations to the application servers of the central information system will be provided;
   - Secure transport communication infrastructure will be provided between the data centers of the Special Telecommunications Service and the Permanent Electoral Authority where IT&C equipment supporting the functioning of the information system is hosted;
   - The communication infrastructure for the secure transport of data from electoral offices to central it system application servers will be provided through a virtual private VPN network;
   - this appropriation is also used to cover the union's financial obligations under the EuropeanUnion guarantee for union financial instruments in the form of guarantees for union's financial interests and the union's financial interests.
   - a tablet cannot be assigned to two or more polling stations at the same time, but depending on operational requirements, multiple tablets may be assigned and assigned to one polling station;
   - this will ensure the stations for centralizing the voting results in the electoral offices and will be managed and managed in a centralized manner;
   - the communication infrastructure will be provided using its communications networks or via communication networks provided by public operators via rental;
   - local it equipment will be managed using the console cable, or remotely via the equipment management network using secure protocols;
   - Encrypted communication will be provided between management stations and technical equipment using secure protocols: SSH or SSL/TLS;
   - Connection and access to the information system of workstations used at AEP/BEC level will be ensured according to security rules and policies established by security instructions;
   - Provide encrypted communication at ISO/OSI Layer 2 of the stack between AEP and STS data centers using MACSec;
   - Tablet authentication to WIFI interface communications equipment at polling stations shall be done using WPA2-PSK (WIFI protected access 2-PreShareKey);
   - Communications between tablets and WIFI access points at polling stations will be encrypted using the AES algorithm with a minimum of 128-bit key;
   - WPA2-PSK beliefs will be generated at random and will be introduced and stored on tablets and communications equipment by staff designated by the Special Telecommunications Service;
   - The disclosure of WPA2-PSK beliefs to unauthorized persons will be strictly prohibited;
   - Communication equipment to be installed at polling stations will have Firewall-type mechanisms to prevent unauthorized access to the communication services provided by them;

- the correlation between the tablet series, the voting station number and the beliefs of the tablet operator in the polling station will uniquely authorize each tablet to access the computer system;
- the authentication between the tablets in the polling stations and the central information system will be done simultaneously using individual digital certificates and the beliefs of the tablet operator;
- the beliefs will be associated with the polling station and can only be used from the tablet associated with that station;
- credit will only be able to be used in the system if they have been allocated in advance at a polling station;
- the data stored in the database on the electoral process tablets in polling stations are encrypted using an internal stored key, not directly accessible by a user;
- the installation of unauthorized applications will be prohibited on tablets;
- Communications between the tablets in the polling stations and the central it system will be encrypted using the HTTPS secure protocol;
- technical measures will be implemented to prevent malware infection by updating operating systems and applications, implementing security updates, scanning with antivirus software, implementing anti-malware protection measures, Implementation of IDS/IPS or communication filtering solutions specific to each component of the information system;
- tablets will disable all services that are not necessary for the operation of the central information system and the technical support center;
- communication equipment installed at polling stations will be continuously monitored during the electoral period by designated technical managers through dedicated applications;
- equipment status and all maintenance performed by administrators will be logged and saved to log files.

f) To provide access to the information system and technical access control shall be implemented as follows:

- the staff who will technically manage the information system will be provided only by specifically designated specialists;
- staff will be appointed as an application administrator who will be able to check application logs and operations with tablets at polling stations;
- AEP and BEC staff to be designated for interrogating databases and logs will be identified by trust of access;
- technical management can only be done by authentication and authorization, locally via the management console or remotely, via the dedicated management network, using secure protocols;
- no direct connection will be allowed through the dedicated management network using full user account;
- Authentication of each Central information System equipment Administrator will be done using asymmetric cryptography, using SSH private key;
- for the other cases, identification and authentication of staff with authorized access to the equipment or applications that make up the computer system will be based on a strong user name and password;
- tablet access passwords for designated computer operators and backup operators will be generated randomly and handed in on paper in a sealed envelope;
- remote access to communication and security equipment in the information system will be blocked for a period of 5 minutes after mis introduction of access credit, 5 consecutive times, for the administrator concerned, in all possible situations;
- the 10 consecutive wrong entry of credit creditors on a tablet at a polling station shall be automatically notified at the technical support center;

g) To ensure the efficient and secure use of the it system, it is necessary to train all authorized staff who will manage and operate the system according to their roles and responsibilities, who must achieve the following objectives:
   - ensuring the application of security, integrity and availability measures for computer data processed and stored by the information system;
   - ensuring the protection of personal data exchanged through the information system;
   - ensuring the technical management and operation of the components of the information system, subject to compliance with security requirements;
   - acquisition of rules and restrictions on the use of it resources for purposes other than those for which they were allocated;
   - The training of management-related personnel designated by AEP and BEC for interrogating the application and equipment databases or logs shall be carried out on the basis of a formalized procedure.

h) Ensuring the system audit work to be carried out in order to minimize security risks to the information system and ensure its functioning in accordance with security measures will pursue the following objectives:
   - the technical, operational and procedural measures associated with the information system will be subject to security assessment;
   - the logs associated with the services necessary for the proper functioning of the it system will be ensured and analyzed as follows: web services, database services, calls and tickets in the technical support center, the logs of operations carried out by tablet operators at polling stations via the right to vote application and all activities carried out on the central information system equipment;
   - Logs associated with the it system services will be accessible by third parties in accordance with the applicable legal rules or decisions of the AEP;
   - security incidents will be reported hierarchically to the it system coordinator.

i) Operational and security measures shall be implemented before, during and after the end of the voting process in order to ensure the integrity of the information to be managed and stored in the information system and shall include the following:
   - data integrity measures prior to the use of the information system:
     - the input data will be sent to the computer system level together with a mechanism to verify their integrity;
     - It will be checked in advance that the data imported into the central information system is the same as the information provided in the electoral register;
     - verification that the system generated reports containing the aggregated history of the minutes entered into the system from the end of the vote until validation are electronically signed with the qualified digital certificates of the presidents of the electoral offices;
     - the computer operator will verify the data transmitted on tablets before the start of the electoral process according to the procedures to be given to him at training sessions;
   - measures concerning data integrity during the use of the information system:
     - check that the data transmitted from the tablet in the polling station, relating to the minutes of the record of voting results, is electronically signed using the digital certificate associated with the terminal;
     - technical and security measures will be implemented to prevent the intentional or accidental deletion, corruption, freezing or alteration of computer data or misuse of information within applications, both at tablet and central information system level;
   - measures concerning data integrity after use of the information system:
     - All documents associated with the it system, technical project, instructions, procedures, etc., will be managed in accordance with security measures adopted at the level of the BEC and the legislation in force;

- When handing over SD tablets and cards by operators at polling stations, the names and size of the audio-video files taken will be given.
- audio-video recordings at polling stations will be protected from alteration using cryptographic hash functions.

j) Ensuring the availability of information to be traded and stored through the information system will be ensured by implementing the following operational and security measures:

- business continuity management:
  - the creation of back-up copies necessary to restore the information system will be ensured and stored in spaces where appropriate security measures will be implemented;
  - Business continuity will be ensured mainly through the existence of two central it systems, installed in redundant configuration, one of which is a principal, installed on AEP and one secondary, backup, installed in the STS information and communication center. If the main system is preserved, the solution will allow the instant transfer of activity to the secondary system, on which the central application will be installed and the database replicated;
  - ensure that the information contained in the databases of the main and backup information system is synchronized as soon as possible in order to avoid loss of information and disruption of the process of centralization and counting of votes;
  - backup copies of equipment configurations of the database contents needed to restore the it systems for their proper functioning will be saved;
  - real-time copies of database and application logs will be made to technical equipment hosted in the data center;
  - regular back-up of data used in the information system will be carried out;
  - minimizing the impact of interruptions to the it system will be as follows:
    - real-time redundancy will be provided for critical systems within the central information system, the data communication infrastructure and the technical support center;
    - the necessary human and material resources will be allocated throughout the electoral processes, for all activities, including the replacement of inoperable tablets in polling stations;
    - the right to vote check application will need to allow the voting process to take place when the tablet is online as well as offline. Information acquired in offline mode will automatically be transmitted to the server when the connection between the tablet and the central computer system is restored;
- security event/incident management:
  - identification, reporting and response to security events/incidents will be ensured in accordance with applicable regulations;
  - security incidents will be reported hierarchically to the it system coordinator as soon as possible;
  - The it system coordinator will report security incidents to the AEP and BEC leadership.
- the maintenance of the communication infrastructure, information systems and applications shall be carried out by specialized personnel trained and authorized to do so by maintaining the equipment, operating systems and applications making up the information system, in accordance with the procedures and instructions for the management and maintenance of the equipment manufacturers, the software or licenses;
- monitoring and evaluation of it system audit logs:
  - technical managers will be given the power to monitor and analyze specific audit logs in order to ensure availability;
  - Cybersecurity events and incidents will be logged and monitored at the level of the operation Center for Security incident response - CERS-STS, in accordance with applicable regulations;

- The logs that will be generated in real-time, both applications and physical or virtual servers will also be accessible by third parties for analysis, based on AEP and BEC decisions.

BIBLIOGRAPHY

1. council conclusions on cyber activities,https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/ro/pdf , website consulted on 20.09.2020
2. https://eurlex.europa.eu/legalcontent/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO, website: 20.09.2020
3. https://www.roaep.ro/legislatie/wp-content/uploads/2020/09/L208.pdf, website: 23.09.2020
4. https://lege5.ro/App/Document/gm4dsobvhaya/regulamentul-de-organizare-si operation-a-authorities-permanent-DIN-26102020, website consulted on 02.11.2020
5. https://www.votstrainatate.ro/, website: 02.11.2020
6. https://prezenta.roaep.ro/ - website consulted on 17.10.2020
7. www.roaep.ro – site accessed on 05.11.2020
8. http://www.primulvot.ro/, website: 23.09.2020
9. https://bec.ro – website consulted on 25.09.2020
10. https://finantarepartide.ro/wp-content/uploads/2020/08/Legea_334_2006.pdf - website consulted on 25.09.2020
11. http://www.roaep.ro/legislatie/wp-content/uploads/2016/01/HG_10_2016.pdf - website consulted on 25.09.2020
12. https://finantarepartide.ro – website consulted on 25.09.2020