Synergy in Innovation and Performant Management at the Government Level

Marius STEFAN[1]
Cristian BRANCU[2]
Oana TURCU[3]
Madalina POPP[4]
Catalina Alexandra NEDELCU[5]

Abstract

National security is that state of equilibrium, legality, economic, social and political stability that guarantees the existence and development of the sovereign, unitary, independent indivisible state, through order, rights and civil liberties.

National security leads to the achievement of continuously evolving values, guided by constitutional-democratic principles. The national interest becoming the fundamental thesis in applied foreign policy. Security policy is represented in the long-term organization, and ensuring safety change and innovation. Security strategies, thus succeeding in the adoption of measures that counteract the threats that evade the security state. A strong nation is built through shared norms and values, goals and aspirations, of greater importance than individual interests. The protection of the citizen represents a vision, an integral and important part of the National Strategy for the Defense of the Country. Since ancient times, networks have provided basic structures for the development of the economic-social system in various areas of the world. In the 20th century, telecommunications networks were added to them, which allow overcoming several barriers of time and space, as well as access to new frontiers of human interaction.

Focusing on prevention and preventive mechanisms in the sphere of national security and defense of the country, respectively better anticipation, knowledge, but also the achievement of an integrated, balanced, flexible and agile reaction capacity. In the current context, in addition to knowing the risks and threats, under all aspects - sources, forms of manifestation, means, techniques - the development of the ability to anticipate, based on knowledge and education, is fundamental. For this purpose, the development of appropriate systems for the timely discovery of dangers, risks and threats, in the perspective of preventing their occurrence, through the combined use of both military means and civilian instruments, is mandatory, as well as the allocation of resources through a integrated, continuous, multi-annual and rigorous planning process, capable of meeting both the new inter-institutional planning requirements, at the national level, and the rigors of the multi-annual budgetary planning principles specific to the North Atlantic Alliance and the European Union.

[1] Marius Ștefan, Bucharest University of Economic Studies, Romania, marius.stefan@mfe.gov.ro

[2] Cristian Brancu, Bucharest University of Economic Studies, Romania, cristibrancu2018@gmail.com

[3] Oana Turcu, Bucharest University of Economic Studies, Romania, ardesbio@gmail.com

[4] Madalina Popp, Bucharest University of Economic Studies, Romania, madalinarusu13@yahoo.com

5 Catalina Alexandra Nedelcu, Bucharest University of Economic Studies, Romania, catalina.nedelcu@fabiz.ase.ro

Keywords: *synergy, innovations; intelligent technologies; e-business; digital transformation; awareness; information management; electronic management.*

JEL classification: O1, O2, O330, D83, O10, O11, K24

DOI: 10.24818/RMCI.2024.3.595

1. Introduction

Information and communication technology has a complex impact not only on the economy and its efficiency, but also on all aspects of people's lives. For a reinvention of governance in the information society, the following concepts have been identified that should be fulfilled:

- increasing the state's capacity to absorb European funds through the use of new technologies.
- increasing the capabilities of government administrations in public policies, both at the national and European level.
- electronic democracy – the internet can increase democratic participation in governance, the citizen of the information society is active.
- the electronic citizen – the citizens of the new society/ young people are drawn into modern technological fields being the key actors of future governments, politics in the digital age is in continuous transformation.
- politics in electronic format - the manifestation of politics in digital form is becoming more and more visible through the significant increase in online electoral campaigns, the electronic state and behavioral patterns.
- the electronic state - in the phenomenon of globalization fueled by the digital integration of the new economy markets, it will be necessary to rethink and redefine the concept of the nation-state.

Thus increasing the chance of creativity and innovation, by profoundly transforming citizens' behaviors and profiles, from reactive to proactive.

The social dimension of the information society is undoubtedly one of the most important facets of the new model of society and must be treated with great care to minimize risks and maximize potential benefits.

Science has made possible the technologies on which the information society is based, and the needs of the scientific community have often led to innovation in information technologies, today benefiting from the Internet and World Wide Web domains.

Science is systematized knowledge, which includes derivative activities such as: scientific research, technological development, technology transfer and innovation.

In the technological age, action plans and policies are drawn up to meet the challenges, the most important technology being ICT, which enables the processing and circulation of information in a revolutionary manner.

We thus identify the key terms that dominate the world we live in today: information, communication, knowledge. The information society is considered to be the knowledge society based on ICT. The technologies of the information society will evolve in the direction of being within reach of the knowledge process, that is, of storing, transmitting and generating knowledge. Knowledge is the result of the information management process, of enormous importance in the global information society, by: supporting innovation, promoting economic development, making decisions in an transparent way, at government level, in central public administration.

2. Literature review

Achieving the performance of the public institution calls for a heightened concern for innovation, creativity, change. Successful leaders in the public institution will have the responsibility to create an institutional culture, employees being encouraged to seek new ideas, to build relationships of mutual trust, to create a climate in which to learn from each other. The efficiency of a leader does not depend only on his own abilities, but also on the involvement, support and participation of the entire team.

Precisely for this reason, the leader in the local public administration must be in a permanent dialogue with the people, to communicate his own vision, so that they can notice the opportunities and form an image of the future. This new perspective on human behavior emphasizes the importance of social needs, attitudes and meanings that guide people's actions, even more so within public institutions.

In the public administration of other European countries, leadership represents a way of mobilizing those who work in public institutions to be more receptive to the public, that is, to the citizens, and more intensively involved in designing and providing services to the public.

Therefore, in their view, leadership is a means of revitalizing public services. The leader is asked to focus on the organizational implications, on his potential to motivate the entire workforce, all employees.

Thus, the role of the leader in the formation of the organizational culture is major, as he is the one who promotes the values in the collective, and not at the individual level. In other European countries, special emphasis is placed on responsibility and cooperation within the public administration, which is why leadership is also given special importance, precisely in order to succeed in achieving all the objectives within the public sector.

In this sense, new institutions were established with the objective of identifying future leaders within the administrative sector and for the purpose of their professional development. Leaders, within public institutions, can help to spread, promote and maintain the new values that are necessary for a successful public sector reform.

While public leadership clearly includes public administration leaders as well as political leaders, the vision of leadership in the future tends to become broader. It includes leaders as change agents spread throughout public organizations to continue the reform process. Leaders prove to be effective through their ability to persuade, motivate public employees and direct their efforts towards a common cause.

Noting at the level of the institution, the emergence of the need for cyber security, by securing the application, starting from the transfer stage of the IT equipment hosting location, in a more secure data center specialized in the field.

These IT events created the premises for the transfer of the development activity of IT services and applications intended for European funds from the private environment of expertise through contracting on the basis of public tenders, to the public environment of inter-institutional cooperation with the related specifics, based on protocol relations established by law.

The management of the equipment that stores and administers information about the submission, contracting and implementation of projects financed from European funds, outlines a character of a strategic objective, of national importance manifested in this way and through the well-defined collaboration between the institutions involved.

In order to develop and host computer applications, cooperation agreements will be defined with the autonomous institutions that have attributions in the field of computer security in Romania: Special Telecommunications Service (Protocol of 05.12.2012 regarding the provision of communication services and technical assistance for the management of the computer infrastructure, between STS and the Ministry of European Affairs - ACIS (Ministry of European Funds), for specialized hosting and the Romanian Information Service for the purpose of cyber defense of critical infrastructure of national interest.

The decision-making transparency in the management process of the submission of projects related to European funds, such as evaluation, contracting and their implementation, will always be achieved much better, in electronic form, implicitly requiring a high degree of cyber protection and security, only in this way will it be reduced drastic and beneficial the current high degree of excessive bureaucratization in the public administration. Transforming governance into an efficient, automated activity, in which to receive the result obtained, especially in a sensitive field with complex implications such as that of European funds.

3. Emerging technologies in a secure cyber infrastructure

The computer applications intended for the management of European funds, were made as a necessary measure to increase the degree of absorption of European funds, by streamlining the management of document flows, using capabilities of computer applications and new technologies, as a calculation technique, thus succeeding, notable first steps in the continuous computerization process of the central public administration.

In the programming period 2007-2013, at the level of 2010, the management of computer applications intended for European funds was carried out in a decentralized manner, each operational program having its own form of computer organization, which also included an computer application with specific characteristics of the related program. POSDRU was a pioneer in the electronic submission of projects.

By means of an IT application, excessive bureaucracy was thus reduced, eliminating the submission of hundreds of documents related to eligible projects and expenses. In the relationship between the project beneficiary and the Management Authority, an electronic communication is established that will make the absorption process more efficient, but not without encountering difficulties or blocking stages in the evolution process, thus replacing the thousands of bibliographies submitted with files uploaded electronically in an account for each project. Within the POSDRU Management Authority, the staff dedicated to the management of European funds use the following software applications dedicated to the monitoring and reporting of programs with non-reimbursable financing:

a) The ACTIONWEB application is a computer system for completing and submitting the funding request, a web application, database (PostgreSQL) developed for the purpose of managing funding requests, submitted in the framework of requests for project proposals launched through POSDRU 2007-2013. The application allows the configuration of several roles: public user, management users, application administrators, general administrator, each with specific permissions. At the moment, the ActionWeb system is not provided with an audit module for the operations performed by the system users.

The ACTIONWEB application is an IT system for beneficiaries and possible beneficiaries of ESF projects, a web application, of databases developed for the management of funding requests, submitted as part of the requests for project proposals launched through POSDRU 2007-2013, by beneficiaries and possible beneficiaries of ESF projects.

Since at the moment the ActionWeb system is not provided with an audit module of the operations carried out by the system users, it is necessary to develop an update module for the partners, the beneficiaries of FSE projects, because in the implementation process, such changes take place in at the moment, only on paper level, not reflected in the records of the ACTIONWEB database. The application database was hosted in 2010 by a private entity under contract. As a result of some cyber attacks, the decision was made to transfer the application based on protocol and it is hosted under security conditions by the Special Telecommunications Service in a specially organized data center.

b) The ASEP computer system aims to improve the analysis process, by taking over funding requests from Actionweb, defining the committees and evaluation grids specific to each project proposal request, effectively completing the evaluation grids, coordinating and monitoring the evaluation process for that the grids are complete, correct and consistent. Access to the system is carried out only with a username and password depending on the permissions granted. The application database was hosted in 2010 by a private entity under a contract.

It is a web-based application, with a user friendly interface, whose database allows the generation of specific reports for different work situations. As a result of some hardware malfunctions of the computer equipment, repair and replacement interventions were carried out together with the representative of the brand in Romania for the equipment not in proper operating condition in the normal efficiency parameters. Thus, the decision was made to transfer the application based on protocol and it is hosted under security conditions, by the Special Telecommunications Service.

All project evaluations, related to the period 2010-2014, were carried out electronically within this computer application, but the equipment that hosts the software used, has been put into operation since 2006, so it no longer benefits from warranty, support or maintenance, a fact that constitutes a situation of possible blockage and vulnerability in the management of documents related to the evaluation of projects, as well as a possible exploitation in case of cyber attacks, due to the outdated technologies used.

c) The SIM POSDRU application is an application in progress, which intends to unify the ACTIONWEB and ASEP applications in order to create analytical reports and define an electronic flow of documents created, signed and approved within AMPOSDRU. The application database was hosted in 2010 by a private company under a contract.

The SIM POSDRU application is an application created in accordance with the informational structure of AMPOSDRU, based on the predefined document flows, declared in the AMPOSDRU procedures, through which the unification of the ACTIONWEB, SMIS-CSNR and ASEP applications is achieved at the informational-operational level. The compatibility of the databases, owned by each of the mentioned applications (SIM POSDRU, ACTIONWEB, SMIS-CSNR, ASEP), as well as the tabular structure, the data entry modules, currently delay the process of relating the data that must be correlated and transferred in order to generate reports in SIM POSDRU, using information created by the other IT systems.

SIM POSDRU complements SMIS-CSNR, developed by the Authority for the Coordination of Structural Instruments (department within the Ministry of European Affairs), which covers part of the information and reporting requirements to the European Commission. User access to the POSDRU SIM system is made only from the INTRANET.

As can be seen from the diagram below, user access to the system is made through a Juniper SRX240 hardware device. The connection is TLS 1.0, encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as a key change mechanism. There are 2 LAN zones and a DMZ zone. There are 3 cars in the DMZ area:

- KEMP – hardware equipment with the role of balancing, https/http decryption/encryption, request verification, etc
- PS – process server – integrates the SIM POSRDU system with other applications (ActionWeb, ASEP, SMIS..)
- 2xIHS – IBM Http Server – proxy server (Apache) node balancing role IBM Websphere Portal and IBM Websphere Application Server.

These applications are also used by 3 national and 8 regional structures - OI POSDRU. In order to grant the access rights to the applications and the permissions associated with them, each of the AMPOSDRU / OI POSDRU employees must follow an operational procedure. This includes a visa from the employee's superior and a description of the access granted, and their operationalization is carried out by the IT managers within AMPOSDRU.

Regarding the security measures of the IT system, actions were started to improve and optimize the existing applications:

a) the direct acquisition procedure for obtaining digital certificates for AM / OI personnel who have access to the IT systems at the POSDRU level has been completed

(ActionWeb, SIMPOSDRU, ASEP), to establish the procedure for beneficiaries and potential beneficiaries;

b) the servers with the ActionWeb, ASEP (project selection computer program implemented at AMPOSDRU / OI) and SIMPOSDRU applications are co-administered by the Special Telecommunications Service - Ministry of Labor - AMPOSDRU;

c) a Government Decision is being signed regarding the collaboration between AMPOSDRU and STS for the purpose of hosting under security conditions by STS, the databases of computer applications intended for European funds;

d) to ensure the highest degree of security, the servers related to the IT applications intended for European funds were moved to the STS data center.

These security measures were started as a result of countering some cyber incidents, consisting of computer attacks carried out on the opening of calls/submissions of European projects through the Actionweb computer application - through electronic mechanisms (bots) for automatic completion of project content, thus violating the established rules of submission and thus not respecting the principle established for the contracting phase - first come - first served. The simultaneous submission of projects is a violation of the legislation in force, but also a form of fraud through a cyber attack, which is why an attempt was made to exploit the vulnerabilities of the open source technology used by the PostgreSQL application.

From the perspective of organizational theory, security means "the state of macrostructural dynamic equilibrium, between inter-socio-organizations of the same level (state; supra-state structure) and with different spheres of coverage achieved by correlating organized and disorganized processes and managing change in such a way that they are not affected their fundamental, generally accepted values (goals), their existence as changing entities".

The globalization of the problems facing humanity accentuates the correlation that is established between the different levels (spheres) of achieving security; on the one hand between the security of the individual (citizen) and the security of the nation, and on the other hand between national security and regional, continental and global security systems.

Romania's national security requires the achievement of a relatively stable state of equilibrium of the social system in which individuals, groups of people organized on different criteria, the Romanian state, can develop freely and promote their own interests under the conditions of compliance with a system of norms continuous evolution.

Security policy is materialized in the Security strategy, which represents the organization and management of activities to achieve the interests and objectives of political power through the rational use of resources, ensuring social stability, ensuring change and innovation regarding the safety and security of the social system. The objectives set in the field of security can be found in the strategies built according to the respective objectives, namely: the political-diplomatic strategy, the economic strategy, the social strategy, the military strategy, etc.

A nation's security policy aims to improve the security of the nation's social, economic and political institutions against threats from other independent states.

Security strategies are built on the basis of a rigorous analysis of the security environment, the national interests established by the political power, the objectives arising from the security policy, the resources made available and adopt appropriate ways of responding to the challenges and threats that escape security.

The strength of a nation is given by its shared values, goals and aspirations, which exceed the sum of individual interests, ambitions and even achievements. A strong state respects and protects its citizens. The National Defense Strategy is the concrete expression of this vision.

"A strong Romania in Europe and in the world" most clearly expresses the final objective of the Strategy and defines the profile that our country is building for the coming years.

The National Strategy for the Defense of the Country reflects the need to promote a concept of extended national security. Through its objectives and content, the Strategy actually refers to defense and national security as a whole, and the two concepts are converging. The National Defense Strategy was developed to adequately respond to the complex reality facing Romanian society.

Afterwards, it is appropriate to mention the approach to fulfill the critical component of the national strategy for national security, to prevent cyber threats, through the existence of the project implemented in the governmental framework, correspondingly: ICIN 54 MFE - SMIS code 48723 - intended for the Ministry of European Funds, which constitutes the infrastructure and technology base of the future project to update existing and used technologies at the ministerial level: ICIN 54 MFE update - SMIS code 127221, for which the National CYBERINT Center is the beneficiary, and the Ministry of European Funds will be the authority public, according to the guide.

In this regard, the draft cooperation agreement proposed by the beneficiary - which will be concluded between the SRI - CNC and the Ministry of European Funds, user of the equipment and solutions within ICIN 54, has been submitted for approval.

The project in the implementation of which the draft cooperation agreement was initiated is financed from the Competitiveness Operational Program, a program managed by AM POC, which as the management authority gives MFE the status of financier. The object of the agreement is the cooperation between the signatory parties, in order to implement the project.

The project has as its general objective/purpose the updating of the existing IT system, through the use of new technologies capable of increasing the level of informational-institutional protection.

- We distinguish the following as activities within the project:

- The IT security assessment of the networks managed or owned by the MFE will be carried out and information will be provided regarding the cyber threats found or existing security incidents within the electronic communications networks and services managed or owned by the MFE;

- Security policies will be defined and updated within the networks of interest;

- The purchased equipment will be installed and configured for the purpose of implementing the project;

- The transfer of knowledge required to use the equipment and/or applications/software services/technologies made available will be ensured;

- Support will be provided for drawing up and updating intervention procedures in the event of a cyber incident or attack within the infrastructures belonging to the MFE;

- Support will be provided in crisis situations generated by cyber attacks to investigate the causes that led to the crisis, to determine the effects of the attack and the damage caused, as well as to restore the situation to normality;

- Confidentiality will be ensured regarding the technical data related to the current architecture and the evolution of the data communications network that MFE manages or will manage in the future, data about which it became aware on the basis of the Cooperation Agreement;

- Updated information on the vulnerabilities of IT and communication systems, security alerts and bulletins, best practices on increasing the security of cyber space, how to manage security incidents, as well as other information that can be used in prevention and reducing the number of security incidents.

- Information will be provided to detect, prevent and counter cyber attacks;

- Additional information will be requested regarding a recorded incident;

- Checks will be carried out on the condition of the equipment made available/in use during the implementation and sustainability period of the project.

- The data necessary for the assessment by the SRI of the IT security of the networks managed or under its ownership will be made available, in order to detect, prevent and counter cyber attacks;.

- The recommendations regarding the drawing up and updating of intervention procedures in the event of a cyber incident or attack within the infrastructures under its administration will be respected;

- The data provided by the equipment/technologies made available within the project will be transmitted, in the original format.

The transmission of information between the parties is done using secure and authentication protocols:

a) in real time, through secure connections and tunnels to a centralized cyber security event management system;

b) through the electronic mail service.

Within the Ministry of European Funds through ICIN 54 MFE, the following security technologies are used: UTM; WE ARE; EndPoint Security (AV, HIPS); APT 1 Email; APT 1 Web; Endpoint level APT; APT 2 solution.

The convenience of the Internet, along with the widespread adoption of smart devices, has made email the most widely used and important communication tool around the world—more so than social media or micro-blogging. Millions of emails are sent every day. Unfortunately, email technologies have some limitations:

- It is difficult to ensure the confidentiality of unencrypted information sent by e-mail;
- It is difficult to determine whether an email has reached the recipient (i) and if or when it has been opened and read;
- There is no secure method of recalling e-mail messages;
- Senders have no control over the recipient.

Thus, these deficiencies can prove difficult for organizations that need to comply with regulatory requirements or protect against data leaks. Creating the premises for the use of security technologies, in order to obtain protection, against threats from cyber space:

- Protection before, during and after an attack.

Performing automated network monitoring and analysis is beneficial. When a compromise occurs, the extent of the damage is quickly determined, remedied and operations returned to normal

- Creating and enforcing granular policies for sites with embedded applications.

- Application visibility and control.

Visualization and control of network traffic is efficient through simple use, so that it can be protected without slowing down productivity or burdening IT resources.

- Automatic traffic analysis, inbound and outbound.

Real-time web traffic scanning for both known and new malware. Using dynamic reputation and behavioral analysis across web content.

- Quickly identify zero-day attacks.

Scan suspicious activity in real-time to find anomalous behaviors and eliminate attacks. Using lookback capabilities with Advanced Malware (AMP) for Web Security to turn back time and remove malware from infected devices.

The antivirus solution is centralized, of the EndPoint Security type, at the MFE level. The management of the solution is carried out through the administration console, the actions taken having an impact at the user and workstation level. The process of updating the signatures necessary to combat attacks with malicious content is performed centrally, in a client-server relationship. Infections can be countered by organizing daily tasks directly from the administration console, without direct intervention on over 2700 workstations

Having as a general objective/purpose the updating of the IT system, through the use of new technologies capable of increasing the level of cyber protection, it was achieved - the need for equipment and security applications that will be purchased within the project: ICIN 54 MFE- code SMIS 127221.

Unified Threat Management (UTM) consolidates multiple network and security functions with a single, unified appliance that protects enterprises and simplifies infrastructure. Simplified network and security capabilities in a single box reduce the risk of cyber threats, enable access to the cloud and free up resources, allowing public administration leaders to focus on what matters most - increasing efficiency and absorption in fund management European.

Email Security Appliance – ensures the protection of the email solution, by filtering traffic according to predefined security policies, according to best practices and new knowledge about cyber attacks.

Web Security Appliance - ensures protection in the online environment of users, filtering traffic according to pre-set policies, offering safe browsing without cyber threats or vulnerabilities in the virtual environment of the Internet – www.

The role of connectors and data transmission through ArcSight SIEM - MFE, is that of research and study of behaviors in the network, as well as anomalies, thus establishing behavioral patterns of possible cyber attacks and threats, in this way prevention for the future is achieved through machine learning activities and isolation of suspicious files or with abnormal behavior, in sand-box areas, specially configured to block any unwanted situations of network penetration or subsequent data exfiltration.

The study of cybernetic behavioral patterns represents the first step in establishing the premises of applied Artificial Intelligence, including in public administration, which will have to align with Euro-Atlantic norms, by harmonizing legislation, but especially by implementing appropriate current security solutions, and adapted to the attack methods used today and even in the future, under conditions of perpetual cyber development and modernization. Thus, as part of the cyber security project - ICIN 54 MFE, the ministry will make available the data necessary for the evaluation by the SRI - National Cyberint Center of the IT security of the networks managed or owned by it, in order to detect, prevent and counter cyber-attacks. ArcSight MFE collects and analyzes events from security systems and tools, detecting security threats in real-time, so that MFE's cybersecurity expert can quickly respond and report analysis to meet demanding security requirements. Thus the Ministry of European Funds tackles cyber threats in real time by using a powerful, scalable and efficient SIEM security software.

In Romania, the evolution of cyber infrastructure intended for European funds is conditioned by inter-institutional cooperation, carried out in the form of strategies, harmonized with European legislation and materialized through specific projects to ensure cyber security. All state institutions will be included in this national system of prevention and protection against cyber-attacks. Desirable and achievable activities through the considerable contribution of cooperation with state institutions, specialized in ensuring cyber security, such as the CYBERINT National Center - the National Authority in the field of Cyber-Intelligence.

The faulty operation or in inappropriate parameters of the applications intended for European funds, integrated in the related cyber infrastructure, will generate the state of vulnerability constituted by blockages of the registration mechanisms and increase the absorption of European funds. The decrease in the absorption of European funds is and will be a real threat to Romania's national security, due to the following implications: economic; financial; social; political; as well as as a result of the obligations assumed by Romania as a member state of the European Union.

In any situation of blockage in this sensitive area of European funds, information for national security will be dominated by the need to capitalize by immediately informing the Minister of European Funds, as well as by adopting the necessary measures to remove the identified deficiencies.

The resuts of the strategy for implementation of cyber security projects, at the level of the MIPE-Ministry of Investments and European Projects, it is shown in Tables 1 and 2 below, while the use of intelligent technologies such as Sandbox Analyzer can be observed in Figures 1 below, and Computers – Security Audit in Figure 2.

Strategy of implementing ML-Machine Learning and AI-Artificial Intelligence functionalities, at the level of the MIPE-Ministry of European Investments and Projects, in 2024

Table 1

Implementation	Protected endpoints	Cyber protection	Detected and remedied attacks	Fixed vulnerabilities	Possible security risks
2013-2019	250 to 450	200 Endpoints	About 50%	About 75%	25%
2020-2023	450 to 1700	1250 Endpoints	About 95%	About 95%	5%
2024-2027	2900 to 3400	500 Endpoints	About 99%	About 99%	1%

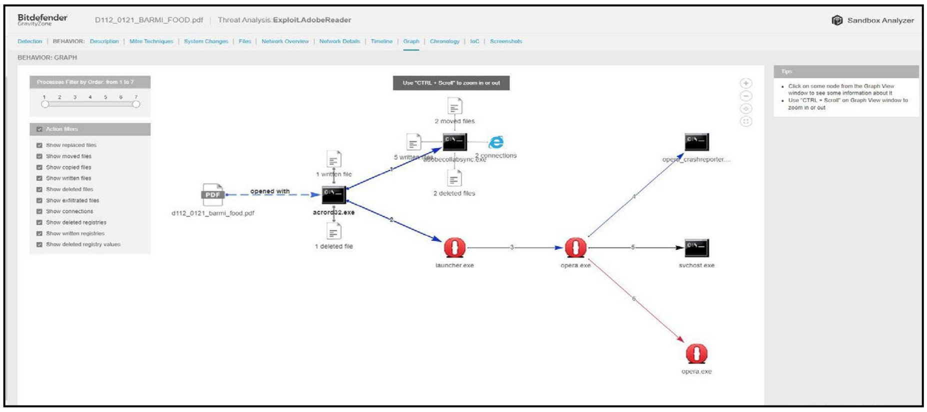
Source: Author’ own research

Results of Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Table 2

Automation	Endpoints	Cyber protection	Automated detected and remedied cyber attacks	Security vulnerabilities	Security risks
2013-2019	450	200 Workstations	50%	75%	25%
2020-2023	1700	1250 Workstations	95%	95%	5%
2024-2027	3400	3400 Workstations	99%	99%	1%

Source: Author’ own research



- Click on some node from the Graph View window to see some information about it
- Use "CTRL + Scroll" on Graph View window to zoom in or out

Figure 1. Module Sandbox Analyzer operations – MIPE

Source: www.bitdefender.com

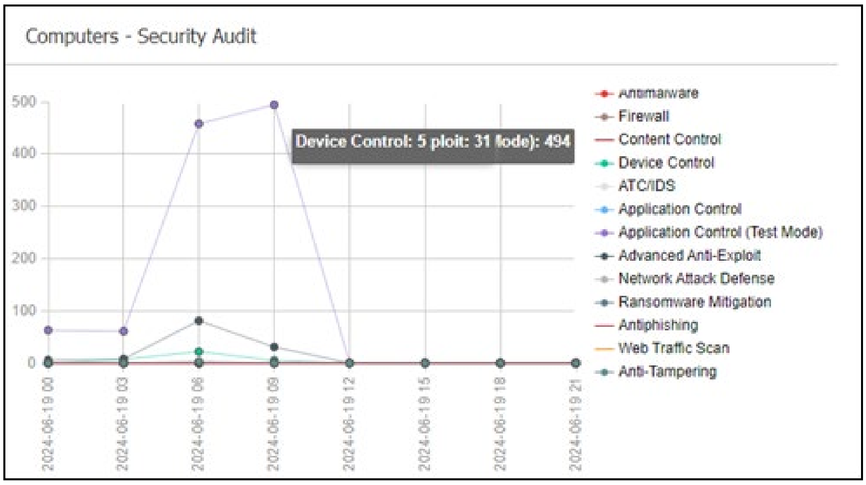


Figure 2. Module Computers Security Audit – MIPE

Source: www.bitdefender.com

4. Conclusions

The critical IT infrastructure of national importance, dedicated to applications with the role of management of European funds, is increasingly becoming a subject of interest for possible cyber attacks, especially since 2016 when the attention of certain organizations began to be focused on the government cyber space.

That is why, at the ministerial level, all the necessary resources were concentrated to create the premises of strategies to prevent and combat any cyber attacks, which could endanger the integrity of information such as those from European funds, which have an impact including in the country's economy, causing damages possible for the interests of the country, stability and development.

Thus, through funding programs, guidelines were established in the future infrastructure protection developments, through the purchase of specific security equipment. With the considerable contribution of the state institutions active in the field of cyber security, as well as through sources of external funding from European funds, it was possible to develop a national system in which all state institutions are included, with the aim of achieving prevention and protection against cyber threats.

Initially at the AMPOSDRU level, through the development of the project for securing critical infrastructures of national interest entitled - ICIN, the role and functionalities of the analytical platform for cyber attacks investigations, intended to be acquired within the project, are being exploited, being described by the technical proposal regarding the expansion of its capabilities by installing in the ICIN 38/39(LAN) - AMPOSDRU network, some sensors that have the ability to detect APT type attacks, through the behavioral analysis of files considered suspicious.

At the same time, the project intention was presented regarding the expansion of the interoperability component provided for in the project by implementing a private cooperation network between the beneficiaries of the project and the Cyberint National Center, on the infrastructure provided by STS. The equipment necessary to implement this network dedicated to cooperation in the field of cyber security, which will be installed within ICIN 38/39 - AMPOSDRU.

Security solutions are needed, bringing real benefits to the institution once they are configured to implement new policies, to make a correct monitoring and alerting. Agile approaches can be used to develop E-business solutions at the government level by breaking the development process into smaller, manageable chunks, testing and continuously iterating the solution, involving stakeholders throughout the development process, and adapting to changing requirements.

References

1. European Commission (2022) Jobs and the economy during the COVID-19 pandemic https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/jobs-and-economy-during-coronavirus -pandemic.ro.
2. European Information Society (2005) - Publisher: Foundation for European Studies.
3. European Commission - Brussels, 3.3. (2021) One year since the outbreak of COVID-19: fiscal policy response
4. https://ec.europa.eu/info/files/one-year-outbreak-covid-19-fiscal-policy-response_en.
5. Presidential Administration - Bucharest (2020) Romania - National Strategy for National Defense for the period 2020-2024.
6. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf
7. European Council - Council of the European Union - March (2010) - European Union Internal Security Strategy;
8. https://www.consilium.europa.eu/ro/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/.
9. Decision of the Official Gazette no. 677 (2020 - August 14) - on the approval of the National Program for the digitization of micro, small and medium enterprises, financed under the Operational Program Competitiveness 2014-2020.
10. http://legislatie.just.ro/Public/DetaliiDocument/229226 - Official Gazette no. 756 of 19 August 2020.
11. EU Directive 1148 / (2016) - Measures for a high level of security of networks and information systems in the Union.
12. https://cert.ro/pagini/ansrsi.
13. Regulation (EU) (2016) / 679 - on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).
14. The European Union Agency for Cybersecurity (ENISA), (2021) September 13 - Methodology for a Sectoral Cybersecurity Assessment
15. https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.
16. The European Union Agency for Cybersecurity (ENISA), (2020) April 15 - Advancing Software Security in the EU
17. https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework
18. National Cybersecurity Directorate (DNSC) - (2021) September 30 - European Cybersecurity Month - ECSM
19. https://cert.ro/citeste/comunicat-luna-europeana-a-securitatii-cibernetice-2021
20. Oracle Romania (2022) Emerging technologies: IoT, EoT, AI, Blockchain https://www.oracle.com/ro/emerging-technologies/.
21. Cloud Computing, Events - October 6, (2021 at 11:19 am) - Cloud Conference brings new technologies to the forefront - (clubitc). https://www.clubitc.ro/2021/10/06/conferinta-de-cloud-aduce-in-prim-plan-noile-tehnologii/.