Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

AGILE TRANSFORMATION AND PERFORMING MANAGEMENT OF IT AND CYBER SECURITY PROJECTS, AT THE GOVERNMENT LEVEL

Marius ȘTEFAN

PhD student,
Doctoral School of Economic Informatics,
Bucharest University of Economic Studies, Romania,
ORCID 0000-0002-4967-6234
Email: marius.stefan@mfe.gov.ro

Abstract: *In an information society in which the quality of life, as well as the prospects for social change and economic development, depend to a greater extent on information and its exploitation, the institutional field of management of IT applications for European funds becomes a matter of national importance, with critical values for national security. Reinventing government can be achieved through digitalization and government computerization, which involves modernizing the current IT infrastructure through specific external funding sources such as European funds, doubled and secured by advanced cyber protection and defense capabilities against possible vulnerabilities or cyber-attacks.*

Knowledge and scientific information are of enormous importance in the global information society, by: supporting innovation, promoting economic development, making decisions in an efficient and transparent way, at the governmental level and especially for the implementation and use of intelligent technologies in the development of the degree of digitization of public services through financing provided by European funds and the National Recovery and Resilience Plan.

In order to move on to building the knowledge society, it is necessary to reduce the digital gap, which accentuates disparities in development, excluding groups and even countries, from the benefit of information and knowledge. The limiting factor in development will be related to the human capacity to assimilate and develop these technologies, to use them in new fields of activity, for new products and services.

Keywords*: synergy in innovations; intelligent technologies; e-business; digital transformation; cyber security awareness; agile transformation; automation of repetitive processes.*

UDC: *[004.056:005.8]:338.246.2(498)*

JEL Classification: *D83, L86, K22, M16, M21.*

INTRODUCTION

This will produce a re-classification of knowledge, so that the model of access to knowledge undergoes changes, the primary interest is no longer directed towards the universal aspect, the concern becomes centered on the local space, introducing migration from the word. to image, from speech to personality.

Postmodernist discourses thus speak of a multitude of local realities or of a global reality, or even of the lack of a reality, in conditions where an ideology can no longer convince large masses of individuals, as a fragmentation takes place at the level of the subdivided currents that are found in many local realities, in one it was marked by conflicts but not by struggle, by problems but not by contradictions, by unions but not by classes, and most importantly (by the fact that) no concrete utopia animates social movements.

Thus, through social changes, and the end of the modern world, certain major changes occur in the social life of the individual, postmodernity leading either to the emergence of a new type of society or to a new phase of capitalism, both based on two phenomena: the development of new technologies and the emergence of consumerism,

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

crystallized as economic-social behavior. Postmodernity, this condition of the contemporary world, is defined as a term used by philosophers, social scientists, art critics, to refer to aspects of art, culture, economy or current social conditions, which are the result of features unique aspects of life in the late 20th and early 21st centuries.

Globalization, consumerism, the fragmentation of authority and the transformation of knowledge into an object of use, being included in the defining features of the postmodern condition. This is how the phrase information society appears in the specialized literature of post-industrialism, a notion that in sociology refers to a type of postmodern society, in which old norms and ways of thinking are replaced by new technologies and new lifestyles. A transformation of civilization is thus produced, leading to the information society through three scientific and technical revolutions: the traditional craft, the scientific organization of production and automation.

PAPER BODY

Starting from the growing role of science in production processes, combined with the emergence of information technologies and the need to automate repetitive processes, the economy and society become centered on the new central principle, called theoretical knowledge.

Within this computerized society, the new social context is based on telecommunications and computers, which become decisive for the way in which economic and social changes are produced, the way in which knowledge is created or recovered and the nature of work and the organizations in which people are employed.

Another relevant characteristic of the informational society is the way in which knowledge and information will replace work and capital, as central factors in the economy, IT, by shortening the actual work, diminishes the role of the individual in the production process, thus replacing work as the source of added value, within the national product.

In the information age, the information society is a society in which the quality of life, as well as the perspectives of social change and economic development, depend, to a large extent, on information and its exploitation. In such a modern society, living standards, work and leisure patterns, the educational system and the labor market are all significantly influenced by advances in information and knowledge.

In the evolution towards an informational society, where the role of informational technologies is decisive, the following major and determining criteria are followed: economic (services and informational goods); technological (telecommunications, computer and new technologies); social (information gets value); political (the flow of information and communication methods can create global realities in which individuals can be involved); cultural (the tendency to replace local culture with the so-called global economic culture).

The ambivalence of the information society, seen on the one hand as a global entity, and on the other hand as a mosaic made up of sub-societies spread around the world, is caused by electronic means of communication, which create a virtual global space, within which the notion of a foreigner loses its semantic consistency, creating a direct relationship between individuals, which will produce deterritorialization, through the creation of world markets, through the existence of a stock exchange accessible from anywhere and permanently, thus providing information about the circulation of capital in the world the whole In this way, a global environment is born, a global space structured on individual models of life.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

Technologies produce a breakdown in local plans, by focusing attention on certain local sectors in the sphere of marketing, advertising and mass media, by resuming certain symbols and elements of culture and reaffirming local identities.

The fragmentation generated by telecommunications is seen as a hyperreal world, in which codes and digital systems are, in fact, simulations, which dissolve the individual's life. Thus we are dealing with the adaptation of the individual to information technologies or are they designed and realized in such a way as to serve the individual, the interdependence between the two actions being inherent in the process of using the technology, as well as the mastery of certain levels of knowledge, the changes continuous advances in technology, challenging and subjecting individuals to a perpetual specialization and discovery of ways of change and innovation.

The new environment of humanity is not so much hardware or physical, its essential poses are information and coded data configurations, which more quickly gives a software image to the environment, identifiable at all levels of the individual's life.

The use of intelligent technologies will result in the development of the degree of digital culture and cyber security, among civil servants, in the economic-social-political-post-pandemic context for e-business, as a result of changing the traditional work style by adopting the new methods developed through new emerging technologies.

The use of intelligent technologies will result in the development of the degree of digital culture and cyber security, among civil servants, in the economic-social-political-post-pandemic context for e-business, as a result of changing the traditional work style by adopting the new methods developed through new emerging technologies.

The Ministry of Investments and European Projects, in cooperation with institutional partners, is the main developer of the national IT exchange program between Romania, as an EU member state, beneficiary of non-reimbursable European funds, and the European Commission, according to the provisions of REGULATION (EU) NO. 1303/2013 of the European Parliament and of the Council of 2013.

The implementation of ensuring the security of the cyber infrastructure intended for the management of European funds, was and will be conditioned by a cooperation with the institutions that have the necessary expertise in the field, thus realizing the premises of some strategies, in accordance with the European legislation in force and transposed into projects financed from European funds , aimed at ensuring cyber security, as well as increasing the level of awareness of the importance of the state of security at the governmental level:

- project code - SMIS 48723 – Titeica 1 - The national system for the protection of IT&C infrastructures of national interest against cyberspace threats, financed by the Sectoral Operational Program for Increasing Economic Competitiveness 2007 - 2013.
- project code - MySMIS 127221 – Titeica 2 - Updating and developing the national system for the protection of IT&C infrastructures with critical valances for national security against threats from cyberspace", financed by the Competitiveness Operational Program 2014-2020. (ICIN\IVC 54 MIPE - project with national coverage, and the implementation period according to the financing contract - 23.08.2019 - 23.08.2022, with related maintenance services and support for applications and equipment until 23.08.2027).
- the Titeica 3 project - will be implemented through PNRR by the National Cyberint Center, intended for the development of the national cyber protection

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

system, included in Component C7, Digital Transformation, through the National Recovery and Resilience Plan - resulting in the expansion of the protection area. of the Information Technology and Operational Technology infrastructures, as a beneficiary entity of cyber security and protection, as well as participation in training programs organized in the field of cyber security.

The objectives of the MIPE cyber security projects, being the updating and development of existing IT systems by including them in the national system, of new IT&C infrastructures with critical values for national security, in order to increase the capacities to identify possible cyber -attacks, as well as to increase the national level of ensuring cyber security, subject to a common approach of national and EU policies in the field of cyber security and interoperability, I sell the transition to a Government cloud as desirable.

Through the results obtained, the projects aim at increasing the cyber security of IT and communications services at the national level, increasing the availability and level of security offered to institutions and entities of public interest by modernizing the security systems related to the existing IT systems. Within the organizations, emphasis will be placed on achieving the interoperability of the security systems to be implemented and integrated, in terms of corroborating information, collaboration, analysis and reaction through the IT mechanism for rapid alerting and disseminating information in real time, thus obtaining effective results in a timely manner.

The outline of a national system of prevention and protection against cyber-attacks, through cyber defense activities, will create the premises for the development of innovation and the use of intelligent technologies, at the government level, with the aim of eliminating repetitive processes through automation and artificial intelligence. The operation in parameters that do not correspond to the performance, of the applications intended for the management of European funds, will generate a vulnerability, manifested in the decrease in the level of absorption of European funds, with implications in the national economy, constituting a real threat to the national security of Romania, due to the economic-financial repercussions , as well as social-political regarding the obligations assumed by Romania, from the perspective of the membership status of the European Union.

The national system of prevention and protection against cyber-attacks, through cyber defense activities, having a beneficial role in the implementation of the new National Cyber Security Strategy and in ensuring Romania's compliance with the commitments assumed at the international level, including those related to the implementation of the Cyber Security Strategy EU Cybersecurity, the NIS Directive and NIS 2.0, as well as in the activity of the European Center for Industrial, Technological and Research Competence in Cyber Security (ECCC) established in Bucharest.

In the undesirable situation of the blockage in this critical area of the national economy, constituted by the field of attracting European non-reimbursable funds, the balance specific to the state of national security will be restored by informing the competent minister as quickly as possible, as well as by adopting the appropriate measures to remedy the identified deficiencies.

Thus eliminating the risk of disengagement, through an automated and efficient management of European funds, fulfilling a better management of an objective of national strategic interest. The realization of national interests, as well as the acts of economic destruction, degradation or decommissioning of the structures necessary for the proper development of life and its quality, can constitute threats - even through the existence of a state of blocking the absorption of European funds, framed from the point of view of

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

information for national security, in the provisions of Chapter 3 related to the National Defense Strategy 2015-2019/National Defense Strategy of the country for the period 2020-2024, and art 3, letter f, Law 51/91.

In this newly developed branch of the national economy, represented by the field of European funds, the countering of these possible risks will be realized gradually, due to a high degree of persistence manifested, including through the lack of the necessary resources, as well as the necessary specialization in the efficient management of IT systems, located in continuous development, the focus being oriented towards the results obtained and efficiency in the creation of public values, including at the level of the national cyber critical infrastructure.

Impediments encountered in the functioning of the gear that is the basis of attracting funds, will bring damage both to the national budget and to the image at the community level, interoperability being a basic principle of the member states, necessary in the expected evolution process through transformation, reinvention and digitization.

Non-compliance with the obligations assumed as a member state can cause economic failures, manifested in the development of society and the increase of the quality of life depending on the evolution in the management of current financial resources and for the future, through the membership of the European Union and its specific financial exercises.

The analysis carried out on these aspects of national interest has an incidence in the current year - 2023, a favorable moment for cyber-attacks that are characterized by frequency and persistence, making it vital that both state and private organizations are armed with the most effective tools and knowledge of cyber security, to prevent, detect and respond to threats encountered. Permanent vulnerabilities will always escalate into possible threats materializing in future risks to national security. Thus, awareness through prevention being the most effective strategic approach of a governmental organization such as the Ministry of European Investments and Projects.

In the international geopolitical context, of the situation between Russia and Ukraine, a considerable increase in the number of attacks, registered in the virtual environment, on public institutions considered to be targets, by cyber attackers, was observed, thus making it imperative to ensure the cyber protection of workstations and mobile devices within MIPE - through the centralized administration of an anti-virus type solution, completing the purchases related to the project carried out in the Cooperation Agreement with Cyberint: Titeica 2 - Updating and developing the national system for the protection of IT&C infrastructures with critical valences for national security against cyber threats.

Ensuring the state of balance and security is increasingly important among organizational concerns, in the context of the exponential increase in the number and complexity of cyber threats (malware/ransomware/social engineering in particular). Deficiencies found in the development solutions, hardware and software used, as well as the lack of an appropriate modernized infrastructure, dedicated to the national IT system, can cause malfunctions in the electronic services offered to beneficiaries and the business environment in the process of developing future electronic business solutions.

As an area of application, the IT system acquires importance at the national level, but it can also slow down certain processes in the economy, such as the annual preparation of the national budget.

The inclusion of interoperability requirements in the relationship with the European Commission requires a clear focus on functional and secure reporting processes, automation of repetitive processes, increased processing of documents in electronic format,

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

and signing with digital certificates. The concentration of resources can only provide solutions under safe operating conditions, ensured by a balance specific to the state of cyber security.

In the national strategy for alignment with European standards, including harmonization with European provisions, this may constitute a vulnerability in the proper functioning of the activity, in the context of increasing rigors/requirements regarding interoperability in the EU.

It is necessary to ensure compliance with the requirements of the NIS2 European Directive and Law 362/2018 - regarding the wave of digital information that must be managed and controlled by technical security measures, as well as Law no. 3652/2018, which transposes the European NIS Directive, and regulates the necessary framework for developing the level of preparation of EU states to deal with possible incidents that may affect IT security.

The EU NIS (Network and Information Systems) Directive 2016/1148 is an essential legal piece launched at the EU level to increase the level of cyber security for critical infrastructure units, including critical infrastructure entities in the fields of utilities, transport, healthcare and digital services, as well as European funds. Establishing a set of principles and rules to define, measure and improve cyber security.

Given the expansion of cyber-attacks, compliance with the requirements of the NIS Directive is imperative. A cyber security strategy based exclusively on prevention is not enough, finding a need for maximum involvement, through rapid detection and use of effective emerging solutions.

An unforeseen attack on a critical cyber infrastructure of national interest, such as that intended for European funds, can occur as a result of security risks not properly treated, with possible results, data leaks, through exfiltration, or by causing syncope in operation, even leading to interruptions in the operation of essential and critical services for the national infrastructure.

According to current and long-term trends, the main frequent threats that should be monitored in an organization are malware and phishing attacks, especially in a government institution such as the Ministry of Investments and European Projects, representing a real area of interest for groups of cyber-crime, for the purpose of espionage activities or theft of strategic information, such as government information.

The measures implemented regarding the awareness of the importance of the activity of ensuring cyber security, especially among specialized personnel and intended for ICT activities as well as public officials, require preparation for combating the risks that the public institution will face, starting from the up-to-date software components according to security standards, and up to e-learning sessions on defense tactics in the cyber environment at the user level.

Adapting to periods with frequent technological changes, or decision-making in moments of calm observed in the governance process, can constitute vulnerabilities in terms of ensuring the necessary balance in the organization.

The behavior manifested in situations such as the loss or lack of administration credentials, access to work environments created through electronic tools, can create certain impediments in the process of administering the cyber security component.

Most of the time, political management changes within the institutional framework are also reflected in the specific activities of technical departments such as ITC, by slowing

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

down the decision-making and construction process, not representing a good institutional practice, especially in the case of ensuring cyber security.

The progress registered in the development of new technologies will establish the desire to align with the new standards of the future, through the use of new solutions such as the private or hybrid cloud, which will be adopted at the governmental level, from the point of view of budget efficiency, but especially for specific considerations of the cyber security component.

Through the analysis of the vulnerabilities described, we find the need to establish within the organization a specific post of cyber security administrator. He will have to possess the necessary specialization in the field, through certified resources in the field of Cyber Security with an emphasis on specific activities such as - National Security Information Management.

At the level of the Ministry of Investments and European Projects, this measure is being implemented, a first step, by signing the Cooperation Agreement, between MIPE and Cyberint, through a national level project of critical cyber infrastructure - ICIN\IVC 54 MIPE, linked to the structures of the European funds and the national critical infrastructure, succeeding in the unification through cyber security solutions of the majority of state institutions of national strategic importance.

The response to Cyber Security incidents, as an activity, requires the existence of its own specialized staff, through a Security-Operation-Center type team, specific to such situations, by nomination and inclusion in the Security Structure of MIPE, being extremely useful public institution, including in situations of cooperation with authorized authorities in the field of cyber defense. Awareness and training in cyber security is very useful within the organization, especially among users - public officials, promoting the use of solutions to protect them from incidents, respecting the regulations related to their own password, which should comply with certain current security standards.

Raising awareness of the importance of ensuring cyber security measures will be achieved by informing users, being the first measure of protection against increasingly frequent cyber-attacks in the post-pandemic context of the current information war, as a result of the events in the geostrategic area of Ukraine.

Error is human but can be avoided through awareness. Hacker attacks will be countered, through periodic information, through constant emails, courses, training, eliminating the possibility of more serious future problems, especially with regard to sensitive government information and data.

In the near future, public administration will evolve towards a new approach to the use of emerging technologies, being transposed into future strategies regarding innovation in development and ensuring cyber security, using solutions in cloud, on-premise, or hybrid cloud environments, depending on the available budgets and of advantages or disadvantages offered. For the efficiency of the activity or in the situation of permanent blocking of employment procedures in the public administration, the subcontracting of services by allowing access to these technologies, represents an effective way of managing platforms and IT systems, with a cost-benefit ratio in favor of the public institution, making the use of internal resources more efficient.

Security solutions used in the organization generate real benefits for the institution when they are configured correctly in accordance with current security standards, ensuring continuous protection of equipment, applications and users.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

Intelligent and intuitive, easy-to-use management tools can optimize the time needed to implement new security policies, through appropriate monitoring and alerting. Also, the collaboration with the National Cyberint Center - the Romanian Information Service - ensures stability and access to the necessary knowledge in the activity of implementing these cyber security assurance systems at the organizational level.

The unified and integrated technologies offer a measurable advantage in efficient results, the organization benefiting from such consoles and tools adapted to the level of expertise, in accordance with the strategies built by the Security IT department. Cooperation with other institutions such as the National Cyberint Center - the Romanian Information Service, by participating in seminars and conferences in the field of cyber security, is an excellent tool for improvement and awareness, building at the local level the principles of an applied guide of good practices, assimilated in order to adopting the best decisions for the public institution.

The budget allocated to innovation in public administration will create and maintain the much-desired stability, especially in critical national areas, such as ensuring the absorption of European funds. In industry and the economy, the role of robotics and process automation will grow considerably, with technology-related changes bringing both benefits and vulnerabilities, particularly in cyber terms. A virtual parallel world will be created, in which the existence of the state, with all that it represents, must be protected, so that the environment is safe and secure, including for the individual. The consequences of competition in innovation produce major transformations including in society, simplifying the complex life of modern man, in the information society.

They will crystallize into a national interest for the Government Strategy, areas such as attracting European funds and ensuring cyber security, with the aim of modernizing, computerizing and digitizing the public administration in Romania.

The inclusion of interoperability requirements in relation to the European Commission requires a clear focus on functional and reliable reporting processes, with results such as increased processing of documents in electronic format, signed with digital certificates. The concentration of resources can only provide solutions under safe operating conditions, ensured only by a state of cyber security.

LITERATURE REVIEW

The new innovation trends in the use of intelligent technologies are reflected in the Cybersecurity Policies, applied at the level of the administration console of the anti-virus type solution, belonging to the Ministry of Investments and European Projects- The software product used is an integrated platform for the security management of the equipment (stations and physical / virtual servers) used and managed within MIPE - Bitdefender GravityZONE Single Central Administration Console.

The integrated device security management platform is based on a simple and integrated architecture with centralized management for both workstations and data centers. It thus allows the efficient and quick installation of the protection solution and requires less administrative effort after implementation, in order to obtain the highest possible degree of accuracy regarding the assurance of cyber security at the MIPE level.

Using machine learning capabilities and automatic incident investigation, certain activities that should have been performed by a security incident response team will be performed automatically in conditions where MIPE does not currently benefit from an internal SOC (Security Operation Center) structure. Integrated and automated response

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

flows will enable designated personnel to respond effectively by limiting lateral spread and stopping potential attacks. Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The result is threat prevention, deep visibility, accurate incident detection and intelligent response to minimize exposure to infection and stop unauthorized access. As an integrated workstation protection package, the integrated equipment security management platform ensures a uniform level of security for the entire IT environment, so that attackers cannot find a weakly protected workstation to use as an entry point. departure for dangerous actions against the organization.

As a result of cyber events, such as attacks such as those associated with the EMOTET and Andromeda Malware Campaigns, it was found the need to implement a centralized component to ensure cyber security at the MIPE level, by configuring the Central Antivirus Solution Administration Console, in order to come in the face of cyber-attacks and to have the possibility of automatic detection and analysis of cyber threats and related possible incidents. In the current geopolitical conditions and considering the possible cyber effects generated by the informational component of the current global state of war, it is necessary to ensure the cyber security component by using emerging machine learning technologies, cloud scanning features and sandbox analyzer to detect malicious activity that evades traditional endpoint attack prevention mechanisms.

Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The integrated central console provides automated alert prioritization with one-click remediation functions. It will thus achieve continuous analysis within the organization, using unique capabilities to identify risk based on hundreds of factors. Providing clear guidance for mitigating potential risks at the user, network and operating system levels.

For the administration of the 3400 licenses of the workstations, centrally from the console, it is necessary to consume a low effort for the maintenance activity of the automatic processes, being easy to implement and integrate into the existing security architecture.

The agent is resource-efficient, with low administrative costs in terms of disk space, memory, bandwidth, and CPU resources.

The flexibility, scalability and upgradeability of the complete endpoint protection platform and managed detection and response services are required in the process of ensuring the cybersecurity standard built at the MIPE level.

By using cutting-edge threat detection technology, including fileless attacks, ransomware and other zero-day threats.

In threat analysis, the event logging feature continuously filters events produced on the endpoint, compiling a prioritized list of incidents for further investigation and response.

In the event recording process, continuous monitoring allows data to be passed to the threat analysis module to visualize the results generated by the events involved in an attack.

The single management console automatically executes suspicious payloads in a controlled virtual environment. The threat analysis module then uses this analysis to make appropriate decisions about suspicious files, according to the automation achieved through the security policy implemented at the level of the single management console.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

Cyber Security incident investigation and response processes will be automated through the IoC search capability, querying the event database to discover possible threats through ATT&CK techniques and indicators of compromise as well as updated information on discovered threats or other possible malware.

METHODOLOGY

The research was carried out at the level of the Ministry of Investments and European Projects, with the main aim of creating scientific and technological excellence by analyzing the results obtained through the use of intelligent technologies at the central administration level, as well as obtaining advantages in the field of cyber security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture in the central public administration and among contractual users or civil servants, with the possibility of establishing within the organization at least 3 positions with specific tasks in the cyber field, in direct collaboration with the Ministry's Security Structure and in a cooperation agreement with the National Cyber Intelligence Center of the Romanian Intelligence Service.

The period included in the analysis activity is between the years 2013-2023, including two programming periods of non-refundable financing from European funds, facilitated by the European Commission, as well as the National Recovery and Resilience Plan.

The three projects carried out by the Cyber-int National Center, to ensure cyber security at the national level, constituting a security umbrella, over the critical infrastructure of national interest, which will be reinvented through the digital transformation generated with the help of emerging technologies, which have produced an evolution considerable in government digital transformation.

Emerging technologies and the integration of machine learning functionalities through artificial intelligence, at the level of the Ministry of Investments and European Projects, as a development measure through innovation, will produce positive effects including on the development of the national economy by increasing the absorption of European funds in a secure cyber environment.

RESULTS AND DISCUSSIONS

The cyber security policies, applied at the level of the administration console of the anti-virus type solution, belonging to the Ministry of Investments and European Projects, ensure a high degree of defense against current cyber threats.

The software product used is an integrated platform for the security management of equipment (stations and physical / virtual servers) used and managed within MIPE.

A complete workstation security solution, designed from the ground up as an integrated EPP and easy-to-use EDR, offering prevention, threat detection, automated response, pre- and post-compromise visibility, alert triage, investigation, advanced search and one-click fix.

Relying on highly effective prevention, automatic threat detection and response technologies, the antivirus software product (the IT solution) greatly limits the number of incidents that require manual analysis, reducing the operational effort required to use an EDR solution.

For the centralized solution, delivered on premise and designed with a single agent and a single console, it is also necessary to ensure the premises to ensure compatibility and

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

an easy way to install and integrate into the existing security architecture, by personnel authorized by the manufacturer.

Integrated device security management platform enables precise protection of digital assets against even the most difficult-to-detect threats by effectively responding to all phases of an attack.

The decisive step in the use of emerging technologies through the integration of Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of Investments and European Projects, was made within the projects financed from non-reimbursable funds, as a measure of the development through innovation, of a critical infrastructure of national interest, through -a cooperation agreement with the National Authority in the field of Cyber-intelligence - the National Cyberint Center - within the Romanian Information Service.

The result is potential threat prevention, deep visibility, accurate incident detection, and intelligent response to minimize infection exposure and stop unauthorized attacker access.

As an integrated workstation protection package, the integrated device security management platform ensures a uniform level of security across MIPE's IT environment, so that attackers cannot find a weakly protected workstation to use as an entry point for dangerous actions against the organization.

The security equipment used within the organization offers advanced management capabilities to prevent, detect and investigate cyber security incidents, by analyzing the risks generated by possible attacks, as well as timely automatic remediation of threats.

Increasing awareness of the importance of ensuring cyber security will be achieved by informing users, making the first measure of protection against cyber-attacks within the organization. Human error can be avoided through e-learning and the implementation of the security assurance component starting from the individual level.

These aspects implemented in the organization will counter the attacks of hackers, by ensuring regular information activities regarding good practices through constantly sent emails, organization of courses and training, eliminating the possibility of subsequent, much more serious problems, especially regarding the information and data belonging to the central administration.

The public administration will evolve towards a different approach to the use of emerging technologies, translating into future strategies, the need to use solutions in cloud, on-premises or hybrid cloud environments, depending on budgets and available advantages or disadvantages, fulfilling a strategy of innovation and development of digitization processes by using the funds related to the National Recovery and Resilience Plan.

In order to make the activity more efficient or to avoid situations of temporary blocking of the procedures applied in the public administration, a solution can be the subcontracting of the necessary services, which allow access to such intelligent technologies, constituting an efficient way of managing the platforms, with a cost-benefit ratio built in in favor of the public institution, with the aim of reducing the use of internal resources and decongesting the high degree of burden manifested in the activity of public officials from the central administration.

Public administration services can be optimized with the help of the use of advanced information technologies. The European Commission tries to set its own example in this sense, through the procedures and tools it uses in its day-to-day activity, in its links with the administrations of the member states and with its own decentralized agencies, marked by constant progress in innovation and computerization. The goal being

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

to facilitate citizens' access to public information through new technologies and computer applications, as well as to achieve better communication between all levels of public administration in the Union, thanks to the high-speed connection.

The development of the European information society requires a considerable financial effort, which is constantly growing, which cannot be fully assumed by the European Union and the governments of the member states.

Practical experience has shown that the private sector is the most capable of taking the necessary risks in operating and developing new adaptable markets, having the necessary capital to make such investments necessary for the digital transformation strategy.

The integration of machine learning and artificial intelligence functionalities, at the level of the Ministry of Investments and European Projects, can be seen in Tables 1 and 2 below, while the use of intelligent technologies such as Sandbox Analyzer and EDR - Endpoint Threat Detection and Response (ETDR) can be seen in Figures 1 and 3 below, and Computers – Endpoint policy compliance in Figure 2.

Table 1. Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Implementation period	Protected workstations	Increasing the degree of cyber protection	Automate responses to detected and remedied cyber attacks	Fixed vulnerabilities	Possible security risks
Cyber Project 1	250 to 450	200 Endpoints	About 50%	75%	25%
Cyber Project 2	450 to 1700	1250 Endpoints	About 75%	90%	10%
Cyber Project 3	1700 to 3400	3400 Endpoints	About 95%	95%	5%

Source: Author' own research

Table 2. Results of Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Automation period	Protected endpoints	Increasing the cyber protection	Automated detected and remedied cyber attacks	Security vulnerabilities	Security risks
2014-2017	450	200 Workstations	50%	75%	25%
2020-2023	1700	1250 Workstations	75%	90%	10%
2023-2027	3400	3400 Workstations	95%	95%	5%

Source: Author' own research

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

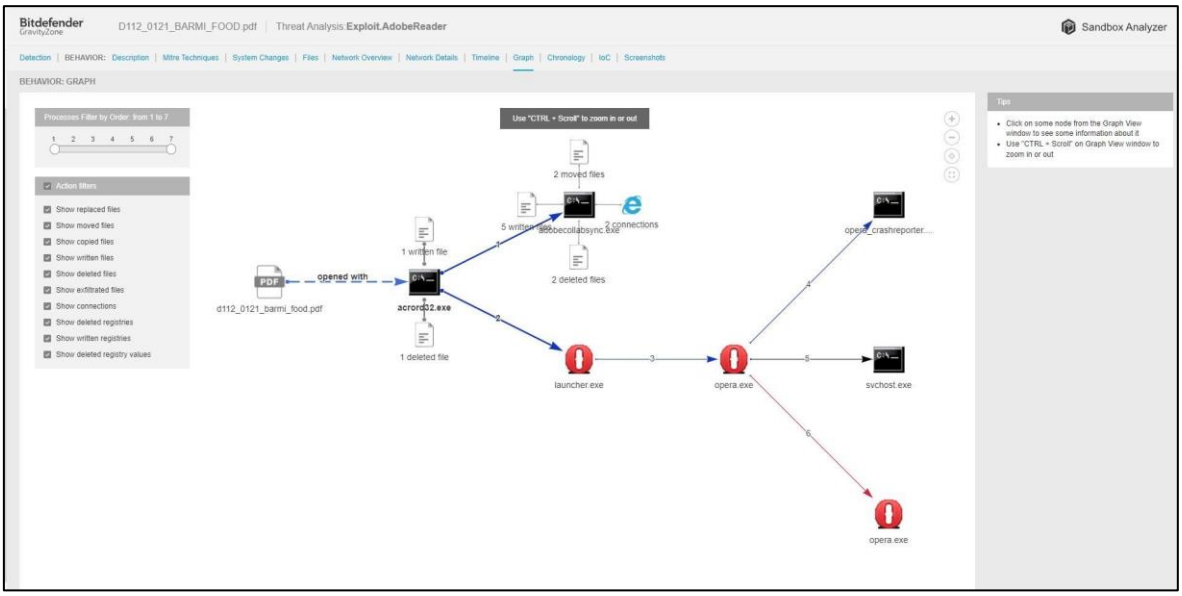

Figure 1. Sandbox Analyzer – Ministry of European Investments and Projects
Source: www.bitdefender.com

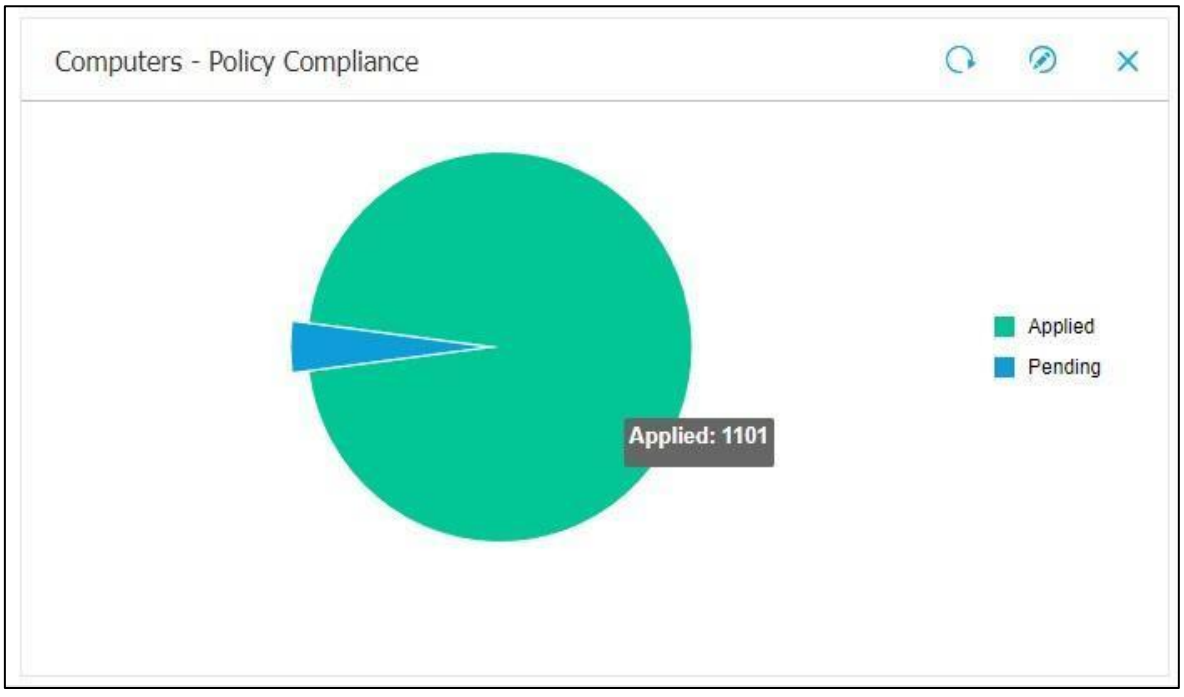

Figure 2. Computers – Endpoint policy compliance – Ministry of European Investments and Projects
Source: www.bitdefender.com

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

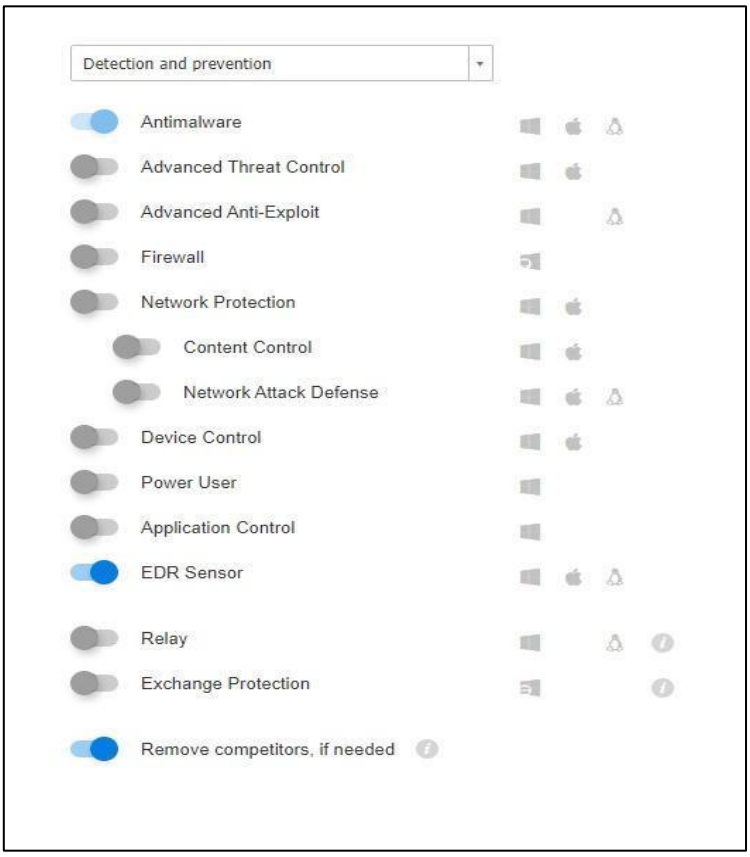

Figure 3. Endpoint Threat Detection and Response – Ministry of European Investments and Projects
Source: www.bitdefender.com

CONCLUSIONS

Using machine learning capabilities and automatic incident investigation, certain activities that should have been performed by a security incident response team will be performed automatically in conditions where MIPE does not currently benefit from an internal SOC (Security Operation Center) structure.

Integrated and automated response flows will enable designated personnel to respond effectively by limiting lateral spread and stopping potential attacks.

Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The EDR module provides automated alert prioritization with one-click remediation features. The EDR module will perform continuous analysis within the organization, using unique capabilities to identify risk based on hundreds of factors. Providing clear guidance for mitigating potential risks at the user, network and operating system levels. EDR administration requires low maintenance effort, being easy to implement and integrate into the existing security architecture, compatible with the antivirus solution used at the MIPE level.

The agent is resource-efficient, with low administrative costs in terms of disk space, memory, bandwidth, and CPU resources. The flexibility, scalability and upgradeability of the complete endpoint protection platform and managed detection and

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

response (MDR) services are necessary in the process of ensuring the cybersecurity standard built at the MIPE level.

By using cutting-edge threat detection technology, including fileless attacks, ransomware and other zero-day threats. In threat analysis, the event logging feature continuously filters events produced on the endpoint, compiling a prioritized list of incidents for further investigation and response. In the event recording process, continuous monitoring allows data to be passed to the threat analysis module to visualize the results generated by the events involved in an attack.

The Sandbox Analyzer component automatically executes suspicious payloads in a controlled virtual environment. The threat analysis module then uses this analysis to make appropriate decisions about suspicious files, according to the automation achieved through the security policy implemented at the level of the single management console.

Cyber Security incident investigation and response processes will be automated through the IoC search capability, querying the event database to discover possible threats through ATT&CK techniques and indicators of compromise as well as updated information on discovered threats or other possible malware.

The use of security solutions through intelligent technologies will generate real benefits within the organization through the necessary configuration in the secure operation standards. Intuitive emerging technologies will optimize the time required to implement new security policies to achieve better monitoring and accurate alerting.

The cooperation with the National CYBERINT Center - Romanian Information Service, ensures stability in the cyber defense component, as well as access to the necessary knowledge in carrying out the awareness activity of the importance of ensuring the state of cyber security.

Cooperation to ensure cyber security, participation in seminars and conferences in the field of cyber defense, represent excellent tools for improvement and innovation in the organization, creating the premises for the assimilation of good practices, in establishing the best decisions for the public institution.

The unified and integrated technologies offer a measurable advantage in obtaining more efficient results, benefiting from unique management consoles and tools adapted to the level of expertise held in the organization, completed with the cyber security strategies built by the Cyber Security department of the Ministry of Investments and European Projects.

The budget allocated to innovation in public administration, through specific European funding programs, will create and maintain the necessary stability, especially in critical areas of the national economy, such as the absorption of European funds.

The economy and society will undergo transformations, the role of robotics in industry and the automation of repetitive processes in organizations will increase considerably.

The revolution of emerging technologies brings both benefits and vulnerabilities, threats and risks, especially in cyberspace, regarding the need to ensure cyber defense.

By reinventing governance and computerizing public administration, a parallel virtual world will be created, in which the existence of the state, with the balance of the necessary security state, must be protected, so that the cyber environment is safe and secure even for the citizens.

The repercussions of competition in innovation produce major transformations through interoperability and synergy, including in society, simplifying the crowded life of modern man in the era of the information society.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

Strategic areas such as the attraction and absorption of European funds, by ensuring cyber security, aiming at the modernization and computerization of the public administration in Romania, constituting a national interest for the government's evolution in innovation.

Creating a global framework of security and trust in ICT, with an expansive trend towards automating repetitive processes, will generate the achievement of optimal efficiency.

These strategic objectives aim at the creation of scientific and technological excellence, obtaining advantages in innovation through the security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture among officials in the central public administration.

An important stage will be achieved in the inter-institutional collaboration, for the achievement of the fundamental objectives of the country strategy, the field of funds becoming a critical infrastructure of national interest, through the inherent implications generated in the national economy, all important plans of the current modern society being affected, from the financial - up to economic, social-educational, even political, with all the necessary risks assumed through the decisions applied at the level of future strategies.

The efficient management of the infrastructure and applications intended for the management of European funds, having a particular importance in the evolutionary process of increasing the quality of life, represents the first step towards knowledge, innovation and development of society in the information age.

BIBLIOGRAPHY

1. European Commission (2022) *Jobs and the economy during the COVID-19 pandemic* [viewed 01 dec 2023]. Available from: <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/jobs-and-economy-during-coronavirus -pandemic.ro.>
2. PUBLISHER:.FOUNDATION FOR EUROPEAN STUDIES, *European Information Society*, 2005.
3. JAN SERVAES, *The European Information Society – A reality check* – Bristol, UK Portland, OR, USA, 2003, ISBN 1-84150-893-4 / 1-84150-106-9.
4. European Commission - Brussels, 3.3. (2021) *One year since the outbreak of COVID-19: fiscal policy response* [viewed 02 dec 2023]. Available from: <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.* [viewed 03 dec 2023]. Available from: <https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf>
6. European Council - Council of the European Union - March (2010) - *European Union Internal Security Strategy;* [viewed 04 dec 2023]. Available from: <https://www.consilium.europa.eu/ro/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/.>
7. 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.* [viewed 05 dec 2023]. Available from: <http://legislatie.just.ro/Public/DetaliiDocument/229226 - OFFICIAL GAZETTE no. 756 of 19 August 2020.>

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

8. EU Directive 1148 / (2016) - *Measures for a high level of security of networks and information systems in the Union.* [viewed 06 dec 2023]. Available from: <https://cert.ro/pagini/ansrsi.>
9. 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).
10. The European Union Agency for Cybersecurity (ENISA), (2021) September 13 - *Methodology for a Sectoral Cybersecurity Assessment*[viewed 07 dec 2023]. Available from: <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.>
11. The European Union Agency for Cybersecurity (ENISA), (2020) April 15 - *Advancing Software Security in the EU*[viewed 08 dec 2023]. Available from: <https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework>
12. National Cybersecurity Directorate (DNSC) - (2021) September 30 - *European Cybersecurity Month – ECSM* [viewed 09 dec 2023]. Available from: <https://cert.ro/citeste/comunicat-luna-europeana-a-securitatii-cibernetice-2021>
13. Oracle Romania (2022) *Emerging technologies: IoT, EoT, AI, Blockchain* [viewed 10 dec 2023]. Available from: <https://www.oracle.com/ro/emerging-technologies/.>
14. Cloud Computing, Events - October 6, (2021 at 11:19 am) - *Cloud Conference brings new technologies to the forefront - (clubitc)* [viewed 11 dec 2023]. Available from: <https://www.clubitc.ro/2021/10/06/conferinta-de-cloud-aduce-in-prim-plan-noile-tehnologii/.>