Pilot platform for identification and evaluation of early warning indicators in crisis management

Vasile Florin POPESCU[1], Victor GÂNSAC[2], Olivia COMȘA[2], Marius Sorin PISTOL[2], Cristian ICHIMESCU[1], Călin Mihai RANGU[3], Mircea-Constantin ȘCHEAU[4], Cătălin CIOACĂ[5]

[1] „Carol I" National Defence University of Bucharest, Faculty of Security and Defence

[2] SAFETECH Innovation

[3] „Danubius" University of Galați, Business Administration and Economical Sciences Faculty

[4] Constanța Maritime University & University of Craiova

[5] „Henri Coandă" Air Force Academy, Faculty of Aeronautical Management

Popescu.VFlorin@unap.ro, victor.gansac@safetech.ro, olivia.comsa@safetech.ro, pistolsorin@icloud.com, Ichimescu.Cristian@unap.ro, calinrangu@univ-danubius.ro, mircea.scheau@edu.ucv.ro, catalin.cioaca@afahc.ro

Abstract: Given the realities that we are experiencing in the Ukraine crisis, with military and financial-banking implications, the need to develop and implement an early warning platform in case of crisis or disasters has arisen. This work addresses this need, with expertise in defence and security, financial-banking and cybersecurity domains, and creates a platform specialized in identifying and evaluating early warning indices for crisis management. The goal is to provide state-of-the-art early warning systems that help the population at risk to avoid crisis situations, while serving as decision support tools for various authorities (Ministry of Defence, Ministry of Internal Affairs, Intelligence Services, Financial-banking systems) when confronted with a crisis situation similar to the one from Ukraine.

Keywords: alerts, data acquisition and analysis, templates and classification, integrated identity, modelling and processing, command and control center.

Platformă pilot pentru identificarea și evaluarea indicatorilor de alertă timpurie pentru gestionarea situațiilor de criză

Rezumat: Având în vedere realitățile pe care le trăim în cazul crizei din Ucraina, cu implicații militare și în același timp financiar - bancare, a reieșit necesitatea proiectării și realizării unei platforme de avertizare timpurie în caz de crize sau dezastre. Astfel, lucrarea de față răspunde acestei necesități, cu expertize din domeniul de apărare și securitate, financiar bancar, securitate cibernetică, și realizează o platformă specializată în identificarea și evaluarea indicilor de alertă timpurie pentru gestionarea situațiilor de criză, cu scopul de a oferi sisteme de avertizare timpurie de ultimă generație pentru a ajuta populațiile expuse să evite situațiile de criză și în același timp va servi drept instrument de luare a deciziilor pentru diverse autorități (Ministerul Apărării, Ministerul Afacerilor Interne, Serviciile de informatii, Sistemele financiar-bancare), atunci când se confruntă cu o situație de criză similara crizei din Ucraina.

Cuvinte cheie: alerte, achiziție și analiză de date, șabloane și clasificare, identitate integrată, modelare și procesare, centru de comandă și control.

1. Introduction

In recent decades, various organizations in different fields of activity have developed numerous ways to provide early warning indicators.

Early warning systems have received many definitions over time, with authors reporting on the objectives and addressed areas. In essence, security crisis prevention involves the systematic collection and analysis of information related to crises in order to: anticipate their escalation; develop strategic responses; present options to key actors so they can make decisions (Schmid, 1998).

Among the main sectors of activity that have developed and used these early warning mechanisms are the organizations involved in crisis management. Predictions and early warnings at different times are very important because they can help determine the objectives to be achieved, develop options for action and compare them, which eventually leads to the implementation of the chosen options, the analysis of the response of the actors and the possible scenarios (Popescu, 2019).

https://doi.org/10.33436/v32i2y202204

To illustrate the importance of early warning systems for different organizations, not only in the field of security, Popescu & Ichimescu (2021) mentioned the main types of hazards and related warning systems in the following areas: severe weather, landslides/floods, drought, fires, earthquakes, volcanic eruptions, tsunami, and epidemics.

To ensure sustainability and resilience for the current and next generation, decision makers and stakeholders need to be well informed about past and current problems. They also need knowledge and tools to help them analyze, assess, and design a viable implementation plan for long-term development (Niculescu-Mizil Gheorghe et al., 2019).

The multiple destabilizing effects of crises and conflicts have led to the initiation of a new strategic approach for prevention mechanisms at the national level, an initiative that has led to the institutionalization of early warning structures in most situations (Brune et al., 2015). Such a pilot platform solves the technical challenge associated with integrating architectures or the procedural challenge driven by interagency coordination requirements.

Indicator-based early warning systems are found in all areas of national security interest, whether we refer to hard power or soft power, constructivist, realist, or liberal perspectives. In the simplest architecture, they are limited to a cyclical process that includes the phases of defining and knowing the risk or threat, monitoring and forecasting, disseminating information to decision makers, and adopting measures to respond or regulate the situation. Indicator-based early warning systems are a tool that adds significant value to preventing and anticipating risks and threats to national security. Even in their simplest form, they allow permanent monitoring of the security situations, determination of the cause-effect relationships, and can signal changes that require the immediate attention of decision makers to make immediate adjustments in the event of negative or positive developments and take action to return the situation to a state of equilibrium that allows the normal functioning of society.

Technology is the most important factor in creating warning systems based on indicators as well as improving their performance. New data mining tools for managing huge amounts of data in space information, indexing software, clustering, quantitative analysis, warning communication are causing permanent changes in a field of research that is still in the crystallization phase and that will not find a place among scientific disciplines under these conditions. The recognition of the need and the possibility to implement indicator-based warning systems at the national and international level, as well as the increase of resources that can be used for the creation of such systems, are the positive aspects that characterize the early warning process.

All these aspects mentioned above are the triggers for the solution presented in this paper to identify and evaluate early warning indicators for crisis management.

2. Analysis of the early warning platforms used in different domains

2.1. United Nations (UN) early warning systems

According to UNISDR terminology, an early warning system can be understood as: "The set of capabilities necessary to generate and disseminate meaningful warning information in a timely manner so that individuals, communities, and organizations threatened by a hazard can prepare and act in time to reduce the likelihood of harm or loss." (UNISDR, 2009).

The concept of early warning has come to people's attention since the December 26, 2004 tsunami, developing a global early warning system for all natural hazards (United Nations, 2006). The UN conclusion has brought to light a not very comfortable situation, in the way that while some early warning systems are quite clear and successfully used, there is still a lack of improvement, especially in the systems used by poor countries. The final report brought a number of recommendations to the international public, such as:

- a set of specific actions to build early warning systems at the national level that address key gaps in global early warning;
- consolidate the scientific basis and early warning data;

- developing the necessary institutional foundations.

In response to the call for an appropriate framework for the implementation of advanced early warning as an important risk management tool, the International Early Warning Program (IEWP) was proposed at the Second Early Warning Conference (ECHR II), in 2003. As a facilitator, a Platform for the Promotion of Early Warning (PPEW) was established in 2004 with the support of the German government to simplify the implementation of the proposed IEWP, support early warning dialog, and mobilize resources to build partnerships and capabilities at all levels.

The Hyogo Framework for Action (HFA) focus area emphasizes the need to identify, assess, and monitor disaster risks while strengthening the concept of early warning. The HFA also emphasizes that Strategy for Disaster Reduction (SAT) must be an integral part of the national disaster risk management strategy, enabling national governments and local communities to take appropriate actions to improve disaster forecasting. Various assessments (UN, 2006; UNEP, 2012), as well as the results of the HFA mid-term review, have shown that many nations around the world operate SATs for natural disasters (Popescu, 2019).

However, government priorities regarding the level of development and overall effectiveness of the EWS at the national and local levels vary widely. For many countries, especially those at high risk but with the fewest resources, building and supporting the SAT from the national level to the community level remains an extremely difficult challenge. According to UN, an effective SAT goes through the following steps:

- Acknowledgement of the risks: the risks are analysed and warning messages are issued;
- Monitoring and warning: hazards are detected, monitored and hazard forecasts and warnings are developed;
- Dissemination: warnings regarding the risks are disseminated in an accurate manner to target audience;
- Ability to respond to emergencies: emergency plans are activated in response to warnings to reduce the potential impact on life and livelihoods.

2.2. Early warning systems used by NATO

As we see now during the war in Ukraine, the early warning indicators used by NATO are of critical importance and it can be said that important technological progress has been made, compared to the situation in the Balkans, Bosnia and Herzegovina and Kosovo.

The lesson learned in the last decade in the Balkans and more recently the situation in Ukraine are clear. Early warning systems of impending crises have become crucial. During the Cold War, NATO used a system of indicators and alerts that could provide early warnings about the evolution of enemy attack strategies. At that time, "indicators" were essential steps in preparing for military action. The "warning" was the formal alert to political-military decision makers and commanders of a potential crisis or attack. The warning system used during the Cold War focused largely, although not exclusively, on military signs, which were usually largely quantitative (Popescu, 2019).

Since the end of the Cold War, changes in the security environment have forced NATO to revise its warnings methods. As a result of the decreasing risk of armed conflicts between states, but with an increased risk of conflicts within states, the Alliance has expanded its approach to early warning in several ways:

- Firstly, the threat of direct aggression on Alliance territory to include non-military risks and even unconventional threats such as terrorism;
- Secondly, it increased interaction with Euro-Atlantic Partnership Council (EAPC) members, who continue to contribute to early warning;
- Thirdly, NATO has developed a new intelligence information system (NIWS).

First of all, it must be specified that NATO benefits from early warning indicators through actions meant to consolidate peace processes. This includes meetings of the North Atlantic

Council, Policy Coordination Group, Policy Committee, Military Committee, and other committees where allies share information on potential ongoing crises.

As mentioned above, NATO has developed its own warning system, called NIWS, based on qualitative analysis procedures that are well-defined and focused on specific events. According to NATO doctrines, NIWS covers not only threats to NATO but also a wide range of military and non-military risk indicators, including insecurity and instability in and within the Euro-Atlantic area and the possibility of new regional crises in the periphery. Once a warning topic is established, NIWS begins monitoring on a monthly basis, or more frequently if needed. It is important to understand that a "warning" is not an event, but a cyclical process of assessing an identified crisis or threat, defining a problem, and developing a critical list of indicators. NIWS is not just about the evolution of a crisis or threat, but about identifying a problem of interest to the Alliance as quickly as possible, developing a critical list of indicators of how and how fast that problem is evolving, and issuing warnings as appropriate. Of course, this is more than difficult in today's complex and diverse security environment, as it is in Ukraine.

2.3. Uses of EWS in the prevention of financial and banking crises

In finance, crises occur at more or less frequent intervals, but they have a significant economic and social impact. Their prediction relies too little on warning systems, although business intelligence, data mining and specialized dashboard solutions can be found in banks, investment firms and government agencies. But these are inconsistent, and results are interpreted differently. Entrepreneurship, new types of complex products, the unexpected reaction of people generate different interpretations and perceptions. It was only after the 2008 crisis that banking authorities began to centralize information and decisions and to unify them. Sławiński (2021) notes that the 1929 crisis was a liquidity crisis: liquidity disappeared from the market, banks stopped communicating with each other, funding for troubled securities firms was cancelled, deposits created by the multiplication of banks disappeared, and cash was reduced by one-third. Of course, panic played an important role in every banking crisis. The lesson was learned, and the 2007-2009 crisis was managed by a substantial injection of funds over a long period of time, even though the impact of the crisis was devastating for many. This global approach was also made possible by the strong interconnectedness of financial systems and IT-based analysis. The rapid response was possible because of the triggers that signalled the problems in time. But what triggered the crisis also relied on the new information and telecommunications systems that enabled rapid, decentralized trading that helped move some toxic products to safety without centralized monitoring or early warning systems. The systems set up after these crises, the new standards applied using high performance computer systems, also created the possibility of real-time analysis that played the role of an early warning system. Thus, the crisis caused by the pandemic COVID did not cause the same economic shocks as the previous crises. This was made possible by the introduction of comprehensive regulations, the increasing role of central banks, their interconnectedness, and the macro prudential approach. Acharya (2013) notes that "a macro prudential or system-wide approach to financial sector capital requirements required a prompt response in the early stages of the crisis to get banks to reduce their reliance on short-term debt by issuing equity to pay down maturing debt. This laid the foundation for an early warning system in the banking sector."

According to Frankel & Saravelos (2012), a specific approach to early warning indicators (EWIs) in finance is proposed, focusing on foreign exchange reserves, exchange rates, credit growth, GDP, and current account balance, with the suspicion that "indicators that have proven to be useful predictors in one round of crises are usually not useful in predicting the next round." At the same time, Bordo & Meissner (2016) mention that "overemphasizing one or a handful of indicators can be misleading, if not dangerous, for economic and financial stability."

In conclusion, several recent studies have worked to improve early warning models by developing new techniques and using more extensive data sets. In particular, decision makers have been given the explicit ability to pre-select their preferences for false alarms and then evaluate indicators for their usefulness with respect to those preferences (Alessi & Detken, 2011).

3. R&D of the pilot platform and elements of innovation

The main advantage of using open-source technical solutions is that there is no additional cost for the beneficiary, which is caused by the licenses for the application software. These free licensed programs are also characterized by numerous updates, faster corrections and high-quality documentation. The open-source solutions specified in the technical offer have been used by the provider for the successful implementation of similar projects. For example, the Integrated Information System for Activity Management (SIIMA) project for Special Telecommunications Service (STS) developed ten modules that can be made available to other entities within SNSOPA for back-end functions, integration, identity management, Business Process Management (BPM), Geographic Information System (GIS) and notifications. STS-validated open-source solutions will be used.

Online web portals are the most important and offer a multifunctional IT system that provides a secure point of access to a wealth of information and services through a web interface (Petre et al., 2018). The functional architecture of the system consists of the following modules, sub-modules, and functional blocks as shown in Figure 1.

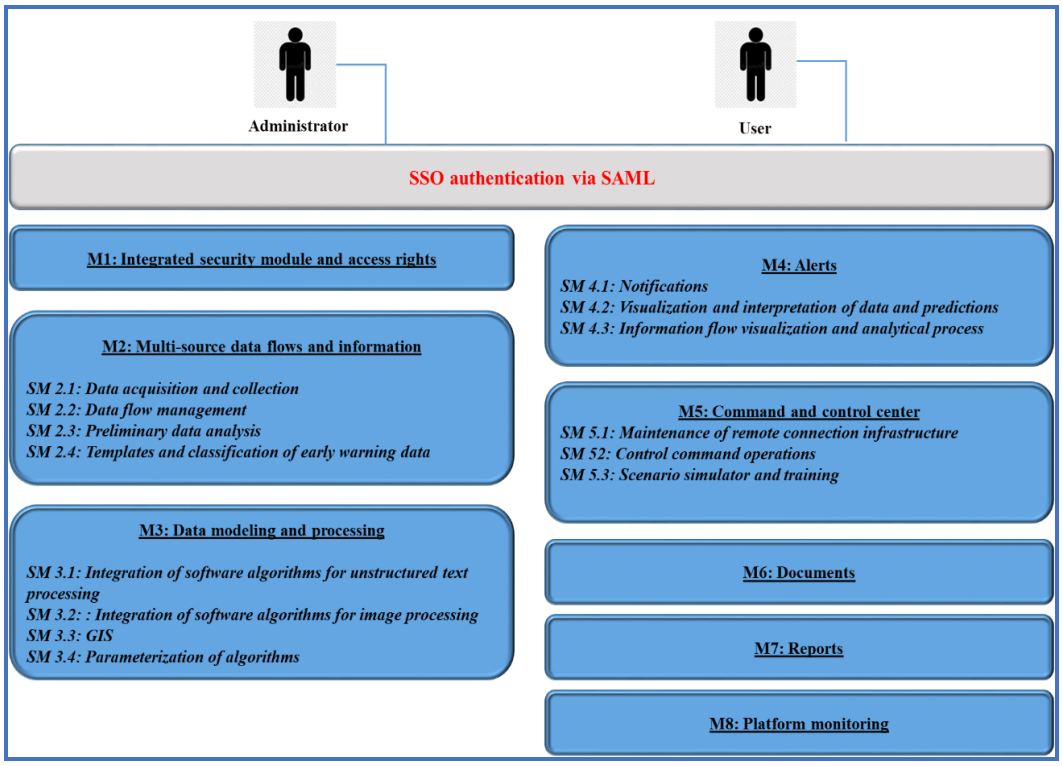

Figure 1. The functional architecture of the system

M1. *Integrated security module and access rights* - it is a unique authentication system which provides unified management of user accounts (creating user accounts, defining users, user groups, and defining access rights to various functions and information) and of authorization rules and a platform-level secure multi-factor authentication mechanisms through the functional blocks which follow it.

The type of configuration of roles is uniform, unlimited in number and takes into account: mode, operation, type of information, organization level, etc. This ensures access to information according to the defined role. The WSO2 Governance Registry component allows you to define the organization's information resources and their dependencies. The registry of these information resources is available through the services SOAP or REST WEB and can be used by all other existing software modules at the organization level, i.e., implicitly by all modules of the platform. It allows the definition of taxonomies that can be used to model/redesign the organizational structure. The database will be implemented and managed through an integrative software platform based on open-source technology used to:

- integrate data from systems with multiple sources;
- allow the development of a mobile component connected to portable devices capable of collecting data in real time, with the possibility of extending subsequent connectivity to other types of wearable devices and the part of dynamic display, validation of correlations and offline and real models-time;
- allow the development of a correlation model between the recorded data, the use of historical data to identify possible correlation models, the validation of historical models using historical data from a different time period. the validation of historical models using real-time data.

    - *Innovation elements*: the module includes WSO2 Business Process Server, BPMN, Activity, Apache Orchestration Director Engine (ODE), WS-BPEL, WSO2 Developer Studio, WSO2 Business Activity Monitor (BAM), Apache Hadoop, Map Reduce, SSL.

M2. *Data and information flows from multiple sources* - the solution, characterized by a set of ICT web-based solutions, ensures first the fluidity and accuracy of the information flows acquired and structured then integrated and accessed within the platform (Postolache, 2016), and secondly, enables integrated management (storage, processing, analysis, visualization) on large amounts of real-time relevant data and information.

- *SM 2.1 Data acquisition and collection* - the acquisition of data from various sources (open data sources, own data sources) and their local storage; identification and centralization of data flow sources; data collection. WSO2 Identity Server component provides platform level identity services. Any other source of identity data is configured at the level of this infrastructure service and allows configuring LDAP directory data sources or relational databases whose number is unlimited. Once a new source of identity data is added at the identity server level, users defined in the new source can authenticate via SAML to any of the systems registered as "service providers" at the identity server level;
- *SM 2.2 Data flow management* - in this sub-module the orchestration of data and information flows takes place;
- *SM 2.3 Preliminary data analysis* - in this sub-module both manual and automatic data analysis are performed using standard statistical methods;
- *SM 2.4 Templates and classification of early warning data* - this sub-module allows managing data standards and nomenclatures for the data collected in the system.

M3. *Data Modelling and Processing* - provides functional capabilities for modelling and controlling the logical structure of processes. The WSO2 Business Process Server component provides the ability to model and harmonize the coordinated execution of business processes at the organizational level. The creation of new business processes or the adaptation of the existing ones is done by uploading the new model in the standardized format (WS-BPEL or BPMN) and publishing connectors of the Web Service type to make them available at the infrastructure level.

- *SM 3.1 - Integration of software algorithms for processing unstructured texts* - within this module, the integration of block chain technologies, artificial intelligence tools and algorithms for extracting information from unstructured sources is achieved;
- *SM 3.2 - Integration of software algorithms for image processing*;
- *SM 3.3 - GIS* - The system enables the step-by-step display of the results of GIS simulations in the form of a "time scale" to provide a clear and easy-to-use picture of the evolution of the simulated events when making decisions. GIS data analysis allows the visualization of geodata at map level, with the possibility of selecting thematic layers and creating spatial perimeters of polygonal type. It can be integrated with any module that requires a geographic representation of the modelled resources.
- *SM 3.4 Parameterization of algorithms* - allows the modification of the values of the parameters of the analysis and modelling algorithms.

- *Innovation elements*: the sub-module includes GeoServer, WMS, Shape File, Leaflet, SSL.

M4. *Alerts*

- *SM 4.1 Notifications* - allows viewing active notifications allows viewing the list of notifications of the current user generated due to existing conditions in business processes, or notifications generated manually by another user; sending notifications allows you to define the information structure of the notification and send it to a recipient or a group of recipients in the system. The WSO Message Broker component of WSO2 Enterprise Integrator provides these features using the MQTT protocol. The possible unavailability of the target system does not affect the communication, as the message can be delivered as soon as the target system returns.
    - *Innovation elements*: include WSO2 Enterprise Service Bus, WSO2 Message Broker.
- *SM 4.2 Visualization and interpretation of data and predictions*
    - *Innovation elements*: the sub-module module includes WSO2 Enterprise Service Bus and WSO2 Message Broker. The WSO Message Broker component of WSO2 Enterprise Integrator provides this MQTT protocol interface. Any unavailability of the target system is not a condition for communication, the message must be available to the target system.
- *SM 4.3 Information flow visualization and analytical process*
    - *Innovation elements*: it includes WSO2 Analytics, WSO2 Business Activity Monitor, Report Server Community.

M5. *Command and control centre*

- *Innovation elements*: the module includes WSO2 Business Process Server, BPMN, Activity, Apache Orchestration Director Engine (ODE), WS-BPEL, WSO2 Developer Studio, WSO2 Business Activity Monitor (BAM), Apache Hadoop, Map Reduce, SSL.

- *SM 5.1 Maintenance of remote connection infrastructure*
- *SM 5.2 Command and control operations*
    - *Innovation elements*: include WSO2 Analytics, WSO2 Business Activity Monitor, Report Server Community.
- *SM 5.3 Scenario stimulator and training* – this sub-module provides simulations and templates for crisis situations, specializing in operational areas, logistics, readiness assessment, etc. It also enables assisted practice of situations for incident analysis, configuration of incident scenarios, analysis of simulator data and generation of suggested actions.
    - *Innovation elements*: include WSO2 Business Process Server, BPMN, Activity, Apache Orchestration Director Engine (ODE), WS-BPEL, WSO2 Developer Studio, WSO2 Business Activity Monitor (BAM), Apache Hadoop, Map Reduce, SSL.

M6. *Documents module* enables the automation of the internal information cycle, for documents in electronic format and for the transmission of documents within the institution, with the definition of the technical requirements and procedure for the security of information and the need to inform a unit of interest and to stabilize common agendas between specific units. Document management and communication allows the modelling of documents and the creation of a classification scheme, the modelling of registers and of authorizations, the registration of documents and fields for general purposes with the aim of automatic mail processing.

- *Innovation elements*: the module includes WSO2 Governance Registry and SSL.

M7. *Report module* - allows you to configure data sources and report templates that authorize you to define the data sources used to receive reports and record report templates with

preference to the data sources used; Jasper Reports and BIRT report templates can also be registered. Scheduling regular execution of reports allows you to plan the execution of reports and send them by e-mail to the configured recipients while "AD HOC" reports allow you to select the query data source, columns and rules for data display.

- *Innovation elements*: the module includes WSO2 Analytics, WSO2 Business Activity Monitor, Report Server Community.

M8. *Platform availability monitoring* - enables the configuration of monitoring rules that allow the definition of monitored devices and software systems, as well as monitored parameters; the configuration of notification rules (EMAIL, SMS) enables the definition of conditions that trigger notification when defined normality intervals are exceeded; availability monitoring provides functions for evaluating the technical state and availability of the platform through a graphical interface that enables individual tracking of each component of the platform or at the group level of the components.

- *Innovation elements*: the module includes ZABBIX Server, Zabbix Agent, JMX, SNMP.

4. Expected impact

The effect of implementing the ECRIS early warning platform is twofold.

- Firstly, lives could be saved thanks to earlier and more warning and decision support systems, as well as specially tailored online services meant to support citizens' self-preparedness, self-protection, and self-reaction.
- Secondly, although most economic impacts are difficult, if not impossible, to avoid, in many cases they could be mitigated by thoroughly improving preparedness through earlier forecasting coupled with more effective support systems which leads to a better coordination of emergency response efforts.
- The main expected impact is to provide advanced technological innovations to emergency response agencies in their management actions before and during disasters and emergencies, especially to support their decision-making processes to enable faster and more efficient responses.

5. Results and discussions

Contributions to solving the problem of crisis prevention are essential in practice, because despite technological progress, crisis management is still quite inefficient, especially because the introduction of new technologies can be disruptive and ineffective. Moreover, there is still no systematic approach to solving the problem of decision support at the strategic, operational, and tactical levels. In extreme situations, interorganizational systems of government agencies have a critical need for decision support to prepare effective mitigation actions and develop responses at the regional level.

The ECRIS project addresses a number of current challenges in crisis management: poor interagency coordination at the operational level, demultiplication of EMS architectures due to technological advances, lack of institutional authority, and lack of knowledge/understanding of the field that translates into decisions.

Risk management in innovative projects is extremely important for all stakeholders: for the sponsor, by identifying the balance between project deliverables and allocated funding; for the project manager, by identifying sources of risk and approaches to resolution; for the end users, by helping to meet needs and add value to investments.

The design and development of the ECRIS early warning platform must consider all specific phases of the systems engineering process: the risk analysis based on identification of operational, functional and performance requirements and the system analysis and control focusing on balancing requirements, costs and risks. For the ECRIS early warning platform, an analysis of the risks associated with the software, hardware, and communications elements is also required.

The expected outcomes and benefits go beyond the purpose of the platform. The scientific approach is consistent with the current needs of society. The approach is not selective, especially not focused only on one institution, but focuses on the concepts of interoperability and alignment with EU standards, using the latest technologies to implement the application of identification and assessment of early warning indices for the management of crisis situations. The updating of methods (procedures, instructions), elaboration and testing of the application for identification and assessment of early warning indices for crisis management demonstrate a high level of operational technological maturity. The systemic approach to the design of the solution opens up further development perspectives for the beneficiary. At the level of application modules for identifying and evaluating early warning indices for crisis management, the beneficiary can scale the solution with new functionalities (modified or improved data collection procedures, a standardized interface) or increase processing capacity, storage space, application (number of users), etc. The opening and connection to information flows and other information systems in the national security system, almost in real time, is an undeniable advantage for the security environment in Romania and consequently for the construction of an integrated national capacity to act accordingly.

6. Conclusion

The critical role of the Early Warning Platform is to provide innovative solutions that go beyond existing technology levels to meet the operational needs of institutions within the national security system to provide a hardware and software tool that supports decision making and coordination of activities in crisis situations.

The pilot platform for identification and evaluation of early warning indicators in crisis management adds value to the early warning domain through:

- development of a technological approach based on methods and algorithms for identification, evaluation and visualization of results;
- research, design, test and validation of a technical solution for identification, assessment and visualization of results under laboratory conditions;
- development of a hardware and software platform for the identification and assessment of early warning indicators for crisis management, validation of the results through testing and evaluation of demonstrators/functional models in the operational environment;
- the operationalization of a pilot center for the identification and assessment of early warning indicators for crisis management within the National Defence College, ICI Institute, SafeTech Innovation, and other interested institutions.

Acknowledgments

This paper was published as part of the project "Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)", Contract No. 270 / 23.06.2020, ID 120436, funded under the Operational Program Competitiveness 2014-2020, Priority Axis: 1. Research, Technological Development and Innovation (RDI) to support economic competitiveness and business development.

REFERENCES

1. Acharya, V. (2013). *Understanding Financial Crises: Theory and Evidence from the Crisis of 2007-08*. NYU Stern School of Business, EPR and NBER.
2. Alessi, L. & Detken C. (2011). *Quasi Real Time Early Warning Indicators for Costly Asset Price Boom/Bust Cycles. A Role for Global Liquidity*. European Journal of Political Economy, 27(3), 520-533.

3. Bordo, M. & Meissner, C. (2016). *Fiscal and Financial Crises NBER*. Working Paper No. 22059 JEL No. E62, G01, N1. Available at: <http://www.nber.org/papers/w22059.ack>, last accessed: 10th of February, 2022.
4. Brune, S. C., Kovacs, A., Reding, A. & Penny, M. (2015). *Crisis and conflict prevention strategies. An international comparison*. RAND Corporation, Santa Monica.
5. Frankel, J. & Saravelos, G. (2012). *Can leading indicators assess country vulnerability? Evidence from the 2008–09 global financial crisis*. Journal of International Economics, 87(2), 216-231.
6. Niculescu-Mizil Gheorghe, P., Vasuthanasub, J. & Gheorghe, A. (2019). *The Resilient City: A Platform For Informed Decision-Making Process*. Romanian Cyber Security Journal, 1(2), 23-29.
7. Petre, I., Cohal, A. M. & Boncea, R. (2018). *Platforma de e-Participare pentru facilitarea implicării cetățenilor în inițiativele Smart City*. Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control), 28(2) 5-14.
8. Popescu, F. (2019). *Modeling a Hybrid Early Warning System for complex and large projects: Predictions and warnings at different stages of time*. Lambert Academic Publishing, Germany.
9. Popescu, F. & Ichimescu, C. (2021). *Building, training and validation an artificial intelligence-assisted Early Warning System for COVID-19 pandemic management*. Revista Română de Informatică și Automatică (Romanian Journal of Information Technology and Automatic Control), 31(2), 7-20.
10. Postolache, Fl. (2016). *Ontology tool for knowledge acquisition in a virtualised ict infrastructure*. „Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1, pp: 484-489, ISSN 1454-864X, Published by „Mircea cel Batran" Naval Academy Press, Constanta, Romania.
11. Sławiński, A. (2021). *What did central banks learn from financial crises?*, Studies in Logic, Grammar and Rhetoric, 66(79), 497-512. DOI: 10.2478/slgr-2021-0028, last accessed: 7th of January, 2022.
12. Schmid, A. (1998). *Indicator Development: Issues in Forecasting Conflict Escalation*. In: Davies, J. L. & Gurr, T. R. (eds.), Preventive Measures: Building risk Assessment and Crisis Early Warning Systems . Rowman & Littlefield Publishers.
13. UNISDR (2009). *Terminology on Disaster Risk Reduction*. Geneva. Available at: <http://www.unisdr.org/we/inform/publications/7817>.
14. United Nations (2006). *Global Survey of Early Warning Systems*. New York. Available at: <http://www.unisdr.org/2006/ppew/info-resources/ewc3/Global-Survey-of-Early-WarningSystems.pdf, last accessed: 17th of April, 2022.
15. United Nations Environment Programme (2012). *Early Warning Systems: A State of the Art Analysis and Future Directions*. Division of Early Warning and Assessment (DEWA). United Nations Environment Programme (UNEP), Nairobi. Available at: http://na.unep.net/siouxfalls/publications/Early_Warning.pdf, last accessed: 11th of March, 2022.

Vasile Florin POPESCU is Assoc. Professor PhD. Eng. Ec. at the National Defense University "Carol I" – Department of Information systems and cyber defense, he has a Ph.D. in industrial engineering at the POLITEHNICA University of Bucharest and he is also expert (EX2020D386217) to assist the European Commission in evaluating the European Industrial Development (EDIDP) and the European Defense Fund (EDF). He is also acting within EOSC Future User Group as expert to co-design EOSC Future services and solutions. He is reviewer for

internationally recognized publications such as SAGE Publishing, United Kingdom and IGI Global Discovery, USA. The results of the research were disseminated to prestigious international publishers who work closely with expert researchers and professionals from top institutions, including the Massachusetts Institute of Technology (MIT), Harvard University, Stanford University.

Vasile Florin POPESCU este Conf. univ. dr. ing. ec. la Universitatea Națională de Apărare ”Carol I” - Departamentul Sisteme informaționale și apărare cibernetică, deține un doctorat în inginerie industrială în cadrul Universității Politehnica din București și este, de asemenea, expert (EX2020D386217) pentru a asista Comisia Europeană în efectuarea evaluării Programului european de dezvoltare industrială a apărării (EDIDP) și European Defense Fund (EDF). Activează, de asemenea, ca expert în EOSC Future User Group pentru proiectarea în echipă a serviciilor și soluțiilor EOSC Future. Este recenzor pentru publicații internaționale recunoscute cum sunt SAGE Publishing, United Kingdom și IGI Global Discovery, SUA. Rezultatele activității de cercetare au fost diseminate către edituri internaționale de prestigiu care lucrează îndeaproape cu cercetători experți și profesioniști din instituții de top, inclusiv Massachusetts Institute of Technology (MIT), Universitatea Harvard, Universitatea Stanford.

Victor GÂNSAC is Chief Executive Officer at Safetech Innovations, with extensive experience in the field of Information Security and IC&T, both from managerial and technical point of view. Victor Gânsac has outstanding technical knowledge and skills, supported by globally recognized certifications: CIPP/IT Certified Information Privacy Professional / Information Technology / CISSP Certified Information Systems Security Professional / CSSLP Certified Secure Software Lifecycle Professional / CISM Certified Information Security Manager / CISA Certified Information Systems Auditor.

Victor GÂNSAC este Directorul General al companiei Safetech Innovations, cu o vastă experiență în domeniul Securității Informaționale și TIC, atât din punct de vedere managerial, cât și tehnic. Victor Gânsac are cunoștințe și abilități tehnice deosebite, susținute de certificări recunoscute la nivel mondial: CIPP/IT Certified Information Privacy Professional / Information Technology / CISSP Certified Information Systems Security Professional / CSSLP Certified Secure Software Lifecycle Professional / CISM Certified Information Security Manager / CISA Certified Information Systems Auditor.

Olivia COMȘA is currently working as Research and Development Manager at Safetech Innovations and is developing innovative projects on cybersecurity. She has outstanding experience in research and development, working as RTD Program Manager for MHTC-Magurele High Tech Cluster MHTC, as Senior Researcher for CITON - Center of Technology and Engineering for Nuclear projects, as External Relations Manager within European Commission, DEVCO, Nuclear Safety and Security United. Over time, Olivia Comșa developed, coordinated, implemented and monitored projects on nuclear safety and security under INSC and IfS instruments.

Olivia COMȘA lucrează în prezent ca manager de cercetare și dezvoltare la Safetech Innovations și dezvoltă proiecte inovatoare în domeniul securității cibernetice. Are o experiență remarcabilă în cercetare și dezvoltare, lucrând ca Manager Program RTD pentru MHTC-Măgurele High Tech Cluster MHTC, ca cercetător senior pentru CITON - Centrul de Tehnologie și Inginerie pentru Proiecte Nucleare, ca Manager Relații Externe în cadrul Comisiei Europene, DEVCO, Securitate şi Siguranţă Nucleară. De-a lungul timpului, Olivia Comșa a dezvoltat, coordonat, implementat și monitorizat proiecte de securitate şi siguranţă nucleară pentru INSC și IfS.

Marius Sorin PISTOL is an SOC analyst at the European Union Asylum Agency, part of the team that monitors and combats threats to the IT infrastructure of the Agency. He is also collaborating with the security company Safetech Innovations in different R&D projects. He is currently a Ph.D. student at the Faculty of Applied Sciences at the POLITEHNICA University of Bucharest, the topic of his Ph.D. thesis being „Warning system against data exfiltration from mobile phones".

Marius Sorin PISTOL este analist SOC la Agenția Uniunii Europene pentru Azil și face parte din echipa care monitorizează și combate amenințările la adresa infrastructurii IT din cadrul agenției. De asemenea, este colaborator cu Safetech Innovation în diferite proiecte de cercetare-dezvoltare. În prezent este doctorand la Facultatea de Științe Aplicate, din cadrul Universității Politehnica din București, tema lucrării de doctorat fiind „Sistem de avertizare împotriva exfiltrării datelor din telefoanele mobile".

Cristian ICHIMESCU is currently director of department in the "Carol I" National Defense University. His fields of specialization include: Information Operations, Crises Management, Military Art and Multinational Operations. He has authored and co-authored a number of 2 books and 11 articles/studies published in international and national journals. He participated as a scientific researcher in two nationally funded research projects. He is also currently involved in other academic activities such as lecturing as a visiting professor at the „Ferdinand I" Military Technical Academy. He received the award of excellence of the General Stefan Gusa Foundation for the book „Fundamentals of Information Operations" in 2019.

Cristian ICHIMESCU este în prezent director de catedra în cadrul Universității Naționale de Apărare „Carol I". Domeniile sale de specializare includ: operațiuni informaționale, managementul crizelor, artă militară și operațiuni multinaționale. Este autor și coautor a unui număr de 2 cărți și 11 articole/studii publicate în reviste internaționale și naționale. A participat în calitate de cercetător științific la două proiecte de cercetare finanțate la nivel național. În prezent, este implicat și în alte activități academice, cum ar fi predarea ca profesor invitat la Academia Tehnică Militară „Ferdinand I". A primit premiul de excelență al Fundației General Ștefan Gușă pentru cartea „Fundamentals of Information Operations" în 2019.

Călin Mihai RANGU is university lecturer, and Dean of Faculty of Economic Sciences and Business Administration of Danubius University of Galați, resolution director of Insurance Guarantee Fund in Romania, Ph.D. in neural networks applied in financial series processing, double degree in engineering and economics, graduate of post-university studies, MBA graduate of the City University of Seattle - US, scientific researcher in the field of communications, co-founder of CIO Council Romania. He has over 25 years of experience in the financial-banking field, in the field of information systems management, of which over 17 years of strategic and operational management in private companies and financial authorities. He was President of the Institute of Financial Studies, Vice-President of the InsurTech Committee of the European Insurance and Occupational Pensions Authority, Member of the European Financial Innovation Forum at EU level. He has published books, and over 100 specialized articles in the field of IT, financial-banking, banking technologies, security computer systems and not only.

Călin Mihai RANGU este lector universitar și decan al Facultatea de Științe Economice și Administrarea Afacerilor a Universității Danubius din Galați, director de rezoluție în cadrul Fondului de Garantare a Asiguraților din România, doctor în rețele neuronale aplicate în prelucrarea seriilor financiare, dublu licențiat în inginerie și economie, absolvent de studii postuniversitare, absolvent de MBA al Universității din Seattle - SUA, cercetător științific în domeniul comunicațiilor, cofondator CIO Council România. Are o experiență de peste 25 de ani în domeniul financiar-bancar, în domeniul managementului sistemelor informatice, din care peste 17 ani de management strategic și operațional în companii private și autorități financiare. A fost Președinte al Institutului de Studii Financiare, Vicepreședinte al Comitetului InsurTech al Autorității Europene pentru Asigurări și Pensii Ocupaționale, membru al Forumului European de Inovare Financiară la nivelul UE. A publicat cărți și peste 100 de articole de specialitate în domeniul IT, financiar-bancar, tehnologii bancare, sisteme informatice de securitate și nu numai.

Mircea-Constantin ȘCHEAU has a Ph.D. in Public Order and National Security with a theme of interest for the economic and security domain *„Cybercrime regarding Financial Transfers”*, who received „Victor Slăvescu Prize” awarded by Romanian Academy. Author / co-author of three volumes, more than forty scientific articles on management, law enforcement, critical infrastructure, information technology, artificial intelligence, defense, cybersecurity, lecturer in numerous international conferences, Honorary associate researcher at University of Craiova and member, inter alia, of European Research Institute at Babeș-Boyai University.

Mircea-Constantin ȘCHEAU deține un doctorat în Ordine Publică și Siguranță Națională cu o temă de interes pentru domeniul economic și de securitate *„Criminalitatea informatică privind transferurile financiare”*, care a primit Premiul „Victor Slăvescu” acordat de Academia Română. Este autor / coautor pentru trei volume, mai mult de patruzeci de articole științifice privind

managementul, aplicarea legii, infrastructurile critice, tehnologia informației, inteligența artificială, apărarea, securitatea cibernetică. Este lector în numeroase conferințe internaționale, Cercetător asociat onorific al Universității din Craiova și membru, printre altele, al Institutului de Cercetări Europene din cadrul Universității Babeș-Bolyai.

Cătălin CIOACĂ is Associate Professor at „Henri Coandă" Air Force Academy in Braşov, Management and military sciences department. He obtained his Doctorate Degree in 2014 at the Transilvania University of Brasov in the field of *Engineering and Management*. He is the author and co-author of 10 books published by national and foreign publishers, and has published over 40 scientific papers in the field of risk management, using multidisciplinary approaches such as stochastic analysis and modeling, real options analysis, systems engineering, decision systems support, strategic management and security of socio-technical systems. He has also participated in 12 research and development projects as project director or member in the research team. He is currently leading three research projects within the sectoral research and development plan of the Ministry of National Defence in the field of autonomous air systems and Internet-of-Bodies architectures, is the initiator of the postgraduate program „Conflict Management and Negotiation Strategies" and Editor-in-Chief of the Review of the Air Force Academy journal.

Cătălin CIOACĂ este conferenţiar universitar în cadrul Academiei Forţelor Aeriene „Henri Coandă" din Braşov, Departamentul de management și științe militare. A obţinut titlul de doctor în anul 2014 la Universitatea Transilvania din Braşov, domeniul *Inginerie şi management*. Este autor și coautor a 10 cărţi apărute la edituri din ţară și străinătate, a publicat peste 40 de lucrări stiinţifice în domeniul managementului riscului, prin utilizarea unor abordări multidisciplinare, cum ar fi analiza şi modelarea stochastică, analiza opţiunilor reale, ingineria sistemelor, sisteme decizionale suport, management strategic şi securitatea sistemelor socio-tehnice. A participat, de asemenea, la 12 proiecte de cercetare-dezvoltare în calitate de director de proiect sau membru în echipa de cercetare. În prezent, conduce trei proiecte de cercetare din cadrul planului sectorial de cercetare-dezvoltare al M.Ap.N. în domeniul sistemelor aeriene autonome și arhitecturilor de tipul Internet-of-Bodies, este iniţiatorul programului postuniversitar „Managementul conflictelor şi strategii de negociere" și redactor-şef al revistei „Review of the Air Force Academy".