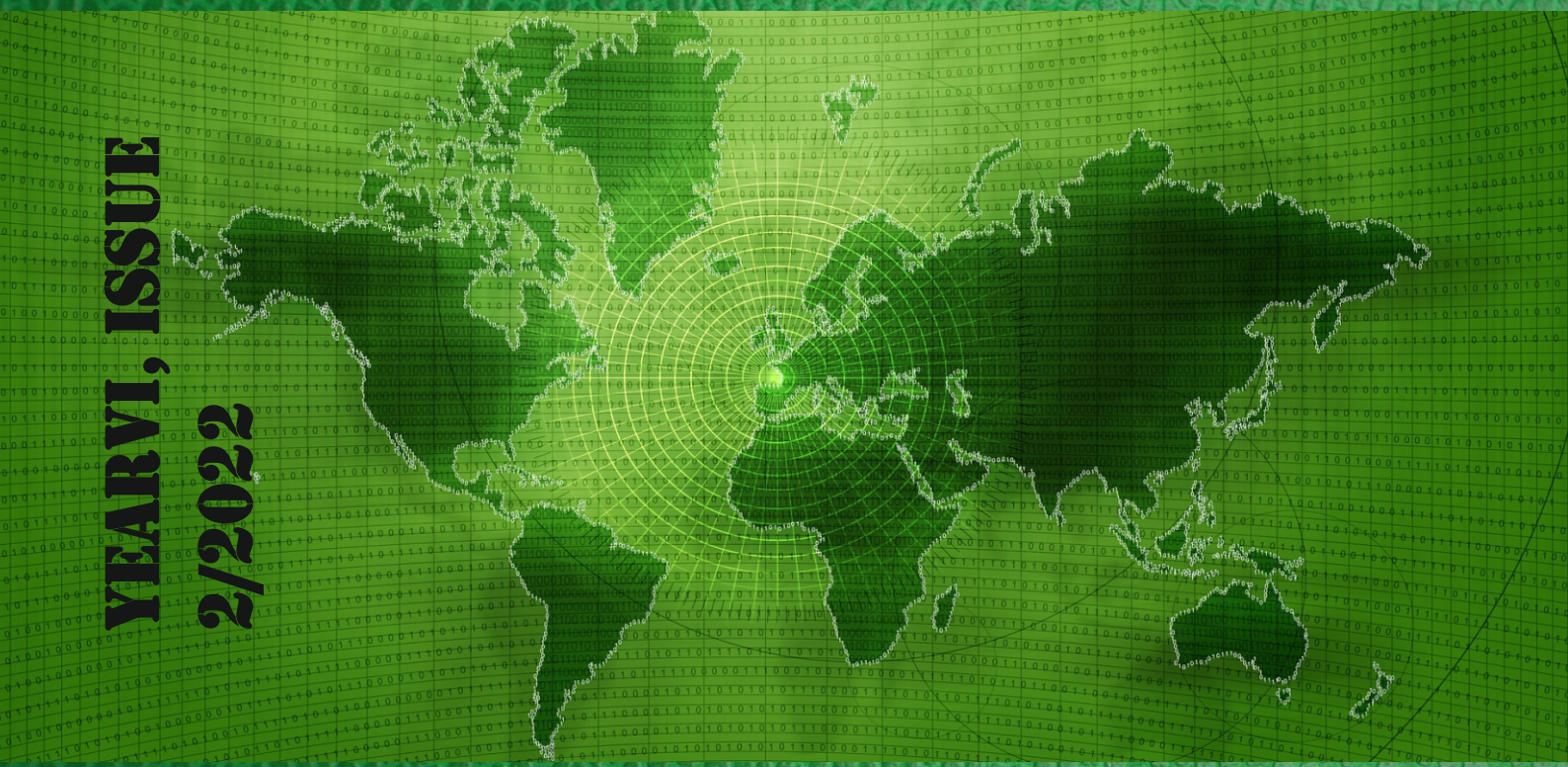
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

ISSN: (PRINT) 2535-0668
ISSN: (ONLINE) 2535-082X



YEAR VI, ISSUE 2/2022

PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA

INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

PUBLISHER:

SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0

108, Rakovski Str., 1000 Sofia, Bulgaria

tel. (+359 2) 987 72 90, **tel./fax** (+359 2) 986 22 40**,**

office@stumejournals.com,

www.stumejournals.com

ISSN (PRINT) 2535-0668; ISSN (Online) 2535-082X

YEAR V, ISSUE 2 / 2022

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov

New Bulgarian University, Sofia, BG

Members:		
Alexander Baranov, Prof.	Higher School of Economics	RU
Alexander Kurbatski, Prof.	Belarusian State University	BY
Alexander Troyanskiy, Assoc. Prof.	Odessa State Polytechnic University	UA
Andrzej Misiuk, Prof.	Warsaw University	PL
Ariana Bejleri, Assoc. Prof.	Polytechnic University of Tirana	AL
Galina Zhavoronkova, Prof.	National Aviation University, Kyiv	UA
Gudrun Biffl, Prof.	Donau University	AT
Dimitar Dimitrov, Prof.	Shumen University	BG
Evgeni Manev, Prof.	University of Library Studies and Information Technologies	BG
Hanáček Petr, Assoc. Prof.	Technical University of Brno	CZ
Iliyan Lilov, Prof., Col.	"Vasil Levski" National Military University	BG
Jaroslav Tureček, Assoc. Prof., Col.	Police Academy of the Czech Republic	CZ
Josef Reitšpís, Prof.	The University of Security Management in Kosice	SK
Juris Borzovs, Prof.	University of Latvia	LV
Kristiina Hakk, Assoc. Prof.	Estonian Information Technology College	EE
Kiril Stoychev, Prof.	Institute of Metal Science – BAS, Sofia	BG
Lev Elisov, Prof.	Moscow State Technical Univercity of Civil Aviation	RU
Milan Popović, Prof.	University of Montenegro	ME
Muhammed Ali Aydin, Assoc. Prof.	Istanbul University	TR
Nebojša Bojanić, Assoc. Prof.	University of Sarajevo	BA
Nikifor Stefanof, Prof.	University of Security and Economics - Plovdiv	BG
Ninoslav Marina, Prof.	University of Information Science and Technology - Ohrid	MK
Nurgali Zaurbekov, Prof.	Almaty Technological University	KZ
Oliver Bacanovic, Prof.	University "St. Kliment Ohridski" - Bitola	MK
Ognyan Ivanov, Assoc. Prof.	Institute of Solid State Physics, BAS - Sofia	BG
Piotr Majer, Prof.	University of Warmia and Mazury	PL
Razvan Rughinis, Prof.	Polytechnical University of Bucharest	RO
Siniša Tatalović, Prof.	University of Zagreb	HR
Stoyan Denchev, Prof.	University of Library Studies and Information Technologies	BG
Tatyana Ejevskay, Prof.	Transbaikal State University	RU
Valentin Todorov, Assoc. Prof.	Varna Free University „Chernorizets Hrabar"	BG
Vladimir Zakhmatov, Prof.	Academy of Ecological Safety, Kiev	UA
Zelimir Kesetovic, Prof.	University of Belgrade	RS

C O N T E N T S

THEORETICAL FOUNDATIONS OF SECURITY

Green Agenda and Green Consumerism in the Function of Plural Society in the Bosnia and Herzegovina and its Energy Security
Slijepcevic Dusanka, Dabrowska-Prokopowska Ewa,Vejnovic Dusko 47

Some benefits of building key partnerships to develop security systems
Valeri Panevski 51

Possible structure of standard operating procedure to ensure the operation of security systems
Valeri Panevski 55

NATIONAL AND INTERNATIONAL SECURITY

Analysis of barriers to adaptation to climate change
Titko Michal, Jana Studená, Jozef Ristvej, Alexander Kelíšek 59

Brief description of the identification of vital areas in nuclear facilities process
Dmitar Dimitrov, Lyudmil Nedelchev 64

Possible approaches to ensure security of information for nuclear facilities
Dimitar Dimitrov 68

Cyber warfare, a new aspect of modern warfare
Fatmir Basholli 72

INFORMATION SECURITY

Information security in archival science
Teodora Licheva 75

Blockchain based solution for securing real property transaction: a case study for North Macedonia
Admirim Aliti, Elva Leka; Marika Apostolova; Artan Luma 78

TECHNICAL FACILITIES FOR ENSURING SECURITY

Technological development: Thermal vision as a phenomenon
Pavel Zahradnicek, Jan Hrdinka, Jan Zezula, Ludek Rak 82

Principle of Operation and Advantages of a Sensor for Fog Contamination Detection
Ognyan Ivanov, Petar Todorov, José Luis Pérez-Díaz, Tihomir Tiankov 84

Green Agenda and Green Consumerism in the Function of Plural Society in the Bosnia and Herzegovina and its Energy Security

Slijepcevic Dusanka[1,*], Dabrowska-Prokopowska Ewa[2], Vejnovic Dusko[3]
Faculty of political Sciences – University of Banja Luka, Banja Luka, Bosnia and Herzegovina[1]
Institute of Sociology, Biallystok, Poland[2]
Faculty of security sciences, Banja Luka, Bosnia and Herzegovina[3]
dusanka.slijepcevic@fpn.unibl.org, ewa.dabrowska@uwb.edu.pl, dusko.vejnovic@fbn.unibl.org

Abstract: *The problem is the lack of social consensus in Bosnia and Herzegovina (hereinafter B&H), as a plural society (hereinafter PS), which is why it is directed with its segments to the only sustainable joint activity of the segments - the market, and related economic activities. The subject are the characteristics of alternative development solutions - Green Agenda (hereinafter GA), green and circular economy (hereinafter GE, CE) and green consumerism (hereinafter GC), which are in the function of PS. We accept the hypothesis that the unsolved pre-political (cultural) issues of B&H even in the 21st century condition the application of alternative development solutions - GA, GE, CE and GC, which are in the function of PS and its energy security (hereinafter ES). The scientific goals are: 1) description of the peculiarities of PS in B&H, 2) understanding the importance of GA for the Western Balkans and the differences between the linear economic model and GE and CE, and between shallow and deep GC, and 3) explanation of functionality of GA, GE, CE and GC for PS and its ES..Analytical-deductive and comparative methods are used, along with the case study of B&H. The main result is the discovery of the functionality of GA, GE, CE and GC for the functionality of PS in B&H and its ES.*

Keywords: *PLURAL SOCIETY; GREEN AGENDA; GREEN AND CIRCULAR ECONOMY; GREEN CONSUMERISM, ENERGY SECURITY*

1. Introduction

A ***PS***, such as B&H, is composed of two or more segments, social orders, which live together in the same political community (state) without interference [18]. The specificity of PS is that among these segments, social communities, there is no social, national consensus, that is, a common social demand, due to the incompatibility of the value systems of these communities, that is, cultural groups. In PS, there are frequent public expenditures with benefits for one community and opportunity costs for others, whose demands are thus negated. Therefore, according to the PS theoretician, J.S. Furnivall, the only common meeting place of different cultures in the PS is the ***market*** [18, p. 12], because the economic desire for profit is characteristic of everyone, regardless of cultural differences. Therefore, in the absence of national consensus, economic competition between separate communities is the only viable joint activity. Therefore, their mutual relations must be guided only by the economic process, in which the production of material goods is the primary goal of social life.

Hence, the future of this country is not in conflicts but in ***collaborative consumption*** [5], which is at the center of CE and GE, as well as GC, with numerous advantages for B&H and its inhabitants: return to nature, economic savings, energy and resource savings, mitigating climate change, new jobs and similarly.

Through a common social demand - ***the market*** [22], as well as ***reflexive ("conscientious") consumerism*** [4, p. 22], it is possible to claim sustainable development and free oneself from slavery to an irresponsible, linear economic model and material pleasures. All this thanks to the fact that "we have developed the human ability to be reflective, which is to say, we have learned to look at ourselves with greater awareness and insight than before" [12, p. 11]. Therefore, "destructive consumption" needs to be replaced by "responsible consumption" [13, p. 213], where one buys "'intelligently' as a subject, not as a consumer-puppet" [13, p. 216].

What GC is and how it is connected to GA, i.e. GE and CE, and how it functions in PS in B&H and its ES, we will find out from the theoretical and methodological framework of the work that follows.

2. Theory and methods

The research problem is the lack of social consensus in B&H as a PS. That is why it is directed with its segments to the only sustainable joint activity of the segments - the market, and related economic activities.

The research subject are the characteristics of alternative development solutions - GA, GE, CE and GC, which are in the function of PS. In other words, it is the question of the analysis of alternative development proposals and their potential integrating effects. ***The research hypothesis*** assumes that the unsolved pre-political (cultural) issues of B&H even in the 21st century condition the application of alternative development solutions - GA, GE, CE and GC, which are in the function of PS and its ES.

The scientific goals of the paper are:

1) description of the peculiarities of PS in B&H,

2) understanding the importance of GA for the Western Balkans and the differences between the linear economic model and GE and CE, and between shallow and deep GC,

3) explanation of functionality (functionalist scientific explanation) of GA, GE, CE and GC for PS and its ES.

The social goals are: expanding the fund of knowledge about PS and its problems, and popularizing new approaches to consumption and affirming the model of sustainable development for PS in B&H.

The analytical-deductive and *comparative method* [15] is used, along with the technique - *a case study* [9] of B&H, which is most often used in social sciences for researching "cases of greater complexity" [14, p. 214], such as the arrangement of B&H. A "heuristic case study" was used, which serves to "verify a certain theory or hypothesis" [24, p. 64].

The main result is the discovery of the functionality of GA, GE, CE and GC for the functionality of PS in B&H and its ES.

2.1. GA, GE, CE, GC and ES

> "To consume also means to destroy. In the course of consumption, the things consumed cease to exist, literally or spiritually. They are either physically "used" to the point of complete destruction, for example when things are eaten or worn out, or they are stripped of their appeal, so they no longer arouse or attract desire and lose their ability to satisfy one's needs and desires - for example, an overused toy or a listened to record - and thus become unsuitable for consumption" [16, p. 23].

GA for the Western Balkans. It is a new growth strategy for the region, which implies a transition from a traditional economic

model to a sustainable economy, in accordance with the European Green Deal; GA is fully owned by the Western Balkan region: the six leaders adopted the declaration on the common market of the Western Balkan countries and the declaration on GA for the Western Balkans at the summit in Sofia, Bulgaria, in November 2020, in the context of the Berlin process [6]. Along with B&H, this declaration was also signed by Albania, Montenegro, Serbia and North Macedonia, which pledged to contribute to the goal of Europe to be the first climate-neutral continent, by 2050, thanks to the introduction of clean energy and the reduction of the negative impact of the use of fossil fuels in production and consumption, the promotion of carbon dioxide emissions tax, the abolition of coal subsidies, the development of market models for the use of renewable energy sources, and social benefits.

Therefore, at the center of GA is the green transition, that is, the transition from non-renewable energy sources, such as "coal, oil", whose final reserves are depleted, to renewable ones, such as "solar or hydropower" [26, p. 99 - 100].

The green transition is one of the 5 priority areas of the new *Consumer Agenda*, which represents the vision of EU consumer policy from 2020 to 2025 [7], which is essentially based on promoting a sustainable economy of reparations and product circulation.

Due to the war in Ukraine, European developed countries (Germany and Austria) are returning to coal, as an energy source, in order to overcome the crisis caused by the problem with the supply of gas and the sanctions imposed on Russia, because the European Union is still dependent on Russian gas. It only means that this war has caused major disruptions in the energy markets, which is also reflected in the implementation of the GA.

B&H lags behind developed countries in transition processes, including in terms of green transition, even though it faces a serious degree of pollution and low utilization of waste through recycling.

GE and CE. The United Nations Environment Program (UNEP) defines GE as an economy with a reduced risk of environmental degradation and deterioration of human well-being [1]. It is an economy focused on transformation towards smart, inclusive and sustainable development [according to the Europe 2020 Strategy in 1].

CE is also connected to GE. It refers to the prevention of waste generation through recycling and reuse as raw materials for further production. In 2015, the European Parliament adopted the Resolution on CE in order to use resources more efficiently, through the most important goal - 70% recycling and the abolition of incinerators and waste landfills. Therefore, it is necessary to circulate resources from nature back to nature and eliminate waste (*Zero Waste*) All in order to preserve the environment from human exploitation and thereby improve the quality of life on Earth.

By the way, Germany, Scotland and Sweden are just some of the European countries with implemented CE, and Germany is at the top of the European top list in this regard, because it is characterized by as much as 65% of recycled and composted waste from the total amount of waste materials.

Like most of the countries in the region of Southeast Europe, B&H is a developing country, so it faces significant "challenges in exploiting the advantages of the GC" [25], if it does not want to lose market share in an important export market, such as Germany, or share of green capital investments (finance for climate change, waste management, environmental protection, etc.).

GC. If consumption, and thus consumerism, refer to the consumption of things - "eating them, wearing them, playing with them and otherwise causing them to satisfy one's needs or desires" [16, p. 23], then what would GC be? GC could be defined as *an ideology about consumer activities that should be accompanied by environmental awareness about the importance of preserving public goods (primarily natural) from which everyone benefits.* GC seems particularly important in the current social constellation of neoliberal capitalism, which "has entered its most brutal phase when we are slowly and perfidiously getting used to the fact that resources and services that were previously available to everyone (water, education, health and others) are becoming more and more privileged for the rich elite and are treated as the most common commodity, not the human right of every person on the planet" [17, p. 78].

GC is consumption based on ecological criteria [20; see also 23, p. 200 - 226], thus being associated with sustainable development. It is the activity of purchasing products that most likely "do not endanger human health and do not harm the natural environment" [27, p. 21]. "Those who are aware of environmental issues will be able to demand from product manufacturers and service providers that their products and services are environmentally safe or neutral" [23, p. 202].

There is "shallow" and "deep GC" [20, p. 26], where the first does not refer to the reduction of total consumption, but only to the awareness of the importance of buying environmentally friendly products. While real GC refers to the awareness of the importance of making purchasing decisions based on ecological criteria, but also to the concrete action of reducing overall purchases in order to foster a minimalist lifestyle "consume less and live better" [23, p. 216].

ES. It represents "non-military security" [11, p. 210], more precisely environmental security [11, p. 211]. The national security of every country depends on energy stability and independence. Through GA, it is possible to provide long-term energy stability, which is why GA remains the main global process.

With the increase in consumption and the advancement of technology, the risks for ES also increase, such as: cyber attacks, terrorism, uncontrolled use of drones and the like (Radovanovic, 2019).

2.2. *Obstacles to (green) consumerism*

According to Roach, Goodwin & Nelson [20, p. 16 – 18], the limits to consumerism, as a universal consumer style, are *global poverty and non-consumer values.*

They state that over 700 million people, about 10% of humanity, live in "extreme" poverty, which the World Bank defines as living on less than $1.90 a day compared to the $10 a day income considered the minimum necessary for a certain degree economic security.

Second, in many places around the world there are traditional cultural, secular or religious values that tend to restrain, or even reject, the consumer society, such as among Muslims - the prohibition of charging interest on loans or in Buddhism - the "middle way" about material simplicity, non-violence and inner peace or in Christianity, in the New Testament, about the spiritual dangers of wealth („it is easier for a camel to pass through the eye of a needle than for a rich man to enter paradise").

In some countries, consumerism is associated with foreign, typically American, values.

Due to the expansion of consumption, which can lead to some level of global homogenization of culture among consumers, there are negative reactions to globalization. As cultural goods are also consumer goods, the expansion of consumption of imported products and services often leads to an exaggerated sense of "panic", a cultural "invasion" which, allegedly, if not contained, will result in the decline of local culture.

European policies on vacation time, parental leave and flexible working hours emphasize work-life balance. Many retail stores in France, Italy, and other European countries are usually closed at lunchtime and on Sundays.

Even in the United States of America, the spread of consumerism was not a continuous process due to periodic anti-consumerist movements that advocated a simpler, less materialistic way of life: *the Quakers* in the 18th century, *the Transcendentalists* of the mid-19th century, *the Progressives* at the turn of the 20th century, and *the Hippies* of the 1960s, to the early 1980s idea of *voluntary simplicity* to reduce the impact on environment and greater focus on family and social ties, healthy living and stress reduction.

Bonini & Oppenheim [3, p. 58] wrote about the obstacles to environmental protection, stating that they are: 1) *lack of awareness of environmentally acceptable goods and services*, 2) *their negative perception*, 3) *mistrust of them*, 4) *their higher prices* and 5) *their low availability*. So they offered simple solutions: 1) to educate consumers, 2) to make better products, 3) to be honesty, 4) to offer more, and 5) to bring products to the people.

3. Research results and discussions

How do GA, GE, CE and GC function for the benefit of the PS in B&H and its ES?

The implementation of the ***GA*** for the Western Balkans refers to 5 main areas:

1. Cleaning of energy sources, protecting the climate (decarbonization);

2. Transition to CE;

3. Removal of air, water and land pollution,

4. Building sustainable agriculture (rural areas) and food systems,

5. Protection and restoration of biodiversity and ecosystems.

So, at the center of GA is the green transition, that is, the transition to renewable energy sources.

The development of ***GE*** and ***CE*** would contribute to the creation of new companies, thus increasing employment due to the creation of new jobs and an increase in the standard of living in Europe and the world. Thus, the green transition or transformation brings competitiveness on the (European) market and survival on the planet Earth and future generations. That is why the principles of the new EU trade strategy are: *sustainability, climate neutral economy and green transformation*, on which the economic interests of B&H depend [8].

Finally, ***GC*** would imply a transition from the existing linear economic model (produce - consume - throw away) to GE and CE, as a new strategy for approaching sustainable development. All because the previous economic development was entirely based on the exploitation of natural resources, leading to environmental degradation [19] because "the limited resources of the planet are too modest to accept the levels of consumption that are growing everywhere in order to meet the standards that are currently being reached in the richest parts of the planet" [2, p. 80].

Therefore, GA, GE, CE and GC are of particular importance for the stability and future of PS, such as B&H, for the reason that they condition the transition from "what's in it for me" to "what's in it for us" way of thinking [5, p. 48], through which we see that our personal interests and collective goods depend on each other. So, for example, it is also in our personal interest to achieve ES, in addition to the fact that it is also an aspect of national security. Accordingly, GC contains a dilemma inherent in prosocial and moral actions - "giving up personal bone in favor of ... somewhat intangible gain" [21, p. 60; see also: 2, p. 72 - 83].

With the increase in the number of inhabitants and the development needs of society, the need for energy resources, i.e. for energy consumption, also increases. Hence, "the issue of the ability to provide sufficient energy resources ceases to be technical and economic, and becomes a complex financial, social, political and security issue" [19, p. 196] due to which governments can "blame globalization for the decline in the performance of their national economies", but "their own mismanagement must also be taken into account" [10, p. 145].

ES. This aspect of security has become a "global geopolitical phenomenon" [19, p. 197]. As for the ES countries of Southeast Europe (Greece, Bulgaria, Romania, Croatia, Slovenia, Albania, North Macedonia, Montenegro, B&H, Serbia), they are characterized by common features: "enough electricity, a very high degree of dependence on oil imports and natural gas, relatively high amounts of coal, outdated energy infrastructure, low level of investment in energy production from renewable sources and low level of energy efficiency" [19, p. 174]. Due to the availability of energy resources, these countries become "important factors on the geopolitical scene, or they become and remain areas that have been exposed to unrest, political turmoil and war conflicts for decades" [19, p. 196].

According to Radovanovic [19], B&H is quite energy independent due to the large reserves of coal that it uses in primary energy consumption, but because of this, it is also ecologically threatened because the use of coal leads to environmental pollution. That is why the use of renewable energy sources is sought, in accordance with the energy policy of the Energy Community, of which B&H is a member, because they "contributed to increasing energy security" [19, p. 197].

She further points out that primary energy production in B&H is mostly based on coal (43.5%), oil and oil derivatives (20.9%), biomass (15.5%), electricity (11.6%) and natural gas (7.6%).

Electricity production in B&H is connected exclusively with domestic resources - coal and hydropower. Currently, 15 large and small hydropower plants and 5 thermal power plants are active. Total electricity is produced from hydroelectric power plants (51.6%), as the cleanest and safest source of energy, and thermal power plants (49.4%).

Finally, B&H is completely dependent on the import of crude oil, but has the capacity to produce oil derivatives, thanks to Oil Rafinery a.d. "Brod". B&H does not have its own sources of natural gas, so it depends on the import of this energy source, exclusively from the Russian Federation, through transport systems via Ukraine, Hungary and Serbia.

Faster and more efficient development of capacities that use renewable energy sources and raising energy efficiency are one of the ways for each country to be independent. The bottom line is to do everything we can to be completely independent in electricity production in the coming decades.

4. Conclusions

People and the environment in B&H are increasingly affected by the global climate crisis, which is particularly noticeable in the fires. This is because in B&H over 60% of energy is still produced from "dirty" sources (coal, ...), about 30% from water resources, and only 2% from wind and solar power plants.

Therefore, B&H, like numerous other countries in the region of Southeast Europe, does not have enough energy resources for its own stable energy supply and energy development, because almost all crude oil and natural gas are imported. Although there is enough coal, its use is not the most adequate solution because of the problem of environmental pollution it produces.

The Western Balkans can secure its ES if it joins EU rules and regulations, such as GA. The transition to our own and cleaner

alternatives would ensure a cleaner and better quality of life, as well as the stability and prosperity of the inhabitants of B&H.

The war in Ukraine made the countries of the Western Balkans more vulnerable in terms of ES. Due to the global energy crisis, the energy transition it is very important. The transition envisages the gradual phasing out of thermal power plants, i.e. the abolition of electricity production from fossil fuels, such as coal, and the introduction of fees, taxes for electricity exporting countries that do not comply with these and similar directives.

In order to overcome the energy crisis, the countries of the Western Balkans will have to improve mutual cooperation within the framework of the Berlin process, e.g. in the form of joint investments in renewable energy and integration of electricity and gas markets.

Although the energy market of the Western Balkans is small, it can play a key role in European energy stability. So, for example, the Republic of Srpska is one of only a few subjects in the whole of Europe that exports a large part of the produced electricity.

Finally, the assumption was confirmed that the unsolved pre-political (cultural) issues of B&H even in the 21st century condition the application of alternative development solutions - GA, GE, CE and GC, which are the function of PS and its ES. Green Agenda, Green consumerism and green economy, because of the dangers of the economic crisis following the coronavirus pandemic and the war in Ukraine, is all the more important to integrate diverse groups in B&H.

5. References

[1] Association of Citizens "Something more" 2020. Primer of green and circular economy. https://nestovise.org › uploads › 2020/03

[2] Bauman, Zygmunt. (2011). *Collateral Damage: Social Inequalities in a Global Age.* UK: Polity Press.

[3] Bonini, Sheila & Jeremy Oppenheim. (2008). Cultivating the Green Consumer. In *Stanford Social Innovation Review.* Leland Stanford Jr. University 56 – 61. [04/09/2022]

[4] Boström, Magnus & Mikael Klintman. (2008). *Eco-Standards, Product Labelling and Green Consumerism*. England, UK: Palgrave Macmillan.

[5] Botsman, Rachel & Roo Rogers. (2010). *What's Mine Is Yours: The Rise of Collaborative Consumption.* New York, USA: Harper Collins e-books.

[6] European Commision. (2021). *Implementing a Green Agenda for the Western Balkans*. https://neighbourhood-enlargement.ec.europa.eu/system/files/2021-10/factsheet_wb_green_agenda_en.pdf [04/09/2022]

[7] European Commission. (2020). *New Consumer Agenda: Strengthening consumer resilience for sustainable recovery*. 13/11/2020 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0696; https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2069 [06/09/2022]

[8] Foreign Trade Chamber of Bosnia and Herzegovina. (2021). *Conference held on green value chains and circular economy in Bosnia and Herzegovina*, https://infokomscience.komorabih.ba/odrzana-konferencija-na-temu-zeleni-lanci-vrijednosti-icirkularna-ekonomija-u-bosni-i-hercegovini/ (19/08/2022)

[9] Gerring, John. (2007). *Case study research: Principles and practices.* Cambridge, UK: Cambridge University Press.

[10] Hopper, Paul. (2006). *Living with Globalization*. Oxford, New York: Berg.

[11] Hough, Peter, Malik, Shahin, Moran, Andrew & Bruce Pilbeam. (2015). *International Security Studies: Theory and Practice.* London & New York: Routledge.

[12] Johnson, Allan. G. (2008). *The Forest and the Trees: Sociology as Life, Practice and Promise*. Philadelphia: Temple University Press.

[13] Lipovetsky, Gilles. (2008). *Paradoxical happiness: An essay on hyperconsumer society.* Zagreb: Antibarbarus.

[14] Mabry, Linda. (2008). Case Study in Social Research. pp. 214 – 227 in *The SAGE Handbook of Social Research Methods*, edited by Alasuutari, Pertti, Bickman, Leonard & Julia Brannen. London: SAGE Publications.

[15] Mahoney, James. (2007). Qualitative Methodology and Comparative Politics. *Comparative Political Studies* 40 (2): 122–44.

[16] May, Tim. (ed.). (2005). *Work, consumerism, and the new poor: Zygmunt Bauman. 2nd edition*. England: Open University Press.

[17] Motik, Bruno & Dražen Šimleša. (2007). *Green tools for a sustainable revolution.* Zagreb: What are You reading.

[18] Rabushka, Alvin & Shepsle A. Kenneth. (2009). 1st ed. *Politics in plural societies: A theory of democratic instability.* USA: Pearson Education. Longman classics in political science.

[19] Radovanović, Mirjana T. (2019). *Energetska bezbednost.* Sremska Kamenica: Univerzitet Educons. https://educons.edu.rs/wp-content/uploads/2020/01/Energetska-bezbednost-knjiga-NOVA-mr.pdf [04/09/2022]

[20] Roach, Brian, Goodwin, Neva & Julie Nelson. (2019). *Consumption and the Consumer Society*. Tufts University: Global Development And Environment Institute.

[21] Sachdeva, Sonya, Jordan, Jennifer & Nina Mazar. (2015). Green consumerism: moral motivations to a sustainable future. *Current Opinion in Psychology* 2015, 6:60–65, www.sciencedirect.com [07/09/2022]

[22]Slijepcevic, Dusanka. (2022). Theoretical conceptualizations of the market. *Defendology Mne* 7 (11-12) 2021: pp. 115-123. Niksic: Center for security, sociological and criminological research „Defendology".

[23] Smart, Barry. (2010). *Consumer Society: Critical Issues and Environmental Consequences*. London: SAGE Publications.

[24] Suzić, Nenad. (2001). *Sociology of Education*. Eastern Sarajevo: Institute for Textbooks and Educational Resources of the Republic of Srpska.

[25] United Nations Conference on Trade and Development. (1999). *Profiting from green consumerism in Germany: Opportunities for Developing Countries in Three Sectors: Leather and Footwear, Textiles and Clothing, and Furniture – Analytical Studies on Trade, Environment and Development.* Geneva: United Nations Publication.

[26] Vejnović, Duško & Slobodan Simić. (2014). *Environmental security and social ecology*. Banja Luka: European Defendology Center.

[27] Zhu, Qingyun & Joseph Sarkis. (2015). *Green Marketing and Consumerism in China: Analyzing the Literature. Working Paper WP1-2015.* Worcester, MA: Foisie School of Business, Worcester Polytechnic Institute.

Some benefits of building key partnerships to develop security systems

Valeri Panevski
Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski"
at the Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *Research and innovation is the part of an organization's business that shapes the ability of its management and staff to acquire knowledge, design, develop and improve products, services, technologies and processes. Realizing key partnerships in collaborative research and innovation are critical to long-term success for high-tech organizations, while at the same time key to improving business skills, expanding product and service portfolios, and delivering cutting-edge applied research in interest of the country's security.*
Presenting some of the benefits of building key partnerships between organizations in the development of security systems is the content of this publication.
Keywords*: KEY PARTNERSHIPS, SECURITY SYSTEMS*

1. Introduction

Building sustainable key partnerships requires a concerted effort during their establishment and ongoing development to keep them moving in the right direction for the partner organizations. The interests of all stakeholders must be aligned, and the relationships between them must be fostered so that they develop and be mutually beneficial, while at the same time partnerships must be continuously improved to remain strong and productive and have a clear and mutual understanding of each partner's contribution and roles. Challenges will inevitably arise, but the partners should nevertheless strive to create a stimulating environment conducive to cooperation for innovative solutions in the field of security systems development.

Organizations whose profile is the development and improvement of the functionality of security systems strive to build and develop a strategic partnership that reflects their priorities for corporate sustainability. When strategic in nature and innovative in design, a comprehensive and dynamic partnership process can help organizations achieve mutually beneficial outcomes. It found that a planned and phased approach to partnerships is needed to build the necessary foundation for the next stages to flourish.

Staying ahead of evolving physical security threats requires more than simply using the best individual products. Even the best security systems become infinitely more valuable when data can be shared between devices from the organization's other systems. When different solutions can interact, patterns emerge, gaps are noticed, and more comprehensive response plans can be put in place **[1,2,3,4]**.

The absence of effective and accountable security systems often breeds or exacerbates insecurity and instability. The support of the key partnerships for the development of the security systems supports the objectives of the EU member states for peace and stability, inclusive and sustainable development, building state structures and democracy, the rule of law, human rights and principles of international law.

2. Key partnerships

Organizations build partnerships for many reasons, and partnerships have become a cornerstone of many business models. A partnership is a dynamic state in which two or more business entities form a type of relationship. This relationship can be with greater freedom, where each partner organization can form new partnerships, or with exclusivity, limited to one partnership and without other accompanying relationships. At the same time, partnerships are developing for various reasons - from optimizing the business models of organizations involved in the development of security systems **[5,6,7,8,9]** to reducing risk or acquiring resources. They have become a major part of the remaining components of the organization's business model.

Types of key partners

- *Strategic alliances:* these occur between non-competing organizations in an arrangement that benefits both parties.
- *Joint competition:* occurs between competing organizations. It helps to spread the risk that organizations also take in trying to do something new in the market, and it can also ensure some supply that they need.
- *Joint ventures:* the focus here is to develop a new business, due to the birth of a new market or access to a new area, in the geographical sense.
- *Buyer-supplier relationship:* this is the most common type of partnership and aims to ensure reliable supplies. One side gets a quality supplier and the other an established and repeat buyer.

2.1 Reasons for Key Partnerships

Although they are quite common, partnerships are not simple, as they involve a lot of negotiation and previously - built trust. However, there are several motivations that encourage the building of key partnerships.

In general, they can be divided into the following major areas:

Optimization and economies of scale

The most basic form of partnership or buyer-supplier relationship is designed to optimize the allocation of resources and activities. In practice, it is impossible for an organization to have all the resources and be able to manage all the activities on which its business depends. This is why partnerships exist for optimization and economies of scale: to reduce costs by outsourcing and sharing infrastructure.

Reducing risk and uncertainty

In a competitive environment that is susceptible to change, it is critical to reduce risk, and partnerships may be able to do so. This happens even among competitors who may band together to create something new and/or protect themselves from market uncertainty.

This was, for example, the case with the development of Blu-Ray technology **[10]**, when a strategic partnership was created between some of the world's leading electronics and computer companies to share the risk of bringing such an entry to market.

Acquisition of certain resources and activities

Few organizations possess all the resources or perform all the activities described in their business models. The organization, especially developing a business in the field of security systems, needs resources, knowledge and/or licenses that require large investments of time and/or money. Consequently, a partnership is eventually created with other organization/organizations that

already have the processes, information or structures consolidated for it. Many new organizations choose to start their operations by creating partnerships that give them access to the resources or processes they need but cannot yet possess.

2.2 Variant of rules for the selection of key partners

When evaluating the various key partners that an organization's business can benefit from, each one is screened based on the following key questions **[11]**:

- Which partners are essential to our business?
- Who are our main suppliers?
- Which of our suppliers and partners acquire our key resources?
- What partner would meet our needs?
- What is the supply chain where the organization should be positioned?

Once the key partners that an organization's business needs are identified, the following factors need to be considered so that these partnerships are built and developed in a sustainable and beneficial way:

- *Proper and sustainable partnership arrangements:* It does not matter whether the key partner will be another organization or an individual. It is important that the agreements are clear and offer benefits to the contracting parties as well. For this purpose, it is important that they be prepared together with a legal consultant.
- *Defined expectations:* To achieve the type of agreement above, it is essential that each organization openly shares its expectations of the partnership to be formed to avoid conflicts later.
- *Customer impact:* The larger objective, with a key partner, is to fill a gap in the value proposition or key resources. Also, consideration must be given to how this partnership will be viewed by the organization's customer segments.
- *Choosing and stopping partnerships:* Some key partners seem interesting and profitable at the beginning, but are not successful in the end. If a partnership becomes harmful or even inappropriate, it should be closed as soon as possible.

In short, key partners represent the network of suppliers and partners that make an organization's business model not only viable, but also effective. The reasons for choosing a partner are many, and some of them are essential to the success or failure of an organization's business.

Regardless of how many successful partnerships an organization can make, it is important to remember that not all relationships are positive for the business. Therefore, it is necessary to consider beforehand and carefully before signing any agreements.

Last but not least, key partners can change over the life cycle of the organization and market variations. It is always necessary to monitor the business model, reviewing and updating when needed.

3. Experience in research and innovation to build key partnerships

3.1 Collaborative business model

For the purposes of the present development, the Collaborative Business Model **[12]** was used, which is an open innovation design, with the aim of creating a collaborative network of different stakeholders to serve as a source of innovation for a specific industry-related problem, which in this case is development of security systems. Therefore, the focus of the model is to maximize the potential and capacity of the innovation system, by connecting different stakeholders in the process of idea generation and decision making. The network serves as a conduit to connect the scientific and educational sector with industry, the public sector and, in certain cases, civil society. In mutual collaboration, the network of stakeholders develops a business model, mutually adding value to each party involved in the model.

The collaborative business model is applicable when:

- The need to expand the innovation system is necessary or desirable;
- Specific local or regional economic and development challenges require joint efforts and are complex in nature;
- Dominant trends may not be comfortable for all stakeholders involved in the collaborative network and should be explored from different perspectives;
- Many different groups are significantly affected by industry business models and decision-making;
- When civil society demonstrates interest in enhanced official participation;
- There is a need to generate input, share knowledge and encourage innovative thinking on real-life issues that require engaging an external audience;
- Exploring in-depth key strategic challenges and opportunities that could improve and deepen the relationship and mutual ownership of results within the participating groups.

What is more important, the model can be applied when the complexity of the problem implies significant change, as well as when it reflects upcoming trends that are long-term in nature. The creation of a collaborative network of scientific and/or educational organizations, industry representatives, representatives of national departments and local authorities is vital for all stakeholders (e.g. infrastructure of security systems of: critical infrastructure; departmental sites and sites of the local administration, which are important for national security, etc., determined by national legislation - degree of acceptance, forecasts, inclusion of interested parties, introduction of new policies, etc.). This reduces the level of uncertainty in key areas at both the micro and macro levels.

Precisely the application of the collaborative business model was used for the development of the business model of Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski” at the Bulgarian Academy of Sciences (IMSETHC-BAS) in the development of security systems.

3.2 Key partnerships in the framework of the business model of IMSETHC-BAS

The main motivations behind the development of the business model framework are related to the creation of a technology and business platform for security systems through which to represent the management of research in this area (Figure 3.1).

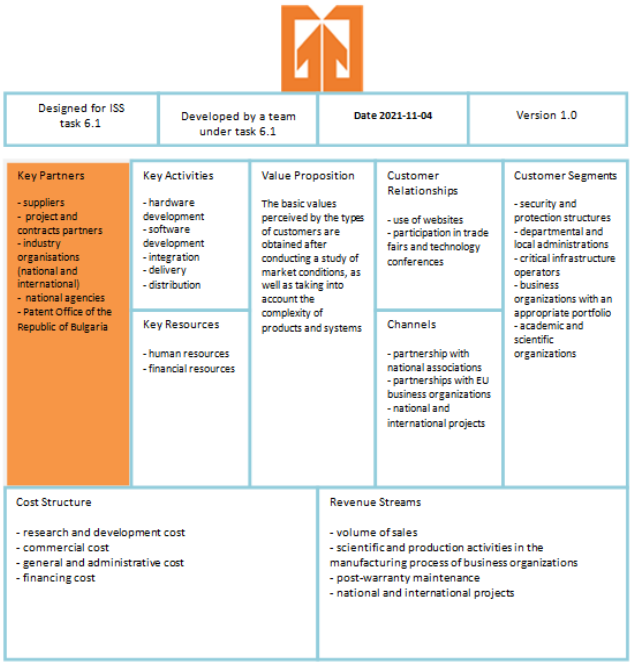


Figure 3.1: *A business model variant of a scientific organization*

After planning the activity, each component of the business model is designed for the management of research and development within the scope of the security systems. The appropriate determination of the element "key partners", from the structure of the business model of the organization, developing security systems (regardless of whether they will be defined as *intelligent security systems* or *integrated security systems*, etc.) is the basis for the adequate implementation of the organization's mission.

Key partners - the following possibilities emerged during the definition of this component:

- ❖ suppliers of microelectronic elements, cloud services, etc.;
- ❖ project and contract partners – with proven capabilities in the field ofrisk assessment, real-time aerial image distribution system to users; simulations of risk events on land and water; providing secure communication (two-way), including quantum communication, etc;
- ❖ business partners, national and international, with a portfolio in the field of security and protection systems;
- ❖ national agencies with responsibilities in the fields of security, defence, education and science, economics, regional development and public works;
- ❖ Patent Office of the Republic of Bulgaria.

3.3 Business model risk profile framework

When developing the business model of the organization, it is necessary to create a better understanding of the risks associated with this activity **[13]**. The proposed risk identification framework (Figure 3.2) would improve the ability to manage potential risks.

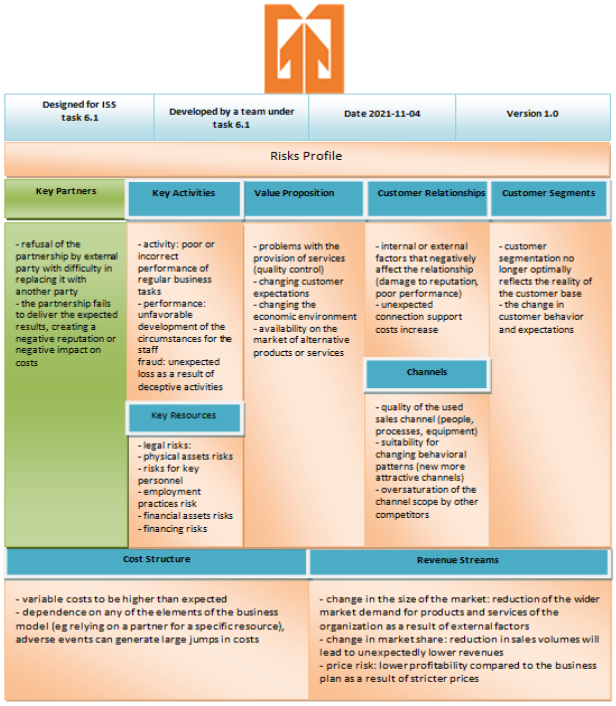


Figure 3.2: *Variant risk profile of a business model of a scientific organization*

Under the Key Partners element, a list of partners to provide critical resources or activities is expected to be identified. Risks associated with partnerships include unexpected development of relations, which deviate from the planned activities of the business model. The framework of the risk profile pertaining to the key partners module of business model mainly includes, but not limited to:

- ❖ refusal of partnership from an outside party and difficulty in replacing it with another partner;
- ❖ the partnership fails to achieve the expected results, creating a negative reputation or a negative impact on costs.

The development of the presented analytical framework for the systematic identification of business model risks **[13]** is only a separate step towards the attempt to determine the possible challenges that may affect the organization's activities.

4. Conclusions

A well-established key partnerships strategy defines the problem the organization seeks to solve, lays the foundation for internal buy-in and commitment, and identifies key assets and current gaps. Central to the development of the key partnership is to first ensure that there is a clear joint advantage to be gained through collaboration. This means creating confidence in the organization that partners can achieve something significant together that they could not achieve alone.

In many cases, key partnerships based on pre-existing relationships can be successful, especially when the needs are in the area of security systems. With existing partners, there is already an established level of trust and familiarity that can help resolve conflicts when they arise and sustain the partnership over the long term.

Acknowledgement

This paper is the result of implementation of the scientific work of the IMSETHC-BAS team, participating in Work package 2. "Intelligent security systems", Project BG05M2OP001-1.002-0006 Competence Center "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)" , funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth", co-financed by the European Union through the European Structural and Investment Funds. It is also related to the implementation of task 06.01 of the Research Plan of IMSETHC-BAS for the period 2020-2022.

References:

[1] Dimitar Dimitrov., "DEVELOPING, IMPLEMENTING AND MAINTAINING AN INTEGRATED PHYSICAL PROTECTION SYSTEM FOR NUCLEAR FACILITIES", Proceedings of the Scientific Conference "Current Security Issues", 6, Vasil Levski National University Publishing Complex, ISSN:2367-7465, pp. 78÷86;

[2] Dimitar Dimitrov, "Comparative evaluation of the modeling and simulation techniques of interdependent critical infrastructures", Collection of reports from the annual university scientific conference, 10, Publishing complex of NMU "Vasil Levski", 2020, ISSN: 1314-1937, pp. 231÷241;

[3] Dimitar D., "Preventive and protective measures against insider threats in nuclear facilities", International Scientific Journal Security & Future, Vol. 5 (2021), Issue 3, International Scientific Journals of Scientific Technical Union of Mechanical Engineering "Industry 4.0", 2021, Print ISSN 2535 - 0668, Online ISSN 2535-082X, pp. 88÷291;

[4] Dimitrov D., "Engineering solutions to ensure protection of nuclear power plants against sabotage", International Scientific Journal "Security&Future", 6, 1, STUME, 2022, ISSN:(PRINT) 2535-0668, (ONLINE) 2535-082X, pp. 18÷21;

[5] Kolarov Al., Georgiev N., Naydenov R., "A TRIP FOR REGISTERING SIGNALS FROM UNDERWATER COMMUNICATION", TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY. 2022, VOLUME II, ISSUE 2 (15), Scientific technical union of mechanical engineering "Industry - 4.0", 2022, ISSN 2535-0315 (Print), ISSN 2535-0323 (Online), pp. 104÷ 107;

[6] Pehlivanski V.I., "Physical model of an integrated security system", Proceedings of the 10th International Scientific Conference "Technique. Technologies. Education. Security.", 6, 2, NTSM, 2022, 2022, ISSN:ISSN: 2535-0315(Print), 2535-0323 (Online), pp. 108÷110;

[7] Varbanov Vladimir, "Modelling uncertainty in multisensory systems at conflict measurements with dempstershafer combinatorial rule", International Scientific Journal "Mathematical Modelling", 5, 3, STUME, 2021, ISSN:2603-2929, p.p. 104÷105;

[8] Tumbarska A., "Guiding principles in the process of developing non-lethal weapons", Proceedings of the International Security Conference "ConfSec 2021", 5, 1, STUME, 2021, ISSN:2603-2953, p.p. 113÷116;

[9] Yavor Boychev, "SEISMIC PIEZOELECTRIC SENSOR MODEL", XIX INTERNATIONAL SCIENTIFIC CONGRESS "MACHINES. TECHNOLOGIES. MATERIALS", YEAR V, ISSUE 2 (22), STUME, 2022, ISSN:2535-0021(PRINT), 2535-003X (ONLINE) , pp. 166÷169

[10] https://www.strategyzer.com/business-model-canvas/key-partnerships;

[11] Daniel Pereira, December 3, 2020 https://businessmodelanalyst.com/key-partners-business-model-canvas/;

[12] https://www.user-participation.eu/planning-the-process/step-5-participatory-methods/development-of-services-or-products/collaborative-business-model;

[13] Philippos Papadopoulos, „Open Risk White Paper: Identification Framework for Business Model Risks", Jan 2016, https://www.openriskmanagement.com/wp-content/uploads/2016/02/OpenRiskWP05_010916.pdf.

Possible structure of standard operating procedure to ensure the operation of security systems

Valeri Panevski
Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski"
at the Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *Standard operating procedures describe the precise steps required to carry out the organization's security tasks in the operation of security systems and are important both for maintaining the level of competence of personnel performing a particular security job and for training new employees. Reducing errors in security-related activities and mission-critical processes is at the core of these procedures.*
Also, providing information on identified gaps, together with a survey of emerging technologies, is expected to help critical infrastructure operators seek future capabilities to create security and optimize the content of standard operating procedures.
Precisely, the presentation of a variant of standard operating procedures for the functioning of security systems is the basis of this paper.
Keywords*: **STANDARD OPERATING PROCEDURES**, **SECURITY SYSTEMS OPERATION***

1. Introduction

It is good practice to make modern applied research and development publicly available and usable for the development of up-to-date products or services. Therefore, the long-term availability of research data is essential for the economics of the production process with an emphasis on the timely application of research. The existence of information, however, is not enough in itself, and its quality must be verifiable. Therefore, measures to ensure subsequent use and/or reproducibility must include the entire development life cycle, from experimental design to data generation, quality control, statistical analysis, interpretation and validation of results. It follows that high-quality records, representing a set of documents to verify the origin of data, are essential elements that can serve as a certificate for potential users. These records, which may be standard operating procedures (SOP), also ensure the optimization of the traceability and transparency of the processes, thereby improving the reliability of the results.

We should not forget that SOPs represent a general guide for the organization's activities. Their development and use is an integral part of a successful management system, as it provides personnel with information on the correct performance of a given job and facilitates consistency in achieving the desired end result.

SOPs describe the precise steps required to perform an organization's security tasks and are important both for maintaining the level of competence of personnel performing a particular security job and for training new employees. Error reduction in security-related activities and mission-critical processes is at the core of these procedures.

At the same time, through the development of the SOP, it is expected to achieve improved coordination of security and resilience efforts, through the use of trusted partnerships in the private and public sectors and the provision of technical assistance and assessments, incl. and risk assessment in the interest of national agencies as well as critical infrastructure (CI) owners and operators across the country. In addition, the provision of information by SOP developers on identified gaps, together with research on emerging technologies, is expected to help CI operators seek future security-building capabilities.

Therefore, in the following lines, I would like to present a variant of a standardized work process that frames the development of SOPs ensuring the functioning of security systems (SEC SYS) **[1,2,3,4]**, developed in the conditions of the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski" at the Bulgarian Academy of Sciences (IMSETHC-BAS), to be used as a starting point for development of appropriate research documentation.

1. Functional model of SEC SYS

Developed by the specialists from the IMSETHC-BAS, the functional SEC SYS model schematically describes the purpose and security activities (if necessary and protection), the personnel who perform them and the interrelationships and consequences of these activities. The purpose of the SEC SYS is, through technical **[5,6,7]**, organizational and other measures and activities **[8,9,10]**, to be identified threats, proposed response to prevent unauthorized access to/unauthorized impact on the protected territory / the protected areas of the CI/ object of the CI.

Actions to prevent/counteract unauthorized access are planned in advance, based on scenarios corresponding to the location and depth of penetration, the specificity of the landscape and the remoteness of the area from the main communications and from the local security and protection structures, to prevent adverse impacts from accidental people and taking measures to neutralize offenders and ensure security and protection of vulnerable assets. The size of the different levels of protection is determined by the level of risk, the response time, the available technical means and the characteristics of the area.

The SEC SYS model consists of two parts:

- Organizational part;
- Technical part.

The model of the technical part is reproduced schematically, through the prism of the structure and content of the purpose of the SEC SYS, by:

- CI location territory model – involves developing a territory model of an organization's key asset, looking in detail at the perimeter security area. The model covers all elements of the territory, assessment of risks and threats and equipment of the security components (including protection if necessary);
- risks and threats against CI model– aims to analyze the possibilities of impact on the critical target/critical asset based on developed scenarios and risk assessment;
- CI's security and protection equipment model - is built to specify the types and amount of equipment depending on the ability of risk factors (man-made destructive events or devastating effects caused by nature) to affect CI.

Of the models listed, the model of risks and threats is of essential importance, since its correct determination will structure the model of the security equipment when positioning it on the model of the territory.

The most obvious benefit of threat modeling is an overall improved security posture of an organization. Ultimately, the goal of threat modeling is to identify threat actors and postulate ways in which they can successfully exploit an organization's vulnerabilities.

Although, training (including education) is one of the most overlooked benefits of threat modeling, it is an important component of building and developing a security culture. Threat modeling is an effective way of drawing attention to the current threats to the organization, and here it is appropriate to mention the two approaches to creating security - reactive and proactive. Unlike reactive security cycles, where security managers and staff only respond after a security incident has already occurred, threat modeling is a proactive security cycle that works to protect against security incidents before they occur.

A proactive approach to security means saving time and money for the organization. In particular, threat modeling tends to provide greater value if performed consistently and repeatedly. Although an upfront investment, threat modeling has the potential to reduce the cost of mitigating the impact on an organization. The threat modeling method chosen will ultimately determine how effectively those threats can be identified and then mitigated.

Also, threat modeling can use developed, field-proven methods that can be applied alone or in combination to create a more holistic view of potential security threats.

2. General framework of the SOP for ensuring the work of the SEC SYS

I's security policy is a well-thought-out system of principles that guides management decisions to achieve rational results. It is a declaration of intent implemented as a procedure or protocol.

The declarations in each procedure, incl. in the field of security, should be able to become SOPs. Combined with a matrix of responsibilities and delegation of authority, these SOPs should ensure the real work that needs to be done on a daily basis in security. In addition, these SOPs should be developed in such a way that they can be revised and improved without changing the security policy.

In addition, the developed SOPs should provide the ability to be hierarchically separated to cover all subsystems of the CI security system.

In this direction, the experience from the development of the Concept for the security levels of the critical infrastructure can be used **[11]**. This Concept applies the rule that the management system of a given organization consists of multiple subsystems that separately implement the various organizational functions. If these subsystems were projected onto the security and defense domain, the organization can say with a fair degree of confidence that the picture presented in Figure 3.1 would result. The elements of the organization's management system are not fixed, and the number of the same can be increased or decreased accordingly, depending on the analytical section to be studied.

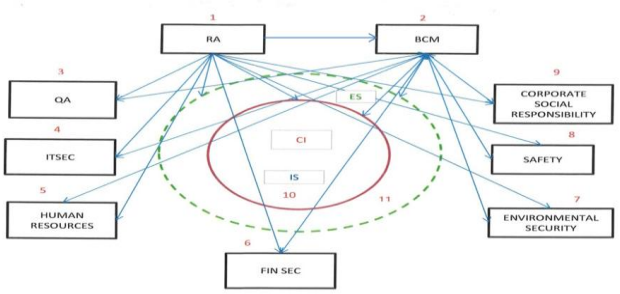


Figure 3.1: The management system through the lens of security **[11]**

Legend: RA – Risk Assessment; BCM – Business Continuity Management; QA – Quality Assurance; ITSEC – Information Security; FIN SEC – Financial Security; CI – Critical Infrastructure; IS – Internal Security; ES – External Security.

As can be seen from Figure 3.1, the input signal for the construction of modern subsystems of the management system is the results of conducting the risk assessment. And the connection is one-way - from the risk assessment to each of the subsystems. And this is because the risk assessment is the source of information about the probability of an event occurring, which enables the relevant subsystem to take the necessary preventive and corrective measures to ensure the security of its functioning.

Figure 3.2 presents variants of models of security and protection equipment deployed on the territory of CI during functionality experiments, within the framework of the European project "Development of necessary tools for coordination of intra-sectoral activities for protection of critical infrastructure in multifaceted/multivariate terrorist threat situation. Increasing the ability to protect key objects of the critical infrastructure in Bulgaria", reg. No. HOME/2010/CIPS/AG/019. The very good evaluation given for the implementation of the project by the General Directorate "Migration and Internal Affairs" of the European Commission is a positive attestation for the scientific and applied developments by the project participants, some of whom participate in the research on the present development.

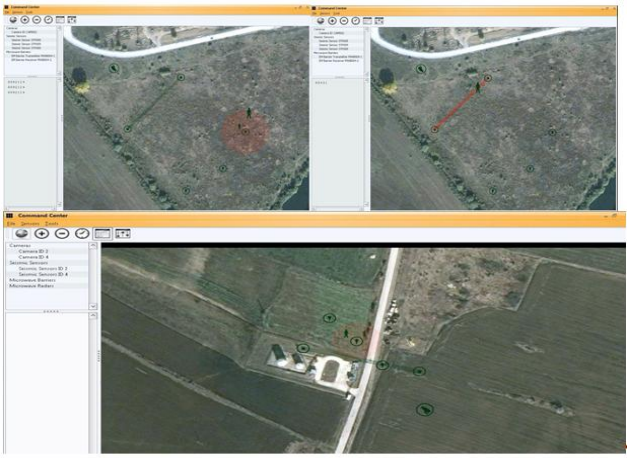


Figure 3.2: Variant of a model of the security and protection equipment deployed in the area of the CI object

The models thus presented set the parameters determined by the likely means of impact by intruders/impact factors from natural disasters, the characteristics of the technical equipment for monitoring and warning of the security forces - transport, communication and information systems, weaponry, territory assessment and timing to reach critical points, etc.

Based on the model of the technical part is the proposed form of SOP model (Figure 3.3), providing the technical support of the modes of operation, training of personnel to maintain and develop capabilities, training of new personnel, as well as review and optimization of the system.

PURPOSE

A brief description of the purpose of the SOP, describing the need for the SOP (e.g. Compliance with internal procedures and guidelines).

Any provisions or procedures referred to in the Purpose section should be identified. The source should be given in the reference section, not in direct quotation marks.

SOP MODEL

SOP # *(number)*

SOP *(name)*

	NAME	POSITION	SIGNITURE	DATE
Developed by:				
Corrected by:				
Assigned by:				

Effective date:	
Date of review:	

Read by			
NAME	**POSITION**	**SIGNITURE**	**DATE**

INTRODUCTION

General introduction with rationale.

SCOPE

A statement that outlines the areas and context covered by the SOP.

If there are areas where this SOP specifically does NOT apply, these should also be mentioned.

DEFINITIONS

Where appropriate, a list of definitions for terms used in the SOP should be included. Abbreviations should be explained at the point of use within the SOP and not listed in this section.

RESPONSIBILITIES

A summary of the roles listed in the procedure and the responsibilities of each role holder for the procedures detailed in the SOP.

The details of the responsibilities should be a short list of the key tasks performed. This section is not meant to be a complete summary of the SOP.

SPECIFIC PROCEDURE

This section is the main text of the SOP. It describes in detail the procedure for completing the task.

There should be sufficient detail clearly stated to enable a trained person to perform the procedure without supervision.

Also, there should be enough detail to enable a trained person to use the document to train others to perform the task.

The use of flowcharts can be useful, especially for complex procedures.

FORMS / TEMPLATES USED

Where forms / templates are referred to in the text, the numbers and titles are listed in this section.

INTERNAL AND EXTERNAL REFERENCES

This section is used to list all controlled internal references (eg SOPs) and external references referred to in the SOP text only.

Internal references

Relevant references are placed as necessary, sufficient for the user to find the source document.

External references

Relevant references are placed as necessary, sufficient for the user to find the source document. Web references should be included where appropriate.

RESPONSIBILITIES

A summary of the roles listed in the procedure and the responsibilities of each role holder for the procedures detailed in the SOP. Details of responsibilities should be brief.

CHANGE HISTORY

Where SOP is the original version:

SOP #: Record the SOP and version number

Effective date: Record the effective date of the SOP or “see page 1”

Material Changes: Status, “Initial Version” or “new SOP”

Previous SOP No: It says “Not applicable”.

Where it replaces a previous SOP:

SOP #: The new SOP # of the version is recorded.

Effective date: Record the effective date of the SOP or “see page 1”.

Substantial changes: The main changes from the previous SOP are recorded.

Previous SOP number: Record the SOP # of the previous version.

SOP #	Effective date	Significant changes	Previous SOP #

Figure 3.3: Proposed form of SOP model

3. Conclusions

SOPs are developed and implemented, according to the specifics of the mission, by government organizations, private business and academic organizations (by scientists and engineers from all science, technology, engineering and mathematics disciplines). SOPs can also be extremely valuable in the area of CI security.

In this regard, the purpose of developing SOPs is to ensure that all CI employees in the field of security and the intelligent security (and protection) systems used perform their tasks in the same way, which is necessary as a condition for obtaining the expected result of the process – security, and in this way ensuring the management of the continuity of the CI's activity.

Therefore, by presenting a major final version of standard operating procedures for the operation of the SEC SYS, it is expected that the contribution of developers from IMSTTCHA-BAS to improving the security of national CIs will be expanded.

Acknowledgement

This paper is the result of implementation of the scientific work of the IMSETCH-BAS team, participating in Work package 2. "Intelligent security systems", Project BG05M2OP001-1.002-0006 Competence Center "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)" , funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth", co-financed by the European Union through the European Structural and Investment Funds. It is also related to the implementation of task 06.02 of the Research Plan of IMSETHC-BAS for the period 2020-2022.

References:

[1] Dimitrov D., "Developing the opportunities for building nuclear security", Technics. Technologies. Education. Safety. 2021., Military sciences and national security., Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering "Industry - 4.0", 2021, ISSN:ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 208÷211;

[2] Dimitrov D., "Examples of nuclear security measures for nuclear facilities", Technics. Technologies. Education. Safety. 2021, Military sciences and national securityy, Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering "Industry - 4.0", 2021, ISSN:ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 212÷2215;

[3] Dimitrov D., "Basic regulations and associated administrative measures providing nuclear security", Collection of reports from the Annual University Scientific Conference, 5, Vasil Levski National University Publishing Complex, 2021, ISSN: 2367÷7481, pp. 73÷80;

[4] Dimitrov D., "Some examples of a nuclear security contingency plans, designed for nuclear facilities", Collection of reports from the Annual University Scientific Conference, 5, Vasil Levski National University Publishing Complex, 2021, ISSN:2367-7481, pp. 64÷72.;

[5] Nikolova V., S. Yaneva., "Individual means of head protection used in military and anti-terrorist operations in objects of the critical infrastructure", Collection of reports from the Annual University Scientific Conference. V. Levski National University, ISSN 2367-7481, 2021, pp. 1177-1185;

[6] Boychev, Y., St. Asenov., "Sensors and Systems for the Detection of Improvised Explosive Devices", Proceedings of the Annual University Scientific Conference. V. Levski National University, ISSN 2367-7481, 5, 2021, pp. 53÷63;

[7] Georgiev N.L, Kolarov A., Iliev I., "Audio recording system for underwater monitoring with fast notification for detected sound anomaly", International Scientific Journal "Security&Future", 4, 2, 2020, ISSN: 2603-2945 (2953), STUME, pp. 68÷71;

[8] Vencislav Pehlivanski, "Tests in the process of designing protection systems", Monograph, IMSETHC-BAS, 2020, ISBN:978-619-188-359-2, pages 169;

[9] Tumbarska A., "Trends in the development of non-lethal technologies and protection systems", Monograph, IMSTCHA-BAN, 2020, ISBN:978-619-7466-07-2, pages 402;

[10] Nikolay Gueorguiev, Aleksandar Kolarov, Iliev Ilian, "An approach for rapid transmission of critical information in underwater monitoring with an adaptively positioned anchor buoy", Proceedings of the International Scientific Conference "Technique. Technologies. Education. Safety", 3, National Technical University of Mechanical Engineering, 2020, ISSN:2535-0315, pp. 160÷163;

[11] Kiril Stoichev, Dimitar Dimitrov, Valeri Panevski, "Integrated security and protection of critical infrastructure", ISBN 978-619-90310-6-3, 2016, pages. 340.

Analysis of barriers to adaptation to climate change

Titko Michal[1], Jana Studená[1], Jozef Ristvej[1], Alexander Kelíšek[1]
Faculty of Security Engineering – University of Žilina, the Slovak Republic[1]
michal.titko@fbi.uniza.sk

Abstract: *Climate change is causing disasters such as floods, whirlwinds, storms, drought, or other extreme weather events that have not yet occurred in certain areas of the world or have not occurred to such an extent and intensity as it is happening now or is predicted in the foreseeable future. Government and, in particular, crisis management system should reflect these facts in order to prepare itself and the population on such events. People should also be interested in preparing for and adapting to these changes and related crisis events. The aim of the article is to examine preparedness of the population in the Slovak Republic and, in particular, to analyse the barriers to climate change adaptation of the population. For the analysis are used the questionnaire survey results on this topic. The initial results indicate the influence of the population by various barriers and factors.*

Keywords: CLIMATE CHANGE, ADAPTATION, PREPAREDNESS, CRISIS MANAGEMENT, CRISIS EVENTS, QUESTIONNAIRE SURVEY

1. Introduction

Crisis phenomena and weather extremes are currently on the rise in frequency and also severity of impacts, as recognised in the assessment reports of the Intergovernmental Panel on Climate Change. The main cause is climate change, which will become more and more extreme. The current situation therefore requires a prompt response and a change in attitudes to the issue, especially from the perspective of the state, but also the population itself. As the reaction to this global negative trend a various strategies and frameworks (Hyogo Framework (2005), EU Strategy (2013), Sendai Framework (2015), Agenda 2030: Sustainable Development Goals (2015), Paris Agreement (2016)) [1-5] have been adopted, which are intended to provide a basic framework for the implementation of climate change risk reduction strategies. In connection to this frameworks a number of national adaptation policies and plans have been developed [6].

The degree of possible manifestation of the mentioned changes and risks varies regionally, but the trend of negative changes is global. The unfavorable consequences of climate change in terms of the occurrence of crisis phenomena and weather extremes are also confirmed by the Slovak Hydrometeorological Institute in its forecasts for the Slovak Republic (SR) and other sources (e.g. statistics of the Ministry of Interior, Statistical Office of the SR). The forecasts relate mainly to an increase in the number of summer and tropical days and heat waves; frequent heavier torrential rains and more intense storms, which are associated with a more uneven distribution of precipitation totals throughout the year and may lead to a reduction in soil moisture and, consequently, periods of drought; in the SR there will be more frequent very strong storms, during which storms and tornadoes may occur and more frequent occurrence of lightning local floods in various parts of the SR can be expected [7, 8]. From the public's point of view, there are several ways to adapt to these changes and better prepare for the impacts of the abovementioned disasters and extremes, but the implementation in practice is quite weak.

Despite considerable international and national effort, adaptation to climate change still encounters various problems and barriers to adaptation actions still persist, whether at the national, local, institutional or individual level [6, 9, 10]. Moreover, climate risks affect different groups of the population differently, with vulnerable groups most affected. Therefore, at the individual level, problems and barriers in the area of adaptation to climate change are deepening. The goal of this article is to identify what the adaptation barriers are in the conditions of the SR and how are perceived by the public. Focus of this study is on the individual level of adaptation. In order to know how we can deal with identified barriers in the conditions of the SR a further research is assumed.

2. Rationale - Barriers of Adaptation to Climate Change

There are several criteria how to categorize the adaptation berries. They can be perceived at national, local, institutional, project, as well as individual levels, and others. The different case studies and theoretical works have produced a large list of commonly reported barriers [11-16]. Commonly most used barriers categories in the local context are: institutional, attitudinal, financial and political [17]. Other authors identify 7 barrier categories (adopted from [18]): (1) conflicting timescales, (2) substantive, strategic and institutional uncertainty, (3) institutional crowdedness and institutional void, (4) institutional fragmentation, (5) lack of awareness and communication, (6) motives and willingness to act, and (7) lack of resources.

At the individual level, there are also many articles and studies that are dealing with adaptation barriers. There are often connected to the research in the selected country and therefore, there can be seen differences between results. The study by Lorenzoni et al. (in UK) identified several groups of barriers [19]:

Lack of knowledge

Although information is mostly available (about the causes, consequences, potential solutions, adaptation options, etc.), the rate of its transformation into knowledge or into use / into practice is relatively low, for various reasons, including [19]:

- Lack of knowledge about where to find information.
- Lack of desire to seek information.
- Perceived information over-load.
- Confusion about conflicting information or partial evidence.
- Perceived lack of locally-relevant information, for example about impacts or solutions.
- Format of information is not accessible to non-experts.
- Source of information is not credible or trustworthy, particularly the mass media.
- Confusion about links between environmental issues and their respective solutions.
- Information conflicts with values or experience and is therefore ignored.

Uncertainty and scepticism

Uncertainty and scepticism are mainly related to the perception of the reliability of evidence on climate change and the existence of conflicting evidence on climate change. These facts then cause problems for the population to know what is really happening.

Distrust in information sources

This barrier is related to media coverage and especially exaggeration and sensationalism by the media, which often have conflicting arguments regarding the effects of climate change. This

barrier is related to the previous one (Uncertainty and scepticism), but focuses more on the bias of the media that people encounter.

Externalising responsibility and blame

The given barrier characterizes the shifting of responsibility to another entity (mostly industry or some specific state or group of states). The individual leaves the proactivity in the area of adaptation and mitigation measures to these entities, as they blame them for climate change.

Technology will save us

People accept change that seems inevitable, while not being afraid of its consequences, because technology can cope with these effects.

Distant threat

The possible impacts of climate change (the more serious ones) are currently too unimaginable and distant that people cannot imagine them and therefore do not prepare for them. Other things are more important Includes: Attention to more immediate priorities, e.g. family and finances, other (local) environmental issues.

Reluctance to change lifestyles

The threat of a reduction in the standard of living, which may be associated with a loss of comfort and increased costs (monetary and time) are the barrier of adaptation.

Fatalism

For some people the evidence suggests that it's too late to do anything or that we can't do anything.

"Drop in the ocean" feeling

Perception of climate change as a global problem and individual helplessness in trying to mitigate or adapt to it.

To a large extent, similar barriers, with different names, are also reported by González-Hernández et al. in their study [10]. They identified seven main barriers:

- **everyday life** – similar as "Reluctance to change lifestyles" but it is more focused on difficulty to change our habits and comfortable life related to using technology.
- **awareness of climate change** – refer to the climate change knowledge and adaptation knowledge,
- **lack of perceived locus of control** – very similar understand as "fatalism" in combination with "drop in the ocean" barrier,
- **physical limitations of the dwelling** – this barrier is connected to the ownership, construction and space limitation to make a change,
- **social** – people feel a discontent and frustration when other people in their community did not take measures to prevent or adapt to climate change,
- **regulatory** – the lack of initiatives related to climate change at the local goverment level affect common population,
- **economic** – a lack of economic resources is a major barrier to implementing climate change adaptation measures.

3. Methodology

The authors utilized the following methods for fulfilling the stated goal:

- analysis of the current state of reported barriers to climate change adaptation,
- questionnaire survey conducted on a sample of students of Faculty of Security Engineering – University of Žilina focusing on perception of the selected barriers too climate change adaptation. The questionnaire was distributed to randomly selected respondents and students of Faculty of Security Engineering in electronic form. For the purpose of this paper only students' responses are investigated.

4. Results and Discussion

Questionnaire survey

A questionnaire survey was conducted in September and October 2022. A structured questionnaire was used, based on various sources [e.g. 19] and supplemented with questions and formulations that the authors considered appropriate with regard to the subject of the research. The questionnaire was distributed to the students of University of Žilina in electronic form. Number of participants was 248 (n). General information about the participants in the survey are summarized in the following table (Table 1).

Table 1: *General information about survey participants*

General information		Share [%]
Gender	Male	63,31
	Female	36,69
Living type	In flats	31,45
	In houses	68,55
Living place	Rural	64,92
	Urban	35,08
Monthly household income	0 - 1000€	11,69
	1001 - 2000€	43,55
	2001 - 3000€	29,03
	3001 - 4000€	10,08
	more than 4000€	5,65

Then the students were asked to express their level of agreement or disagreement (from 1 – I completely disagree to 5 – I completely agree) to selected statements which are related to the common barriers reported in another studies:

- I don't have enough knowledge about climate change and its effects
- I don't know how to adapt, I don't know any concrete measures
- It is financially difficult for me to adapt (some measures are beyond my means)
- I don't want to limit myself in my lifestyle
- I am addicted to technology and its use
- Other issues are more important to me at the moment (I have other priorities)
- I'm just not interested in this topic at all

Knowledge

First of all, the knowledge of the students about meaning of terms "adaptation" and "mitigation" was examined as it was important for proper understanding of following questions in the questionnaire survey. 93% of students know what does the adaption to the climate change means (Fig. 1). It's a little worse with understanding of mitigation meaning – only 81% know what does the climate change mitigation means (Fig. 1). For those who had trouble understanding the meaning of these important terms (as well as others), the following section of the survey explained this terminology and the underlying context.

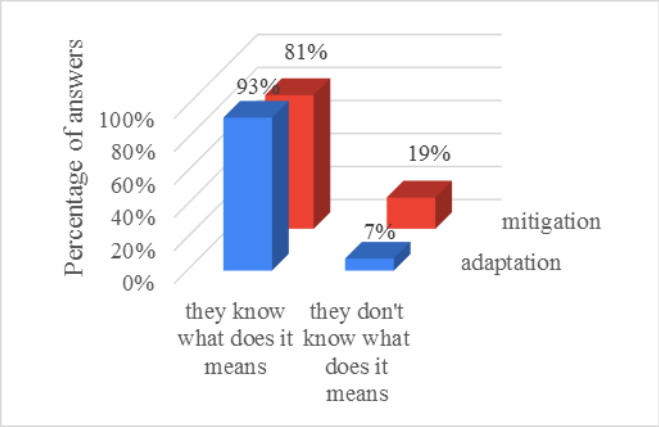


Fig. 1 *Percentage share of knowledge of adaptation and mitigation meaning*

In the section of knowledge exploration, we have also explored if students have enough knowledge about climate change and its effects. This tells us a lot about the potential of young people to have a reason at all and to understand the reasons why it is necessary to start implementing certain adaptation measures. Only 12% of respondents state that they have no knowledge or only very weak knowledge about climate change and its impacts (Fig. 2 values 4 and 5). About 55% of students have enough knowledge or almost enough knowledge about the topic (Fig. 2 values 1 and 2) and about 33% is in the middle so they are also group that need to enhance they level of knowledge about climate change. In order to enhance the overall climate change knowledge level a proper information strategy should be prepared and implemented.

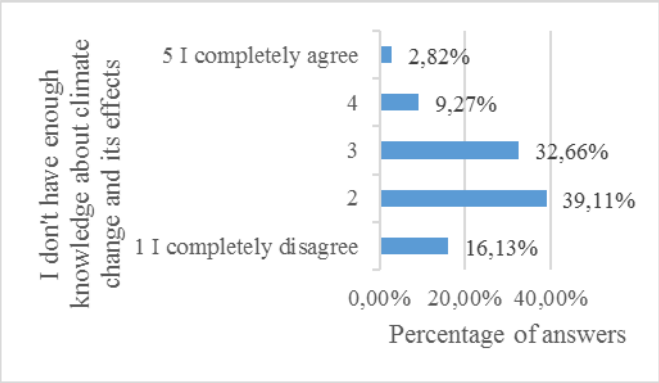


Fig. 2 *Percentage share of knowledge level about climate change and its effects*

As the rest of the survey focused primarily on adaptation measures and barriers to their implementation, it was important to examine the knowledge of adaptation measures and the possibilities of how to adapt at the individual or household level. About 57% of respondents are aware of adaptation options and measures (Fig. 3). The rest have average (24,19%), below average or no knowledge at all (18,55%). The results are not very optimistic, but not alarming either. However, additional research revealed that only 26% of respondents agreed or rather agreed with the statement that "I have implemented several adaptation measures in my home or life".

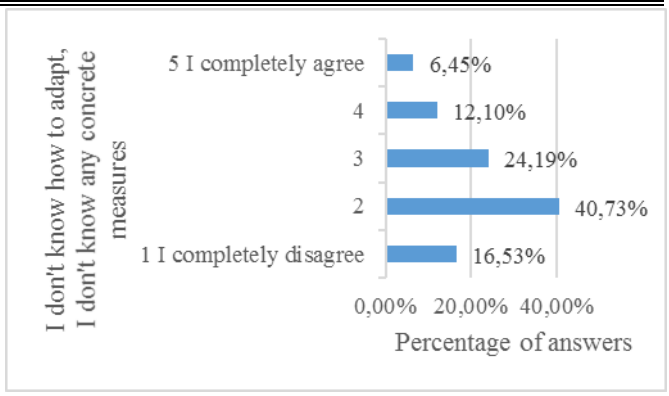


Fig. 3 *Percentage share of knowledge level about the adaptation options and about concrete measures*

Financial barriers

A common problem that often occurs in connection with the implementation of adaptation measures is their financial burden. There are several measures that are relatively effective and do not require any or only a minimal investment, and therefore even less solvent households can contribute to the fight against the effects of climate change. Of course, there are also those that require investment, and this obviously affected the results of the survey. 7,26% of respondents completely agree or rather agree (22,98%) that it is financially difficult for them to adapt (Fig. 4). It is connect to the fact (see general information about respondents in Table 1) that the income of the households is rather low.

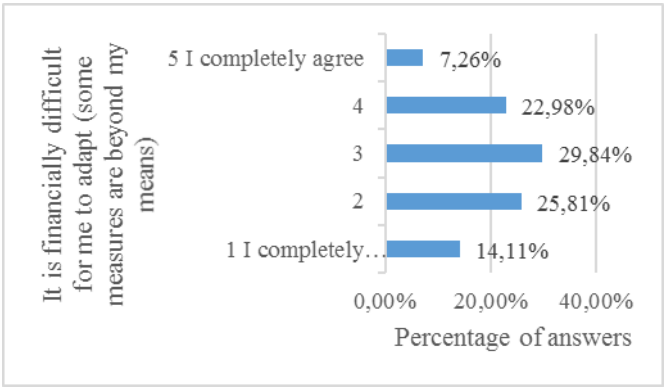


Fig. 4 *Expression of different degrees of financial difficulty of adaptation*

Standard of living

According to the results of the survey, the biggest barrier to adaptation to climate change among young people is a low willingness to change their way of life or their priorities (Fig. 5). The high-end and consumptive way of life associated with the use of modern technologies offers many new and interesting possibilities for all age groups, but it also forces large industrial giants, clothing, food and other industries to increase production. This cycle can be slowed down by lower consumption, modesty, or a total change in the consumer way of life. This seems to be the most difficult for young people, while practically all of us can do it.

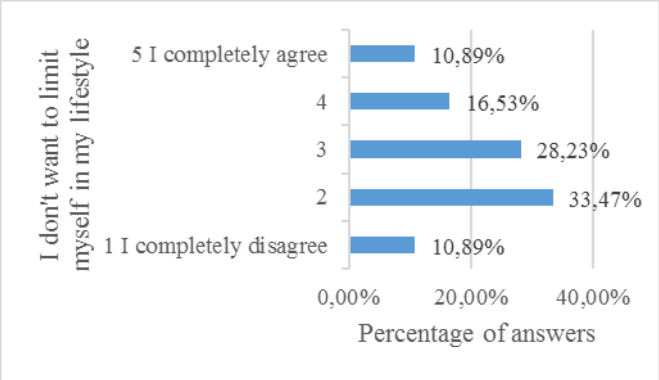


Fig. 5 *Expression of different degrees of willingness of students to limit themselves in lifestyle*

Lifestyle is closely connected with the use of new technologies, which can limit us in the application of adaptive measures. In the conducted survey, this dependence is confirmed by almost half of the respondents (Fig. 6). However, this fact can also be seen as an opportunity to change, because many innovative and technological elements can help fight the manifestations of climate change. At the very least, it is possible to distribute information in a more targeted manner, and to use modern technological communication channels to strengthen the information base regarding climate change.

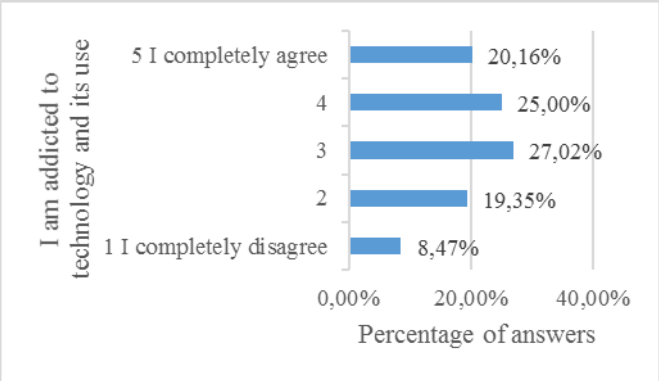


Fig. 6 *Expression of different level of dependence on technology*

Interest

We live in a hectic time and people are busy both professionally and personally. Students also try to make extra money and gain experience, they are engaged in various leisure activities, so it is quite common that they have different priorities and interests. In connection with the perception of the consequences of climate change as a distant future, it is then obvious that question of climate change is not included among the main priorities of the individual (Fig. 7). As a result, he/she does not show any interest in the issue (Fig. 8) and does not try to find ways to adapt to the changing situation or to change something in his/her life.

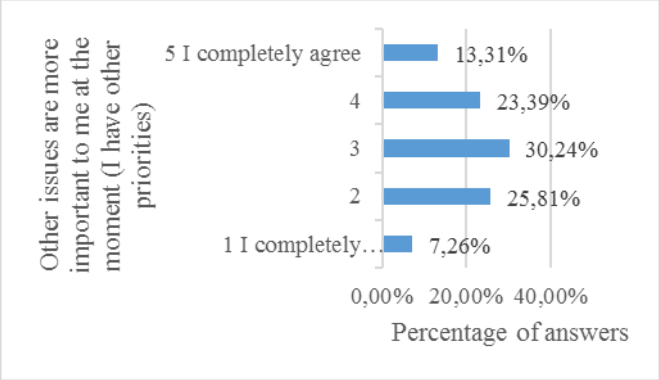


Fig. 7 *Expression of different degree of agreement in the statement "Other issues are more important to me at the moment"*

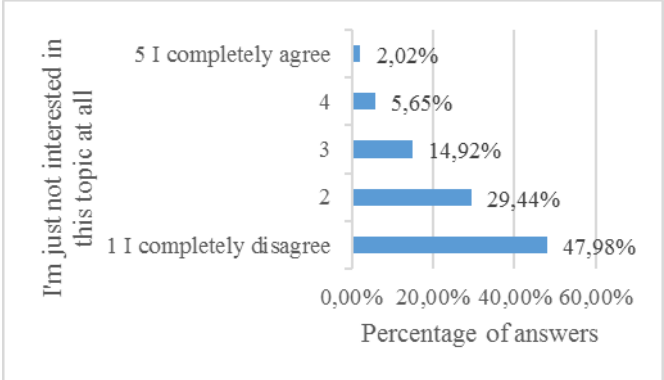


Fig. 8 *Expression of different degree of agreement in the statement "I'm just not interested in this topic at all"*

4. Conclusion

Based on the questionnaire results can be stated that students in the SR perceive similar barriers of adaptation to climate change as it was reported in previous studies, while the biggest barrier appears to be reluctance to change or modify their lifestyle. The results for individual barriers are not clear-cut, and a significant part of the students is able and willing to take adaptive measures and be an active player in the fight against climate change. A certain part of students feels only small barriers or perceives them as average, but surmountable. It is on the examples of young people's active work that it is possible to build future activities and support even those people who do not want to get involved with the issue or people who need to be initiated in their activism from the outside.

In the Slovak Republic, strategic decisions were made in the direction of strengthening adaptation efforts to climatic changes (Climate Change Adaptation Strategy) and action plans for the implementation of these strategic decisions were also adopted. Most of the measures of these action plans are of a national, regional or local nature. The position of the individual is solved by his support (e.g. financial) of his activities aimed e.g. at reducing the energy consumption of his home. The issue of supporting public awareness of climate change and involvement in adaptation activities is only partially addressed.

In order to reduce the impact of climate change on the population and social and economic system it is necessary to focus on vulnerable areas and vulnerable elements of society. This can be achieved by supporting the adaptation process of the general public and with the support of competent and interested entities, their cooperation and appropriate communication with the public. A support for the adaptation process is expected through improving the availability of information, supporting the distribution of this information and its communication, and generally raising public awareness of the possible impacts of climate change. In connection with the results of the survey, it can be seen that young people's knowledge of climate change is acceptable and it is possible to build on it in the future. Our effort in further research is to more deeply examine the perception of these barriers in society and also examine the perception of support from the state for the individual.

Acknowledgements

Publication of this paper was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic – VEGA No. 1/0459/21: „Proposal of adaptation measures to reduce the risks arising from climate change in terms of the occurrence of the disasters and the extreme weather events.“

Publication of this paper was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic – VEGA No. 1/0628/22: “The security research in municipalities with emphasis on the citizens’quality of life”.

References

[1] UNISDR, Hyogo Framework, (2007). Retrieved from https://www.unisdr.org/2005/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf

[2] European Commission, An EU strategy on adaptation to climate change, Communication from the Commission to the European parliament, the council, the European economic and social committee and the committee of the regions, (2013). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013DC0216

[3] UNISDR, Sendai Framework, 2015. Retrieved from https://www.undrr.org/implementing-sendai-framework/what-sendai-framework

[4] UNFCCC, United Nations Framework Convention on Climate Change, Paris, p. 32, (2015). Retrieved from https://unfccc.int/sites/default/files/resource/docs/2015/cop21/eng/l09r01.pdf

[5] UN, Transforming Our World: The 2030 Agenda for Sustainable Development, p. 41, (2015). Retrieved from https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf

[6] S. Lee, J. Paavola, S. Dessai. Towards a deeper understanding of barriers to national climate change adaptation policy: A systematic review. *Climate Risk Management* 35 (2022) 100414

[7] SHI - Slovak Hydrometeorological Institute. E. Peterová, I. Garčár, Klimatická zmena a jej vplyv na zdravie a majetok na Slovensku [Climate change and its impact on health and property in Slovakia]. Aktuality SHMÚ [online] [cit. 18.10.2022]. (2018). Available at: http://www.shmu.sk/sk/?page=2049&id=927

[8] Ministry of Environment SR. Stratégia adaptácie Slovenskej republiky na nepriaznivé dôsledky zmeny klímy – aktualizácia [Strategy of adaptation of the Slovak Republic to the consequences of climate change - update] [online]. [cit. 18.10.2022]. (2017). Available at: https://www.minzp.sk/files/odbor-politiky-zmeny-klimy/strategia-adaptacie-sr-nepriaznive-dosledky-zmeny-klimy-aktualizacia.pdf

[9] UNEP. Adaptation gap report. UN environment programme. (2018).

[10] L. González-Hernández, E. W. Meijles, F. Vanclay. Household Barriers to Climate Change Action: Perspectives from Nuevo Leon, Mexico. *Sustainability*. (2019), 11, 4178.

[11] G. R. Biesbroek, J. E. M. Klostermann, C. J. A. M. Termeer, P. Kabat. Barriers to climate change adaptation in the Netherlands. *Clim. Law* 2, 181–199 (2011).

[12] W. N. Adger, et al. Are there social limits to adaptation to climate change? *Climatic Change* 93, 335–354 (2009).

[13] I. Lorenzoni, S. Nicholson-Cole, L. Whitmarsh. Barriers perceived to engaging with climate change among the UK public and their policy implications. *Glob. Environ. Change* 17, 445–459 (2007).

[14] S. Burch, In pursuit of resilient, low-carbon communities: an examination of barriers to action in three Canadian cities. *Energ. Policy* 38, 7575–7585 (2010).

[15] H. Eakin, A. M. Lerner, F. Murtinho. Adaptive capacity in evolving peri-urban spaces: responses to flood risk in the Upper Lerma River Valley, Mexico. *Glob. Environ. Change* 20, 14–22 (2010).

[16] L. Jones, E. Boyd. Exploring social barriers to adaptation: insights from Western Nepal. *Glob. Environ. Change* 21, 1262–1274 (2011).

[17] J. A. Ekstrom, S. C. Moser. Identifying and overcoming barriers in urban adaptation efforts to climate change: case study findings from the San Francisco Bay Area, California, USA. *Urban Clim*. (2014).

[18] K. Eisenack, et al. Explaining and overcoming barriers to climate change adaptation. *Nature Climate Change.* 2350 (2014).

[19] I. Lorenzoni, S. Nicholson-Coleb, L. Whitmarsh. Barriers perceived to engaging with climate change among the UK public and their policy implications. *Global Environmental Change.* 17 (2007) 445–459

Brief description of the identification of vital areas in nuclear facilities process

Dmitar Dimitrov,[1*], Lyudmil Nedelchev[2]
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria[1]
Kozloduy NPP PLc, 3321, Kozloduy[2]
E-mail: ddimitrov@ims.bas.bg, lnnedelchev@npp.bg

Abstract: *The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. Operators have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to effectively respond to nuclear security events. Nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported. Identification of vital areas is an important step in the process of protecting against sabotage. Vital area identification (VAI) is the process of identifying the areas in a nuclear facility around which protection will be provided in order to prevent or reduce the likelihood of sabotage.*

KEYWORDS: *NUCLEAR FACILITIES, PROTECTION OF NUCLEAR INSTALLATIONS, VITAL AREA IDENTIFICATION, HIGH RADIOLOGICAL CONSEQUENCES, UNACCEPTABLE RADIOLOGICAL CONSEQUENCES, INITIATING EVENTS OF MALICIOUS ORIGIN*

1. Introduction

The objective of this report is to describe a process that can be used to [1]:

(i) Identify all candidate sets of vital areas at a nuclear facility;

(ii) Select a specific set of vital areas that will be protected.

The process for selection of a specific set of vital areas to be protected is based on consideration of the potential radiological consequences of sabotage, and the operational, safety, and physical protection features of a nuclear facility.

This report focuses solely on the process for Vital Area Identification (VAI) at nuclear facilities. The VAI process can be used for existing facilities to identify vital areas and to evaluate the effect that design changes have on vital area selection.

This process may also be applied to new facilities in the design stage to analyze how design and layout features may be optimized for vital area selection.

Also, the concepts and principles (i.e. identifying material or components that require protection in a vital area on the basis of unacceptable radiological consequence thresholds) of this publication may be applied at facilities other than nuclear ones.

2. Vital area identification process

This part of the report describes the process used to identify vital areas in a nuclear facility. The vital area concept is used to define a boundary around the vital equipment, systems, or devices, or nuclear material to which physical protection can be applied. The objective of the VAI process is to identify a set of areas of a facility containing the equipment, systems, structures, components, devices, or of operator actions that, if adequately protected, will prevent high radiological consequences (HRCs).

The VAI process should be repeated when design changes are being considered or prior to their implementation, and when the threat has been modified. The best time to apply this process is in the design phase of a new facility, when physical protection can be optimized, and retrofitting avoided.

Typically, an operator is responsible for identifying the vital areas, and the countries' regulatory body is responsible for validating the VAI process.

2.1 Process overview

The steps of this process are as follows:

- Gather information that is input to the VAI process:

• Identify VAI process team;

• Policy considerations. Address the key policy considerations essential to the VAI process.

• Site and facility characteristics. Identify the inventories of nuclear and other radioactive material. Evaluate the facility and site characteristics needed to determine whether sabotage could lead to HRCs;

• Conservative analysis for each nuclear and other radioactive material inventory. Determine whether the complete release of any inventory could exceed the HRC criteria. Include direct dispersal of any such inventory as an event in the sabotage logic model and continue with the process described below.

- Identify any initiating events [2] of malicious origin (IEMOs) that can lead indirectly to HRCs.

- Identify any IEMOs that exceed the capability of mitigation systems. Include each such IEMO as an event leading to HRCs in the sabotage logic model.

- Identify systems, structures and components to mitigate each IEMO. For each IEMO that does not exceed mitigating system capability, identify the safety functions necessary to mitigate the IEMO, the systems, structures and components that perform the safety functions, and the success criteria for the systems.

- Develop a sabotage logic model that identifies the combinations of events (direct dispersal, IEMOs that exceed mitigating system capability, and IEMOs coupled with mitigating system disablement) that would lead to HRCs.

- Eliminate from the sabotage logic model any events that the assumed threat does not have the capability to perform.

- Identify the locations (areas) in which direct dispersal, IEMOs, and the other events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.

- Solve the sabotage area logic model to identify the combinations of locations that should be protected.

- Select the vital area set that will be protected to prevent sabotage leading to HRCs.

Facility safety analyses can provide valuable information and models to support VAI. If a deterministic safety assessment (DSA) or a probabilistic safety assessment (PSA) has been completed for the facility, it will provide analyses of response of the facility to various initiating events (IEs) that may be caused by random failure, human error, etc.

These events could also be caused by malicious acts. DSAs and PSAs [3, 4] provide extensive information on site and facility characterization that will be useful to the VAI team. Either type of

analysis will contain information that can be used to construct the logic models needed for VAI [5, 6, 7 and 8].

2.2 Input to the VAI process

2.2.1 Policy considerations

Policy considerations to be addressed prior to initiation of the VAI process are:

- The explicit definition of unacceptable radiological consequences (URCs) that will require protection against sabotage;

- The explicit definition of HRCs that will require designation and protection of vital areas;

- The operational states for which vital areas should be identified and protected;

- The safe facility state that should be achieved following a sabotage attack for each operational state;

- Whether equipment unavailability events, other than malicious disablement acts, should be considered to occur concurrent with a sabotage attack;

-Whether the analysis can take credit for accident management recovery actions following a sabotage attack;

- The threat against which the facility should be protected.

2.2.2 Site and facility characteristics

The first step in performing VAI is to identify the inventories of nuclear or radioactive material present and also the facility and site characteristics that will be needed to determine whether sabotage could lead to HRCs. This requires information on:

- The site (area in which the facility is located), such as:

• The population density in the vicinity of the facility and other site characteristics to determine the consequences of a potential radiological release when the criteria for HRCs involve off-site exposure rather than a surrogate, such as core damage or containment failure.

- The facility, such as:

• The locations, inventory forms, characteristics, and quantities of nuclear and other radioactive material;

• The nuclear facility's critical safety functions (e.g. shielding, criticality prevention, cooling, confinement, fire prevention, structural integrity); the detailed design information on process and safety systems needed to determine the equipment, systems, structures, components, devices, and operator actions that should be protected to prevent HRCs.

The information needed for site and facility characterization should be available from the facility safety case or other safety analysis documentation.

2.2.3 Analysis of radiological consequences

A conservative analysis should be performed to determine the potential radiological consequences of the complete release of each nuclear or other radioactive material inventory at the facility. The analysis should be performed without consideration of physical protection and mitigation measures present at the facility.

If the potential radiological consequences estimated for an inventory under these conservative analysis conditions are below the URCs, sabotage leading to URCs is not possible for this inventory. Consequently, it is not necessary to designate any areas to be protected against sabotage for this inventory. For such inventories, the operator should protect safety related equipment and devices by controlling access and securing them.

If the potential consequences are between the URC and HRC levels established by the State, the operator should identify the areas to be protected against sabotage and protect them as specified by State requirements. If the potential consequences are above the HRC level, the operator should identify vital areas as described in the following sections and protect them as recommended in [2].

If the conservative analysis indicates URCs, it may be appropriate to conduct a more sophisticated and resource intensive analysis to identify a more realistic estimate of the potential consequences from the same specified amount of radioactive material. The calculation of radiological consequences should be based on conservative, yet realistic, data and assumptions, considering such data as release fractions and plating. The parameters for the analysis should be defined or approved by the competent authority.

2.3 Direct sabotage of nuclear or other radioactive material inventory

Acts that lead directly to release of radioactive material are those that apply energy from an external source (for example, an explosive or incendiary device) to disperse the material.

If the potential radiological consequences of the release of a complete inventory are equal to or greater than the HRC level, the direct dispersal of the inventory should be included in the sabotage logic model as a potential malicious act leading directly to HRCs, and the remaining steps of the vital area identification process should be performed for the inventory.

The feasibility that the threat could cause direct dispersal of the inventory is addressed when the threat characteristics are considered later in the process.

2.4 Indirect sabotage of nuclear or other radioactive material inventory

Malicious acts that lead indirectly to the release of nuclear and other radioactive material are the ones that use the potential energy (i.e. heat or pressure) contained in the nuclear or radioactive material or in a process system to disperse the material.

Indirect sabotage attacks do not require that the adversary gain access to the area in which the material is located; instead, they involve attacks against equipment, systems, structures, components, devices or operator actions that normally maintain the facility in a safe state.

If the potential radiological consequences of the release of a complete inventory are equal to or greater than a HRC limit, the possibility of sabotage that could lead indirectly to HRCs should be considered. To determine the areas that should be protected to prevent acts that lead indirectly to HRCs, two types of sabotage attacks should be considered, namely those:

- Causing an initiating events (IE) [3] that creates conditions more severe than the facility mitigating systems can accommodate (that is, events that are beyond the safety design basis);

- Causing an IE and disabling the systems needed to mitigate the effects of the IE.

An IE that is deliberately caused by an adversary in an attempt to cause a release from a facility is called an IEMO.

2.5 Sabotage logic model

The next step in performing a VAI is constructing a sabotage logic model that identifies the events or combinations of events that could lead to HRCs necessitating protection in vital areas, including the direct dispersal of radioactive material, IEMOs that exceed mitigating system capacity, and the combinations of events that will lead to HRCs for IEMOs that are within mitigating system capacity [9].

A logic model can be a statement; an algebraic expression or a graphical representation, such as a fault tree or an event tree. The sabotage logic model includes all direct dispersal events and all

IEMOs and associated mitigating system failures that will cause HRCs.

Direct dispersal and IEMOs that exceed mitigating system capacity are included in the logic model as single events leading to HRCs. The portion of the logic model that deals with IEMOs within mitigating system capacity includes each such IEMO combined with the malicious disablement of the specific systems designed to mitigate the IEMO. Logic models for system disablement are developed to the component level using a top-down approach.

The logic models should be developed in sufficient detail to allow linking of disablement events to the facility locations (areas) in which disablement can be accomplished [10].

Information provided in the facility safety analyses and other safety documentation can be used to develop the sabotage logic model for IEMOs within mitigating system capability. Typically, this is done in two stages.

The first stage is the development of the facility sabotage logic model that represents the combinations of IEMOs and disablement of front line systems leading to HRCs.

The second stage is developing sabotage logic models for individual front line systems and the support systems they are dependent upon.

This activity is performed either by modifying existing logic models from the facility PSA, if one has been prepared, or by developing logic models using facility system configuration information and the success criteria and dependency information.

This process produces the portion of the facility sabotage logic model that links each IEMO with the disablement of the front line systems and corresponding support systems and operator actions that are required to mitigate the IEMO.

The sabotage logic model will have the direct dispersal events, the IEMOs, and the events that disable mitigating system components as basic events.

2.6 Capability of threat to perform sabotage events

The sabotage events addressed in the preceding sections do not consider the capability of the threat to perform the malicious acts. Indeed, all events that could lead directly or indirectly to HRCs are included to ensure that no potential vital areas are overlooked without regard to whether the assumed threat capabilities are sufficient to perform the sabotage acts.

If the assumed threat characteristics change, the information and models developed in the preceding steps will be valid for use in identifying vital areas under the changed threat conditions.

In this step of the process, any events that are not credible given the assumed threat capabilities should be eliminated from consideration. The threat's capability to perform the direct dispersal of material, to cause an IEMO, and to disable mitigating systems should be assessed. Events that are beyond the capability of the threat may be removed from the sabotage logic model.

In addition, any events that are beyond the ability of the facility physical protection system to prevent should be identified. In the analysis of the sabotage logic model, any such events will be assumed to occur always.

Generally, any events that the threat can accomplish without gaining access to the site should be assumed to occur. For example, it is practically impossible for the facility physical protection system to prevent the loss of off-site power; the threat can cause loss of off-site power in many ways without gaining access to the facility.

Therefore, the VAI process should assume that off-site power is unavailable. Any other such events in the sabotage logic model should be identified and highlighted for proper treatment in the area identification process.

3. Conclusions

An effective national nuclear security regime builds on:

- Implementation of relevant international legal instruments;

- Information protection;

- Physical protection;

- Material accounting and control;

- Detection of and response to trafficking in such material;

- National response plans;

- Contingency measures.

Each operator carries the full responsibility for nuclear security, i.e. to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; and to combat illicit trafficking and the inadvertent movement of such material. It should also be prepared to respond to a nuclear security event.

The report presented a structured approach to identifying the areas that contain equipment, systems, and components to be protected against sabotage. It specifically provides detailed guidance with regard to the identification of vital areas, that is, the areas to be protected in high consequence facilities [11].

However, the process described is applicable to the identification of areas that should be protected at any nuclear facility. The method builds upon safety analyses to develop sabotage logic models for sabotage scenarios that could cause unacceptable radiological consequences.

The sabotage actions represented in the logic models are linked to the areas from which they can be accomplished. The logic models are then analyzed to determine areas that should be protected to prevent these unacceptable radiological consequences.

Bibliography

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of vital areas at nuclear facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/ Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).

[6] SANDIA NATIONAL LABORATORIES, A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities, SAND2004-2866, SNL, Albuquerque, NM (2005).

[7] VARNADO, G.B., ORTIZ, N.R., Fault Tree Analysis for Vital Area Identification NUREG/CR-0809, SAND79-0946, Albuquerque, NM, Nuclear Regulatory Commission, Washington, DC (1979).

[8] KOREA ATOMIC ENERGY RESEARCH INSTITUTE, The Application of PSA Techniques to the Vital Area Identification of Nuclear Power Plants, KAERI, Seoul (2004).

[9] VALERI PANEVSKI. Possible approach for standard operating procedures development for intelligent security systems functioning. International Scientific Journal “Security&Future”, 5, 3, STUME, 2021, ISSN:2535-082X (online), 2535-0668 (print), 81-84;

[10] VALERI PANEVSKI. Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes. International Scientific Journal “Security & Future”, 5-ти, 2-ри, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2021, ISSN:2535-0668 (print), 2535-082X (online)), 42-45;

[11] VALERI PANEVSKI. Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems development – peripheral security systems. International Scientific Journal “Security & Future”, 5-ти, 1-ви, Scientific Technical Union of Mechanical Engineering "Industry 4.0", 2021, ISSN:2535-0668 (print), 2535-082X (online)), 3-6;

Possible approaches to ensure security of information for nuclear facilities

Dimitar Dimitrov
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *Sensitive information is information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Information security not only includes ensuring the confidentiality of information, but also includes ensuring the accuracy and completeness of the information (its integrity) and the accessibility or usability of the information on demand (its availability).*

KEYWORDS: *INFORMATION, SENSITIVE INFORMATION, CONFIDENTIALITY, INFORMATION SECURITY, ENSURING SECURITY OF SENSITIVE INFORMATION, IDENTIFYING AND SECURING SENSITIVE INFORMATION, SECURITY POLICIES*

1. Introduction

The overall objective of a country's nuclear security regime is to protect persons, property, society and the environment from harmful consequences of a nuclear security event.

Groups or individuals wishing to plan or commit any malicious act involving nuclear material or other radioactive material or associated facilities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with the appropriate measures [1].

Ensuring the security of sensitive information is a cross-cutting prerequisite for nuclear security, and the systems and measures to achieve effective information security are key elements of a countries' nuclear security regime.

This report provides short guidance on implementing the principle of confidentiality and on the broader aspects of information security. Much national and international guidance exists regarding the establishment and management of information security frameworks for information of various types, in the form of both high level guidance and detailed standards.

Instead, its goal is to assist operators in bridging the gap between existing government and industry standards on information security in general, the particular concepts and considerations that apply to nuclear security, and the special provisions and conditions that exist when dealing with nuclear material and other radioactive material.

2. Concepts and context

2.1 Definition of information

Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems.

Information can be represented and communicated by almost any means. In the nuclear domain, there is a vast amount of information in many forms.

Information assets are the equipment or components (including media) that are used to store, process, control or transmit information.

For the purpose of handling and security, information may be grouped into information objects. These may be defined as all elements of information that have value to an organization.

Typically, an information object comprises a set of data, information or knowledge that shares a common usage, purpose, associated risk or form of storage or transmission.

2.2 Identifying and securing sensitive information

Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport.

Such information may refer, for example, to the nuclear security arrangements at a facility, the systems, structures and components at a facility, the location and details of transport of nuclear material or other radioactive material, or details of an organization's personnel

Securing sensitive information is necessary because easy access to inadequately secured information can help adversaries to plan or commit malicious acts with relatively little effort or risk.

If, for example, a facility's physical protection plan were acquired by adversaries planning an attack on the facility, they would know the obstacles they would face, the size and arming of the guard force, the size of the response force and the approximate time it would take for that force to arrive at the site.

They would also know the important targets within the facility, their locations and the measures protecting them. Similarly, if an adversary wishing to steal nuclear material during transport succeeded in acquiring a device giving access to detailed information about the planned transport - because the device had been inadequately secured - the adversary could plan an attack more effectively. Thus, the possession of such information or information assets by adversaries would increase the likelihood of their success.

Ensuring confidentiality depends on the application of security measures to selected sensitive information and sensitive information assets (the equipment or components, including media, that process, handle, store or transmit sensitive information) in order to ensure that it does not fall into the hands of unauthorized individuals or organizations, either external or internal.

Guidance on measures against the insider threat is contained in Preventive and Protective Measures against Insider Threats [2]. Security measures should be based on risk analysis. The risk analysis should be kept up to date by a process of periodical reviews.

2.3 Information security

Information security, refers to the system, programme or set of rules in place to ensure the confidentiality, integrity and availability of information in any form [3].

At a minimum, it includes:

(a) Security of information in physical forms (e.g. paper and electronic media);

(b) Security of computer systems, sometimes referred to as computer security, information technology (IT) security or cybersecurity (additional IAEA guidance can be found in Computer Security at Nuclear Facilities [4];

(c) Security of information assets (e.g. information storage and processing equipment, communication systems and networks);

(d) Security of information about facility employees and third parties (e.g. contractors and vendors) that could compromise the security of the above;

(e) Security of intangible information (e.g. knowledge).

While confidentiality is often singled out, organizations should ensure that their information security programme addresses all three attributes. Loss of integrity or availability can negatively affect nuclear security just as loss of confidentiality can.

For example, if authorized users do not have timely access to information necessary for their duties (loss of availability), or if that information has been altered in such a manner as to mislead them (loss of integrity).

Information security should be considered and applied in the context of the overall security framework. It is closely interdependent with other security domains such as physical protection and personnel security [5].

For example, physical protection measures can be used to protect sensitive information and sensitive information assets, while confidentiality measures make attack against physical protection systems more difficult or uncertain for adversaries.

Gaps or shortfalls in any of the security domains can affect security in the others, so it is essential to use a comprehensive approach considering all domains together.

3. Framework for securing sensitive information

Securing sensitive information on a fragmented, facility by facility basis will not be effective. An effective national framework is necessary to ensure comprehensive security measures across all facilities, sites and organizations (governmental and non-governmental) handling sensitive information.

The operators should build this national framework, which will include establishing:

(a) The responsibility of the operator;

(b) A legal and regulatory framework;

(c) National guidance;

(d) Security policies;

(e) Classification schemes.

3.1 Responsibilities

The responsibility for ensuring the existence and effective operation of a countries' comprehensive nuclear security regime rests with the government of that country. Ensuring the security of sensitive information is an integral part of the nuclear security regime that the country should enforce.

Countries typically have government organizations or agencies that are responsible for overall national security, hereafter referred to as national security authorities. The national security authorities usually have the responsibility of defining the fundamental national policy on all aspects of security.

The security policies and instructions issued by the national security authorities are often general in nature, and not specifically designed for nuclear security.

However, many countries' national security authorities do have policies and guidance for securing sensitive information, for example in government or military use.

The countries relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities.

These are usually based on, and in accordance with, any national security policy and requirements issued by the national security authorities, but taking into account the special nature of the activities that involve such materials.

The competent authorities should also maintain close liaison with the national security authorities in order for the national threat assessment or design basis threat to be devised (for more information, see Development, Use and Maintenance of the Design Basis Threat [6].

Each organization should establish its internal policy, plans and procedures for ensuring the confidentiality, integrity and availability of any sensitive information related to nuclear security that it holds or handles, and for protecting related sensitive information assets, in compliance with the national security policy and the relevant national laws and requirements. All employees should be fully aware of the need for information security and follow their organizations' information security rules and procedures.

3.2 Legal and regulatory framework for securing sensitive information

Requirements for the maintenance of nuclear security within a country' boundaries should apply to all ministries, departments, agencies and other organizations that deal with matters identified by the country to be necessary for national nuclear security. The country may impose these requirements by laws, regulations or other legally binding requirements.

There should also be legislation in place that defines the sanctions or punishment that will be applied to any individual or organization who breaches such information security requirements. Such legislation may have sections which define the severity of particular types of breach of confidentiality or other information attributes and corresponding sanctions.

The competent authorities' regulatory powers should allow them to place obligations on the holders of sensitive information. The laws enacted for this purpose should mandate sanctions or punishment for unauthorized disclosure.

The legislation should also mandate that State ministries, departments, agencies and other organizations provide the competent authorities with all necessary support to enable it to fulfil its task of ensuring the security of sensitive information.

3.3 Security policies

In addition to issuing information security policies that comply with national requirements, the competent authorities should provide details of how these requirements should be applied to facilities and activities involving nuclear material and other radioactive material.

The countries' policy on nuclear security should demonstrate a commitment to information security. It should encourage this through the issue and maintenance of a comprehensive and appropriate information security policy to be applied to all facilities and activities involving nuclear material and other radioactive material, as well as any other locations where related sensitive information is held. The aim of the policy is to ensure that sensitive information is secured against compromise

Each organization and facility that handles sensitive information should then compile its own dedicated information security policy, based on that of the competent authorities where applicable. This policy should be communicated throughout the organization in a form that is relevant, accessible and understandable to the intended users.

4. Identifying sensitive information

The first step in classifying and securing information is to identify the information that is considered sensitive information.

Security controls should be considered for information of at least the following types, which could affect nuclear security

(a) Details of physical protection systems and any other security measures in place for nuclear material, other radioactive material, associated facilities and activities, including information on guard and response forces;

(b) Information relating to the quantity and form of nuclear material or other radioactive material in use or storage, including nuclear material accounting information;

(c) Information relating to the quantity and form of nuclear material or other radioactive material in transport;

(d) Details of computer systems, including communication systems, that process, handle, store or transmit information that is directly or indirectly important to safety and security;

(e) Contingency and response plans for nuclear security events;

(f) Personal information about employees, vendors and contractors;

(g) Threat assessments and security alerting information;

(h) Details of sensitive technology;

(i) Details of vulnerabilities or weaknesses that relate to the above topics;

(j) Historical information on any of the above topics.

Some of the above information, such as personal information, may also be subject to specific security requirements under other national laws or company policies.

5. Sharing and disclosing sensitive information

5.1 Sharing information

It is sometimes necessary for certain sensitive information to be shared with authorized agencies or companies and organizations that have a need to know the information. Sharing information can create efficiencies that would not exist if the information were to be developed and handled independently.

There are also occasions where not sharing information may damage security or weaken the overall planning, design and implementation of security measures.

Furthermore, as nuclear security responsibilities are often not held exclusively by any single agency, company or organization, it is often necessary that information be shared among those who share the security responsibilities.

For example, it is often necessary in the interests of national security for the competent authorities to pass sensitive information to the national security authorities and vice versa, for example changes in threat assessments or information on security events should be communicated in a timely fashion to relevant parties, in order to enable adjustment of security measures and exchange of operational experiences as a basis for continual improvement. In addition to security considerations, information sharing may be needed to support other objectives, including safety assessment, operational and commercial needs.

It is often also necessary to share certain information with other countries or relevant international organizations. In such a case, there should be an agreement in place to guarantee that sensitive information is secured by the recipient in a manner consistent with the requirements of the owner of the information.

Security of information may be assured through a bilateral or multilateral treaty or agreement that defines how information will be secured against disclosure. Such agreements would typically describe the required protection measures to be applied to sensitive information for different classification levels in each country.

5.2 Disclosing information

Most countries have in place laws addressing the security of information of importance to the national interest. Such laws specify sanctions that will be imposed should a person, a national of that country or otherwise, breach the laws on confidentiality of such information.

There are also usually laws that regulate an individual's access to official government information. There may be mechanisms to resolve disagreements between the government and other parties regarding which information can be withheld to protect national security.

Several countries have freedom of information legislation or other laws that allow members of the public to request access to information held by the authorities. Typically, the only information that may be withheld by the authorities is that of types covered by specified exemptions, such as information associated with national defence, or private and personal information.

Other laws and regulations may require that certain types of information, which may include sensitive information, be disclosed. One example is environmental legislation that requires public reporting of specified information. It should be ensured that such laws allow exemption of information that might affect national security or the security of third parties.

6. Management framework for confidentiality

A management system should be in place that establishes policies and objectives and enables the objectives to be achieved in an efficient and effective manner. An integrated management system, The Management System for Facilities and Activities [7], is a vital support element to a nuclear security culture. Many activities at facilities are controlled by management systems.

These ideally integrate security, safety, health, environmental, quality and economic elements in a single management process or a set of integrated and mutually reinforcing systems. Information security should be integrated into the existing management system of the facility or organization to ensure information confidentiality, integrity and availability.

Ensuring the confidentiality, integrity and availability of sensitive information depends on effective designation of roles and responsibilities, classification to identify which information is sensitive and needs to be secured, why it needs to be secured and to which level, decisions on how to secure such information, implementation of the necessary security measures, and response (including recovery) if such information is compromised, stolen or lost.

The management framework explained in the following applies to all levels of management at organizations holding or handling sensitive information.

Management has the overall responsibility for ensuring information security is in place and effective throughout the facility or organization, in order to secure sensitive information.

All personnel who handle sensitive information have a responsibility to ensure its security in accordance with related national legislation as well as the organization's policies and procedures.

7. Conclusions

All information security incidents should be investigated. Policies and procedures should be defined governing information security incident investigation. An investigation should aim to determine

whether a security incident has a minor or major impact on information security and confidentiality [8].

The competent authorities may then initiate any appropriate action. An example of a minor incident may be a failure to lock up or secure a document properly that did not result in the loss or compromise of any information. A major incident, for example, may be the theft of a security plan that results in a strategic threat to an organization.

The competent authorities should maintain records of the number and type of reported information security incidents. Recurring incidents or trends in security failures should be identified and may indicate the need for changes to security policy or improvements in security procedures or programmes.

Updates on trends and changes should also be included in awareness training so that an appropriate security culture among employees and contractors is maintained. Organizations and facilities should also maintain their own records.

Bibliography

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, Vienna (2015).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[3] PANEVSKI V.S., "Opportunities for determining factors affecting the development of intelligent security systems models", 1/2020, International Scientific Journal Security & Future, 2020, ISSN:(PRINT) 2535-0668, ISSN: (ONLINE) 2535-082X, p.p. 6÷9;

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[5] PANEVSKI V.S., "COMPATIBILITY BETWEEN DESIGN OF MECHATRONIC SYSTEMS FOR CRITICAL INFRASTRUCTURE SECURITY AND TECHNOLOGICAL READINESS LEVELS", International Scientific Journal "Security & Future", 4, 3, Scientific Technical Union of Mechanical Engineering "Industry-4.0", 2020, ISSN:2535-0668, p.p. 111÷114;

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[8] Valeri Panevski, Lyudmil Nedelchev, "Structuring key partnerships in the field of critical infrastructure security systems", International Scientific Journal Innovations, 10 (2022), 2, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING "INDUSTRY-4.0", 2022, ISSN:ISSN PRINT 2603-3763; ISSN WEB 2603-3771, p.p. 53÷56;

Cyber warfare, a new aspect of modern warfare

Fatmir Basholli
Lecturer in the Department of Engineering, Albanian University, Tirana, Albania.
fatmir.basholli@albanianuniversity.edu.al / fbasholli@yahoo.com

Abstract: *Cyber warfare nowadays is a new and very important concept of the modern world. After land, sea, air and space, the war has entered the fifth dimension: cyberspace. Some computer glitches or attacks paralyze military e-mail systems, refineries and pipelines explode, air traffic control systems collapse, trains derail, financial data gets misdirected, power grids damaged, satellites go out of control. Worst of all, the identity of the aggressor remains a mystery. The effects of a cyber war are similar to those of a nuclear attack. This requires protective measures and security for the information that circulates in these communication systems and networks and constitutes one of the challenges of today's time. Threats to communication and information systems have made cyber defense in the field of homeland security an element that must be taken into consideration.*
Keywords: *CYBERNETIC WARFARE; ELECTRONIC; IT; NETWORK; COMMUNICATION*

1. Introduction

The Internet, as one of the most important inventions, has broken all barriers and transformed the way we communicate, work, have fun, perform services, etc.

Our world has become increasingly networked, with digitized information supporting key services and infrastructures [1]. Nations, states, organizations and ultimately users are all concerned about threats to the confidentiality, integrity and availability of digitized information [2]. In a digital world that is progressively permeating every area of our daily lives, both public and private, security is a must. In the field of information technology, cyber security plays a critical role. When we are in an attack, cyber security is the first thing that comes to mind. Protecting our personal data online has become a major concern. The large number of digital devices [3] connected to the network has expanded at a rapid pace in recent years, exceeding by the end of 2021 about 50 billion and this results in an increase in the number of vulnerable devices [4]. Businesses are transforming into data exchange relying on telecommunication network technology [5], therefore "data security" is vital to the future of intelligent cyber security systems and services. The focus of this paper will be the analysis of cyber attacks against the e-albania digital platform and the preventive measures that must be taken against cyber threats on the Internet and especially on the Intranet.

2. Problem discussion

Cybersecurity requirements will be a fundamental feature of the twenty-first century. The term "cyber security" refers to approaches and procedures for protecting digital information. An information system stores, transmits or uses data that a criminal claims to possess. The network, servers, and computers are simply conduits for data. Effective cyber security reduces the risk of cyber attacks and protects companies and individuals against the illegal use of systems, networks and technology.

Cybersecurity refers to the technologies, techniques, and procedures used to prevent hackers from damaging computers, programs, networks, and data [6]. Cyber security specialists are increasingly dealing with a wide range of cyber threats in near real time, to detect, analyze and provide protection against such threats with the intelligent use of a protection practice.

Cybersecurity is essential for government infrastructure, where data is stored on computers and other devices [7] and may contain sensitive information, such as intellectual property, financial data, personal information or other types of data [8] , in which illegal access or exposure may result in adverse effects. Cyber attacks are the fastest growing crime in the world and they are getting bigger, more sophisticated and more expensive.

Hackers steal an individual's personal information and sell it for profit, which is known as identity theft [9],

recognizing that no one is immune to the threat posed by cybercrime. Digital educational platforms are a critical component of any cybercrime plan related to the use of the network in scientific research and simulation applications[10]. Because of the above, cyber security has become an important part of business and the focus is now on developing appropriate response plans that minimize the damage in the event of a cyber attack.

The types of cyber security are numerous and are often known as electronic information security. They act as a barrier, ensuring that data on digital devices is invulnerable to external attacks [11]. So cyber security is more about risks from outside the network.

The security of Critical Infrastructure, on which companies rely heavily, is vital and uses a variety of security techniques. Among them, we can mention electricity networks, water purification, traffic lights, shopping centers, hospitals, etc. They can serve as a platform for cyber malware to infect endpoints to which these systems are connected. These organizations must have a contingency plan that would help their businesses withstand cyber attacks, because the security and resilience of this critical infrastructure is vital to our safety and well-being.

Network security is about protecting against hostile intrusion and limiting access to it by recording user activities. As a result, institutions, public or private enterprises, must implement a security program to monitor the internal network and infrastructure and to combat cyber-attacks and network-related viruses. Security teams are prepared to implement policies and procedures to protect the network, highlight errant traffic, and be alerted to real-time threats, which helps them better manage network security monitoring from exploits spam and creating fresh and strong passwords.

End-user education recognizes that cybersecurity solutions are only as strong as their weakest links, which are the people who use them. End-user education includes instructing users on best practices such as not clicking on unexpected links or opening strange email attachments, which can lead to the spread of malware and other dangerous programs. Advising users not to connect unidentified USB drives.

Endpoint security shows us that today's threats increasingly come from endpoints, meaning that centralized network protection is insufficient. Moving security perimeters that are not clearly defined require adding new levels of security through endpoint protection. In order to avoid risks that may come from the use of remote devices, security must keep access points under primary control [12]. This enables businesses to protect their servers, workstations and mobile devices from cyber attacks both locally and remotely. The interconnection of devices in a network create access points for threats and vulnerabilities, and by stopping attempts to access these entry points, endpoint security becomes more effective. File integrity monitoring, antivirus and anti-malware programs will be the main techniques used.

Website Security is used to prevent and protect websites from cyber security threats. In recent years, the incidence of data breaches on websites has increased steadily, resulting in identity theft, financial loss, reputational damage and damage to the image of the institution or business. The main reason for this is that many website owners believe that their site is protected and maintained by their provider. Some of the important techniques and tools used for internet security are site scanning, malware removal, firewall application and security testing.

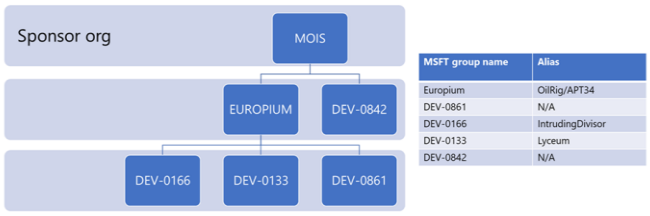
3. Objectives and research methodologies

In the middle of July of this year, devastating cyber attacks were launched against the digital platform of the Albanian government,

blocking the websites of the ministries and the public services of the e-albania platform [13].
From the analysis of this attack on the scale of a "Cyber War", it can be seen that there were several phases in this campaign such as:

- ❖ Initial intervention, deployment of ransomware malware.
- ❖ Exfiltration of data, gaining initial access to their receipt.
- ❖ Data encryption and destruction.
- ❖ Information acquisition operations.

The Microsoft Threat Intelligence Center (MSTIC) estimated that the actors involved in gaining initial access and exfiltrating data in the attack were linked to Iran's Ministry of Intelligence and Security (MOIS) using three unique groups in this activity. criminal *(fig.1).*



MSFT group name	Alias
Europium	OilRig/APT34
DEV-0861	N/A
DEV-0166	IntrudingDivisor
DEV-0133	Lyceum
DEV-0842	N/A

Figure 1. The threat actors behind the attack against the Albanian digital platform.

The analysis of the attacks based on the evidence collected from the traces left in the digital systems showed that:

- ♣ The attackers operated outside Iran.
- ♣ The attackers responsible for the intrusion and extraction of data used tools used in previous attacks.
- ♣ The data wipe code was previously used by known attackers.
- ♣ The ransomware was from the same digital certificate previously used by the Iranian hackers.

The crime triangle [14], which is often used to define cybercrime, states that for a cybercrime to occur, there must be three variables: a victim, a motive, and an opportunity. The victim is the person (subject) that will be attacked, the motive is what motivates the criminal to commit the crime, and the opportunity is when the crime will be committed on the system or on an unprotected device.

It was noted that the intrusion and exfiltration was carried out by a group that likely had access to the network of an Albanian government victim from May to July 2021, exploiting a vulnerability in ***a patched SharePoint server, called the administration. al*** and using a service account of a member of the misconfigured local administrative group. Through this intervention on the Internet was provided the possibility to upload, download and delete files, to rename and execute commands with an option as a specific user.
Analysis of Exchange logs later showed that between October 2021 and January 2022 mail was exfiltrated using the victim's network from the following IPs:

144[.]76[.]6[.]34; 176[.]9[.]18[.]143; 148[.]251[.]232[.]252

The attack group most likely associated with MOIS used ***the Jason.exe tool*** to access compromised mailboxes. The cyberattack on e-albania used a common tactic of attackers deploying ***ransomware first, followed by malware.*** The group in this attack had the motive of deleting data in the target systems. They use the same ***EldoS RawDisk*** license key and driver as ***ZeroCleare.***
The code used in this attack had the following characteristics: Filename cl.exe; rwdsk.sys; Embedded; GoXml.exe.
The attacker's logo was an eagle of the hacker group "Predatory Sparrow" inside the Star of David *(fig.2).* This signals that the attack on Albania was a revenge. The messages from these attacks targeted government politicians for their support of the MEK organization.



Figure 2. Ransomware image and Homeland Justice banner

DART and MSTIC relied on attack analysis using Microsoft 365 Defender. The analysis identified the use of vulnerabilities to ensure web resilience, discovery actions, common credential harvesting techniques, protection evasion methods to disable security products, and a final effort of actions to target encryption and wipe digital information. . This destruction attempt had less than 10% total impact on the target systems environment.
Unrecoverable tools were identified, suggesting that discovery attempts were present in the form of executive file names, resident mailbox data, database and user details. Similar actions by threat actors observed by MSTIC and DART detail the custom and open source tools used for these efforts that were:

IPGeter.exe; FindUser.exe; recdisc.exe; NetE.exe; advanced_port_scanner.exe; mimikatz.exe; shared.exe; Stored CSV and TXT files

Before the final phase of the attack began, threat actors gained administrative access to a deployed endpoint detection and response (EDR) solution to make modifications, removing libraries that affected agents across the enterprise. In addition, a binary to disable Microsoft Defender Antivirus components was spread using custom tools. The distributed binary named ***disable-defender.exe*** queries for ***TokenElevation*** using the ***GetTokenInformation API*** and checks if the process was running with the privileges granted. *(fig. 3)*



Figure 3. How the attacker was able to evade the defense components

After successfully creating its own process with the ***TrustedInstaller*** privilege, it proceeds to disable ***Defender components***.

3. Conclusion

"Cyberwar" organized and directed by restructured Hacker groups and when there is state support is dangerous and defeating these attackers is extremely difficult.

The most dangerous attacks that continue to be used in this "cyber war" continue to be:

- Phishing attack where cyber attackers attempt to obtain personal information or data, such as usernames, passwords and credit card numbers, by impersonating a trusted entity under these circumstances.
- Malware is designed to disrupt the normal operation of any device, including mobile phones, desktop computers and servers.

- Ransomware, a specialized malware distributed to extort money from targets and is one of the most widespread and well-known cases of cyber attacks. To gain access to the target computer's hard drive, the attacker distributes malware like a virus. It then encrypts the data and makes the computer and its contents inaccessible until the user pays the ransom demanded by the attacker.
- Denial of Service (DoS) attacks involve flooding the server host with far more requests than it can handle, causing the server to fail.
- Smurf attack, to overwhelm a target network with traffic, this attack uses IP spoofing and ICMP protocol.
- Botnets, are millions of malware-infected systems under the control of hackers to carry out DdoS attacks. These attacks are difficult to track because the botnets are located in different geographical locations
- Rogue Access Point The rogue access point is one of the most common wireless security risks, and has been used in a variety of attacks, including DoS and data theft. A rogue access point is an illegitimate yet functional network node.
- Zero Day Attack, where the source of the vulnerability can be a flaw in your software, hosted application, or even your hardware.
- IoT Based Attacks, where IoT devices are less secure than most modern operating systems. Hackers can go after medical devices, security systems, and smart thermometers, or they can try to exploit IoT Devices to carry out large-scale DDoS attacks.
- Insider Threats, is a threat to a company's security or data that originates from within the company. They are difficult to identify and avoid. They come from employees, contractors, and third-party affiliates of a business.

Some protective measures for cyber security:

- Firewalls are at the heart of security technologies and have become one of the most critical security tools. [124].
- Penetration Testing, often known as pen testing, is a method of assessing a company's security systems and the security of its IT infrastructure by safely exploiting vulnerabilities.
- Web Vulnerability Scanning Tools, are automated programs that analyze the organization's web, applications for security flaws.
- Staff Training, is not a "cyber security tool", but it is one of the most effective types of defense against cyber attacks to have knowledgeable staff who understand cyber security.
- Out-Dated Hardware, software updates must match the hardware ones.

4. References

[1]. M. Gallaher, A. Link and B. Rowe, Cyber Security: Economic Strategies and Public Policy Alternatives, Edward Elgar Publishing, 2008

[2]. T. Rid and B. Buchanan, "Attributing cyber-attacks", Journal of Strate St., vol. 38, no. 1-2, pp. 4-27, 2015

[3]. Lillian Ablon, Martin C. Libicki and Andrea A. Golay, Markets for Cybercnme Tools and Stolen Data: Hackers‟ Bazaar, pp. 1-85, 2014

[4]. Dawson, J. and Thomson, R., "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", Frontiers in Psychology, 9(JUN), pp. 1–12, 2018

[5]. C. L. Philip, Q. Chen and C. Y. Zhang, "Data-intensive applications challenges techniques and technologies: A survey on big data", Information Sciences, vol. 275, pp. 314-347, 2014

[6]. C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends", Tech. and Health Care, vol. 25, no. 1, pp. 1-10, 2017

[7] S. King, & D. B., Boykin IV (2019). *DISTINCTLY DIFFERENT DOCTRINE: Why Multi-Domain OperationsIsn't AirLand Battle 2.0.* Army Magazine, 69(3), 18–21.

[8]. C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Res., vol. 22, no. 9, 2020

[9]. Asif Perwej "The Impact of Pandemic Covid-19 On The Indian Banking System", International Journal Of Recent Scientific Research (IJRSR), ISSN 0976 –3031, Volume. 11, October, 2020

[10]. S. Wu, Y. Chen, M. Li, X. Luo, Z. Liu and L. Liu, "Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools", EEE/ACM Transactions on Networking, vol. 28, no. 2, pp. 874-887, 2020

[11]. S. Aftergood, "Cybersecurity. The Cold war online", Nature, vol. 547, no. 7661, pp. 30, 2017

[12]. M. Schwenk Jensen, J. Gruschka and N. Iacono, "On technical security issues in Cloud", IEEE International Conference on Cloud Computing, pp. 109-16, 2009

[13] Microsoft's report on the cyber attack in Albania July 2022

[14]. N. Dhanjani, B. Rios, an d B. Hardin, Hacking: The Next Generation: The Next Generation. O‟Reilly Media, Inc., 2009

Information security in archival science

Teodora Licheva
New Bulgarian University
Sofia, Bulgaria
teodora_licheffa@abv.bg

Abstract: *The article with the title "Information security in archival science" focuses on the need for the state archives system to be able to meet the modern needs of archival information users, individuals and legal entities. Modernization and updating of archives cannot happen without using the new technological possibilities. At the same time, a challenge of the modern society of rapidly developing and changing information technologies is to what extent can digital information be trusted? Archival institutions have the opportunity to participate in the creation of the so-called a new architecture of security, trust and reliability.*
The article is divided into an introduction, presented a model of the development and implementation of blockchain technology in the National Archives of South Korea, conclusion and literature.
Keywords*: BLOCKCHAIN, INFORMATION SECURITY, ARCHIVE*

1. Introduction

Blockchain is an innovative database technology. It is a digital ledger and the information is distributed in a "chain of blocks".

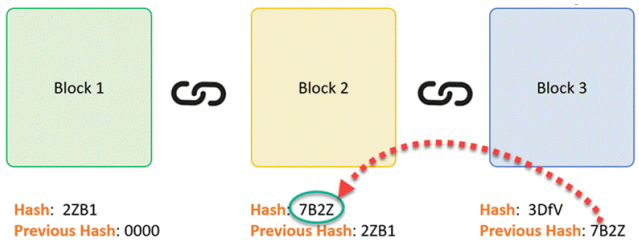


Fig.1 *Blockchain technology*[1]

The blockchain system consists of the following elements:

1. Information that is stored in a block;

2. Hash. This binding element is unique and is passed on to the next block. There is a role of fingerprint;

3. The hash of a previous block is the last piece in a blockchain.

Blockchain is a data storage platform that, once stored, cannot be changed. This function is achieved by distributing authority and monitoring by all participating members in the system, rather than using centralized control.

The inherent property of blockchain decentralization meets the most important value in record management and is neutral to all external forces. Blockchain platforms are an extremely attractive technology in the field of record and archive management.

Data authenticity and integrity are essential attributes of records and archives management. Integrity is a necessary condition for maintaining authenticity. And although there are many practical constraints (e.g. budget, technology and time), it is necessary for national archive and archival institutions to apply blockchain to their management systems and create a long-term plan to achieve such application.

In this article, I will focus on the results of a research project of the National Archives of South Korea, which was conducted from 2019 to 2021.[2]

2. Presentation of blockchain technology from the point of view of information security

Thanks to the Korean government's policy of investing in digital transformation, NAK Blockchain has developed the NAK document storage platform for research and development (R&D).[3]

In 2019, NAK developed a blockchain recording platform using a hyperledger[4] system. As early as the following year, R&D was conducted to implement archival practices for recording and storing documents using the platform. In 2021, research continues to verify the integrity of input data from the multiple government administration systems in South Korea.

To understand the rationale behind the introduction of blockchain technology, we must first understand the digital environment of the Korean government[5]. In 2001, the Korean government passed the E-Government Act and began to electronically convert paper-based government activities. Various types of paper documents such as government taxes, criminal justice records, social security and financial documents have been digitized and a number of information systems have been created for their use and management[6]. Since the early 2000s, the Korean government has provided a significant budget to create various business systems to convert large amounts of paper records into digital versions.

Thanks to these investments, there are now more than 16,000 information systems used by government administrations and institutions involved in the digitization of paper records. The types and number of electronic records through these systems are growing significantly. NAK archivists, who are responsible for the preservation of public records, face increasing difficulties in ensuring the authenticity of these new types of records with traditional records management methods. This is the main reason why NAK employees are looking for a solution and are interested in innovative technologies, including blockchain technology.

It is the responsibility and obligation of archival institutions to maintain authenticity and deliver unaltered documents to future generations, regardless of the type of public record. Durability is the minimum requirement for all electronically created records to maintain authenticity from creation to end of life. In particular, the bitstream[7] of the records must not be changed, except in cases where it is determined that it is no longer possible to maintain the current state of the records and they must be properly converted to another format.

Extremely rare are cases that involve changes in the storage format due to a change in record-keeping policy, a change in the method of providing information, a change in the information itself if there is a change in the method of authentication, and other factors.

NAK adopts a long-term storage strategy that combines migration and encapsulation to ensure the authenticity of digital documents, their security and non-tampering. The storage strategy aims to convert digital record objects into PDF and encapsulate them by adding electronic signatures as well as recording metadata. NAK refers to these encapsulated objects as NAK Encapsulated Objects (NEOs)[8]. Converting most types of electronic documents to NEO is usually not difficult, but converting large objects, such as audiovisual recordings, and a number of objects such as data sets in information systems, is actually not easy at all. Thus, NAK was unable to apply authentication strategies, such as NEO, to audiovisual recordings or datasets.

In 2020, NAK decided to use blockchain audit trail technology[9] to solve the authenticity problem of audiovisual recordings. In this way, the security of the network and information resource is guaranteed. Next year, National Archives officials are auditing measures to ensure the integrity of documents, using blockchain auditing technology to monitor transactions in the data sets created in these systems. Based on this solution, NAK promotes R&D projects that have developed a blockchain system for audiovisual records and an authenticity dataset.

The organization of the National Archives of South Korea to use blockchain technology consists of two phases of research and development. In the first case, the use of blockchain transaction auditing technology to ensure the authenticity, authenticity and reliability of audiovisual archives. The second case is the use of blockchain technology to verify that the data sets of multiple information systems built by government institutions are managed without falsification or manipulation.

In addition to existing electronic documents, the former offers a method of maintaining authenticity suitable for a new type of record called an audiovisual record, and the latter datasets. In addition to the fact that each R&D case deals with a different type of record, the location and environment in which each record physically exists should also be noted. Audiovisual records are transferred and managed by the Central Archives Management System (CAMS) and Multimedia Asset Management (MAM), which are managed by NAK. In contrast, datasets are managed in two main ways according to record evaluation. The first is a method of transferring records to NAK, such as audiovisual records, and the second is a method of self-management of records by the institution that creates them. When the data sets are transferred to the NAK, a newly designed and built system can manage them without considering the system before the transfer. Therefore, this study focuses on self-administered datasets. In the NAK transfer method, a new system can be designed and built freely. However, in the method of self-management from the source institution without transfer to NAK, there is a limitation that it should not affect the information system, including the current data sets, and it should be applicable to different information systems[10].

2.1. Applied concept

The ISO 15489[11] standard establishes the basic concepts and principles of records management. According to ISO 15489, records must maintain the characteristics of authenticity, integrity, reliability and usability throughout the management process. To demonstrate that these four characteristics are preserved in records management processes, the metadata that is used in records is managed along with the records themselves[12]. Dr. V. Memljo[13] distinguishes three separate stages in the development process of the concept of recording archives in the blockchain. In the first stage, the integrity of the authentic records is ensured by separately establishing a blockchain platform as a cryptographic mirror system to the records preserved within the existing information system currently in use. In the second stage, tasks are performed together with record management within a system by developing and implementing the new work system itself as a blockchain platform. In the final stage, tokens ensure the integrity of non-electronic records by attaching to the records and tracking the specific tokens that can be recognized by the blockchain platform[14].

NAK currently creates and manages audiovisual records in three distinct formats – original, copy for use and preservation, and the MAM system.

A blockchain system has been developed for the authenticity of audiovisual recordings.

The hyperledger variant of the blockchain system and the prototype code are used to verify the authenticity of the records[15]. This code is provided only if the request is approved and authorization is required when disclosing inside information.

2.2. Authenticity check

Archives should be able to provide part of a whole record and in different formats, depending on the needs of the users as well as the service policy. Audiovisual records can also be changed in different formats according to the needs of users of archive information, and blockchain should be able to verify and track all change transactions and provide authentic verification services.

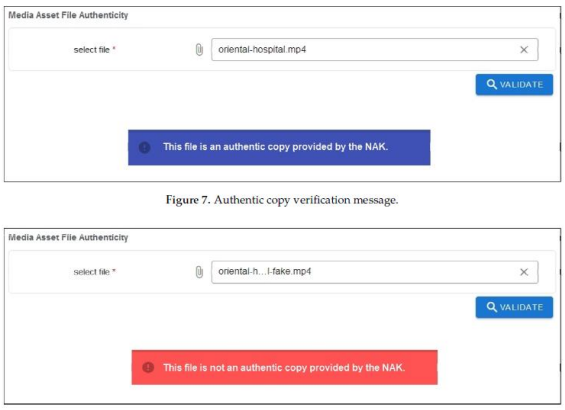


Figure 7. Authentic copy verification message.

Fig.2 *The interface of a developed authentication service*

2.3. Execution

To test the effectiveness of the proposed model, NAK staff are using Loopchain[16] as a blockchain platform[17], with prototype code available online[18].

It is difficult to introduce a public blockchain into the public domain due to the presence of confidential or private information that should not be exposed to the public sector and needs to be protected from detractors. For this reason, private blockchain is suitable for public administration, involving several participating institutions or authorized groups of administrations with similar activities. The larger number of participating nodes provides more security and stability, and the participation of private blockchain nodes should be increased by establishing the control of government administrative organizations, such as close cooperation.

3. Conclusion

Administrative information systems in South Korea were established after the enactment of the E-Government Act in 2001, and the e-Government Support Project was promoted. This document proposes a method for verifying the integrity of administrative datasets. When administrative information systems were first created, there was no blockchain technology and therefore this system was not set. For different types of DBMS, a method for checking integrity should be offered in a consistent and unified manner. It is best to adopt a mirror system method with a small amount of integrity information and metadata such as hash values for real datasets.

With the advent of blockchain technologies and the creation of an administrative information system in the future, it must be designed to store data sets on the blockchain. The transaction of creating, reading, updating and deleting in the database should not reflect the actual data by blocking with the blockchain through a smart contract, but should put the end goal in the direction where the actual data itself is stored in the blockchain.

4. Literature

1. ISO 15489-1. Information and documentation-records management part 1. In Concepts and Principles; ISO: Geneva, Swiss, 2016; pp. 4–6

2. Jung, C.-S. The Theory of Electronic Government, 1st ed.; Seoul Economic Management Publishing Company: Seoul, Korea, 2007; pp. 99–128

3. Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]

4. National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017

5. Wang, H.; Yang, D. Research and Development of Blockchain Recordkeeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090

6. https://www.guru99.com/blockchain-tutorial.html#1

[1] https://www.guru99.com/blockchain-tutorial.html#1
[2] Wang, H.; Yang, D. Research and Development of Blockchain Record-keeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090
[3] Research and development and developments in science
[4] An open source blockchain platform and collaborative approach to distributed ledgers. By developing standards and a comprehensive blockchain framework, Hyperledger has received support from organizations including Cisco, American Express and IBM. https://www.hyperledger.org/
[5] Wang, H.; Yang, D. Research and Development of Blockchain Recordkeeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090
[6] Jung, C.-S. The Theory of Electronic Government, 1st ed.; Seoul Economic Management Publishing Company: Seoul, Korea, 2007; pp. 99–128.
[7] Binary sequence, bit stream. A sequence of bytes.
[8] National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017.
[9] The so-called audit trail. A series of computer event records for an operating system, application, or user activities. It is an analysis of managerial, operational and technical control.
[10] National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017.
[11] Records Management Standard.
[12] ISO 15489-1. Information and documentation-records management part 1. In Concepts and Principles; ISO: Geneva, Swiss, 2016; pp. 4–6.
[13] Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]
[14] Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]
[15] NAK-DLT. Available online: https://github.com/Hosung-wang/NAK-DLT (accessed on 12 July 2021).
[16] An enterprise blockchain platform where only identified users can participate in the network.
[17] LOOPCHAIN. Available online: https://www.iconloop.com/en/loopchain (accessed on 21 July 2021).
[18] Prototype for Verifying Integrity of Dataset using Blockchain. Available online: https://github.com/likeba/VID (accessed on 21 July 2021).

Blockchain based solution for securing real property transaction: a case study for North Macedonia

Admirim Aliti[1], Elva Leka[2]; Marika Apostolova[3]; Artan Luma[4]
South East European University, Tetovo, North Macedonia[1,3,4]
Polytechnic University of Tirana, Tirane, Albania[2]
aa03511@seeu.edu.mk, elva.leka@fgjm.edu.al, m.apostolova@seeu.edu.mk, a.luma@seeu.edu.mk

Abstract**:** *This paper will focus on the implementation of decentralized technologies, such as blockchain, on the issuance and management of real estate properties, starting with ownership of the certificates. The focus will be the improvement of the actual process, as well as increasing integrity and trustworthiness of ownership certificates. A series of technology and methodology selections will be made, along with the main plan of setting up the decentralized networks and enabling communication with the user. We propose a framework to manage real estate property's certificates and explain in detail the architecture of the system and each component of the system. This system will be based on Ethereum EVM, where the main execution will take place, the smart contracts will be deployed and the main dataset will be stored. IPFS will be used to store files such as photos or scanned documents and will be attached to the certificate in blockchain.*
KEYWORDS: *BLOCKCHAIN TECHNOLOGY, REAL ESTATE, CADASTRAL MANAGEMENT, TRANSPARENCY, PUBLIC ADMINISTRATION*

1. Introduction

Blockchain is being used even more in fields such as DeFi (Decentralized Finance), Education, Cryptocurrencies, NFT markets, Copyright, IoT, Health care, insurance, etc. [1,2]. However, there doesn't seem to be a solid implementation of real estate. Most solutions focus on creating a relationship between owner-client, agency-client, or investor-client, making the payment process automatic. A blockchain system that enables ownership still remains to be developed. The current process of obtaining an ownership certificate is tedious and time-consuming.

As of now, most of the institutions which issue certificates are based on a centralized system, where data is stored in a single location owned by an entity or company, or in some cases not stored digitally at all. Furthermore, actual systems are not made to handle large amounts of parallel requests and lack the integrity of the data stored. One example would be the downtime during a DDoS attack, or temporary (maybe even permanent) loss of data due to attacks, viruses and errors, or even human errors [3]. Another issue, as mentioned above, is the integrity of data stored and transparency, where digital access to the certificate is often missing.

From our literature review, we identified that there exists a gap to the implementation of blockchain in the Land Administration System (LAS), especially in real property management. LAS represents a system that is used to manage a real property with the main functions such as: (1) locating and identifying that property; (2) keeping a record of ownership of past and current data; (3) value; (4) and use of the property. It also contains data about the physical, spatial and topographic characteristics of real property [4].

Taking into consideration that LAS generates very important data seeing from a social, economic and political perspective, it is of great importance that the LAS be immutable, transparent and tamper-proof. Even though a lot of public services rely on data stored in systems that are used for LA, we still face a lot of problems in those LAS, relating to: (1) the correctness of stored data, (2) efficiency, (3) time consuming on the process of registering real estate transactions (month/years) [5]. In our previous paper [6], we have done a Systematic Literature Review and have analyzed that blockchain technology has the potential to play a critical role in the digitalization sector, not only in terms of administrative efficiency, but also in terms of increasing transparency and accessibility of services. Blockchain-based solutions facilitate citizen-government collaboration by safely streamlining and automating procedures while maintaining privacy and secrecy.

We propose to use blockchain technology to implement a system to manage real estate properties and to avoid all above mentioned actual drawbacks. Therefore, in this work, a blockchain-based

framework is proposed to develop a land administration system to manage those properties. The proposed framework was simulated in Ethereum blockchain platform; and showed that the framework contributed to develop a secure, reliable, scalable, effective and efficient land administration system.

In Section II is presented a background and related work of blockchain adoption in Land Administration System. Section III presents the architecture and details about each component of the proposed system. The necessary interfaces to be implemented are described at section IV and conclusions and future work in section V.

2. Background and related work

2.1 Background

A Blockchain network is a distributed system that relies on a consensus algorithm, which responsibility is to ensure agreement on the states of certain data among distributed nodes [7]. Considering that the consensus algorithm is the core component that indicates in the performance and the way how the system behaves, it is important to choose the right consensus algorithm depending on the system needed to be implemented. There are several consensus algorithms that can be used in blockchain, which are categorized into two categories: (1) *proof-based*, which requires the nodes joining and verifying the network to show that they are more qualified than the others to do the appending work and (2) *vote-based consensus algorithm*, which requires nodes in the network to exchange their results of verifying a new block or transaction, before making the final decision [8]; such as: Proof of Work (PoW) and Proof of Stake (PoS).

For the implementation of the system, we need to develop smart contracts in the Ethereum platform. A smart contract is a piece of software that stores rules for negotiating the terms of an agreement, automatically verify fulfilment, and then executes the agreed terms [9]. The correct execution of smart contracts is enforced without relying on a trusted authority. We have chosen Solidity [10] programming language to develop the smart contracts of our system. Solidity is an object-oriented programming language developed in 2014, somewhat similar to Java. With the use of Solidity, we would encounter a new definition which is a "smart contract". This is a set of instructions that does certain actions depending on user input. These contracts operate within the internal blockchain environment called Ethereum Virtual Machine (EVM) [11], and it is where the contract will rest after its deployment and using these smart contracts we will issue and verify certificates.

2.2 Related Work

Many solutions have been proposed and developed from the perspective of using blockchain in public administration. We limit our discussion to the systems and architectures that propose blockchain-based solutions in LAS or especially in real estate certificate management.

Blockchain technology is already being used by European states, but Sweden [12] is the first country that has adopted blockchain on

the country's land registry since 2016, with the intention to address security issues, reduce fraudulent activities, eliminate paperwork, and speed up transactions. Furthermore, Georgia and Netherlands have advanced in using blockchain in government. Georgia [13] created a blockchain registry system that allows citizens to verify the ownership of a property. Meanwhile, the Netherlands initiated a project in May 2018, which utilizes blockchain and Artificial Intelligence (AI) to register ownership details of a property and geographical coordinates.

In their paper [14] authors have proposed a system architecture for a blockchain-based Land Information System (LIS) in Serbia, which responsibility would be keeping track of transactions in LIS by offering immutability, increasing security, efficiency, integrity and improving the necessary time for a transaction to be processed. Furthermore, they have provided and detailed the design of the system, framework, and implementation of the system in the Ethereum platform. They argued the benefits this system could bring compared to the actual system of how transactions are handled in Serbian land administration.

Torun *et al.* [15] have proposed a hierarchical blockchain architecture for a relaxed hegemony cadastre data management in Turkey. In his study, he has identified the problem of inconsistent boundary determination and has proposed a methodology, where a transaction of a boundary change could not be booked in the land registry without the common and joint approval of all stakeholders. The study gives the design and implementation aspects of "the GIS part" of the component and aims to solve the particular problem of multiple physical boundaries for identical cadastral boundary data and for providing an approach to introduce the land owners into the core of cadastral decision making in the environment of open-data-policy, decentralization and democratization of geospatial data.

Furthermore, in their paper [16] the authors have analysed the possible applications and limitations of adapting blockchain in Land Administration. In this article are discussed all characteristics of blockchain technology and how they may have an impact in different blockchain-based implementations of land administration. The authors argue that the number of peer-reviewed papers on the possible application of blockchain in LAS is limited and blockchain implementation/development is still in the early stages.

Muller *et al.* [17] have presented the possibilities for the implementation and the potential design of a blockchain-based land register in Germany. The idea of upgrading the current electronic land registry with a blockchain solution takes into account the emerging importance of blockchain technology that has been developed in recent years. They have addressed also potential obstacles, and legal, organizational and technical issues.

Authors in their paper [18] have conducted a detailed study by analysing the adaption of blockchain technology and its implementations by various governments around the globe and additionally they have analysed the evolution of e-government based on empirical evidence from a Dubai government entity which has used blockchain technology to offer end-user services. They have analysed and addressed the challenges of using blockchain in government for public services as well.

3. Proposed solution

We propose to use blockchain technology to implement a system to manage real estate properties and to avoid all actual system drawbacks in Cadaster of North Macedonia. Therefore, in this work, a blockchain-based framework is proposed to develop a land administration system, which will be implemented and simulated in Ethereum blockchain platform and will contribute to developing a secure, reliable, scalable, effective and efficient system.

In a LAS can be stored two important kinds of information. The first is referred to as legal data, which presents ownership data and other rights of that real property. And the second is referred to spatial data, which presents real property's data about position and shape. Thus, in North Macedonia, we have two main records of a real property, which is Land register and Cadaster. Land register provides answers to questions about who an owner of certain property is and on what legal document is that right based on. Cadaster provides answer to questions regarding location of certain property, property addresses, and land use, nature and duration of tenure, details about construction buildings, population, and land taxation value.

The activities which should be considered in adapting blockchain technology in real property management are as follows: (1) What kind of implementation should be used? Public, private or hybrid approach [19] is better to fulfill all the necessary requirements of management of user identity and record the transactions?; (2) Design the system architecture; (3) Implementation and development of smart contract; (4) Testing and evaluations; (5) Analyze business potential of such a prototype.

In this paper we will be focused mostly in the first two tasks. The main function, the system should perform are: (1) to offer the possibility to save and update the real property data information; (2) to offer the possibility to the buyer to check for the interested real property related information; (3) to initiate the real property's ownership transfer process; (4) to add the transaction of 'ownership transfer process' to the blockchain network.

3.1 What we propose

The solution we propose is a collection of services deployed in different production environments. Ethereum EVM will be used to deploy and execute a smart contract, which is simply a program or set of instructions written in "Solidity" and executed on the blockchain. Smart contracts are used as a type of automation on blockchain based on predefined conditions. On top of that, an Interplanetary File System (IPFS) network [20] will be used to store large files, such as photos of a property scanned documents or aerial images.

In order to connect and interact with those networks, a set of interfaces have been developed. The interfaces are developed in HTML/CSS/JavaScript using modern frameworks such as ReactJS and libraries such as Web3JS, crypt-js and IPFS-client. These interfaces have been split in two parts by having separate interfaces for issuing certificates to the blockchain and another interface for verifying and getting certificates from the blockchain and IPFS network. The first interface will be used by the cadaster, whereas the other one by the buyers/owners of a property in order to verify ownership of a property.

3.2 The architecture of the system we propose

The architecture of the system we propose is presented in Fig. 1. As the figure shows, firstly the cadastre deploys an encrypted certificate that can only be decrypted by using the encryption key. The key is used to encrypt both blockchain and IPFS data, thus rendering them useless without the encryption key and making the system more secure. The encryption key then is communicated to the owner of the property, who then can use this key in order to view his certificate.

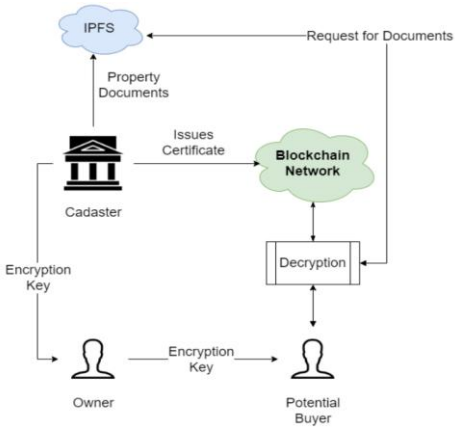


Figure 1. *The Overall Architecture of the System*

Alternatively, the cadaster stores this key in their private serves, in case the owner loses the key. Afterward, the owner can send this encryption key to a potential buyer (this is done by using a QR code, where the buyer will not be able to copy and get hold of the

encryption key) and then the buyer can verify the ownership of the property. Otherwise, the owner can use the interface on his own and show the result to the buyer.

3.3 Role Configuration

The proposed solution consists of roles. We will be creating a role-based system, where the main identifier will be the blockchain address. Roles are as follows: The ministry or the highest institution to this project (government entity) will allow other entities (such as cadaster) to issue certificates. This entity also has permission to issue certificates itself. After being given permission, Cadasters will be able to issue certificates on their own. If a certificate is issued twice, its data will be retained as an older version, and the new data will be displayed to the user, thus pushing the old data further into the history changes.

When issuing a smart contract, we need to fill in a parameter called "master address". This address will be used to issue other addresses that in turn will issue certificates. This address will be owned by the main entity that owns the network. Another address would be the ROOT address, which will be used to issue the smart contract. After the deployment of the smart contract, the private key of this address will be encrypted, fragmented and stored as safely as possible. This is done because this address will be later used as a failsafe in case the master address is compromised or stolen. Being the highest address on the "hierarchical" system, it is suggested to be stored offline, encrypted and in a place hard to be accessed. Ain storage techniques include storage in a local server, offline on a USB< disc CD/DVD, paper or using services used to store classified data. The next address will belong to the issuer, and this address will be used a lot of time. This because it will be used to issue and modify certificates. For ease of use, this address will be identified by name and institution ID.

3.4 Certificate Verification

Firstly, the issuing entity issues a certificate using its address, signing it using its private key, after which this certificate is added to the network pending verification and included in a block. In case it is accepted by the network, it is checked against the smart contract, where it is checked if it fulfils all the requirements and if the issuer is valid and authorized. If everything goes as expected, it is added to the network according to the smart contract instructions, and the certificate is added to the network. Otherwise, the transaction remains verified, but the storage of this certificate to verified certificates is blocked. This means that the operation has been canceled and this certificate cannot be used. In both cases, a fee is paid to the network, so we should make sure to use an authorized address.

Due to the costs and size limits that we have in a transaction, we will need to minimize the length of data sent to the blockchain network. This will be done by offloading some data such as photos, videos, and documents on other networks, be it IPFS of a private server, where in both cases we would store the hash of this file in blockchain (unique value for each file/document), making it possible to verify the integrity of the file requested in the certificate. We should mention that every piece of information will be encrypted, and it will be impossible to view it without the encryption key. Only transaction data and block numbers will be visible. This is done in order to protect the privacy of users.

4. Interfaces

In this solution we propose two interfaces will be deployed. The interfaces will be used in order to communicate with the blockchain network. They should be easy to use because their target audience will be the common users and the public.

4.1 Verifier Interface

Verifier will make it possible to verify a certificate on the system. As input, we will need the ID of the certificate. Fig. 2 presents the flow of information from the verifier to the network.

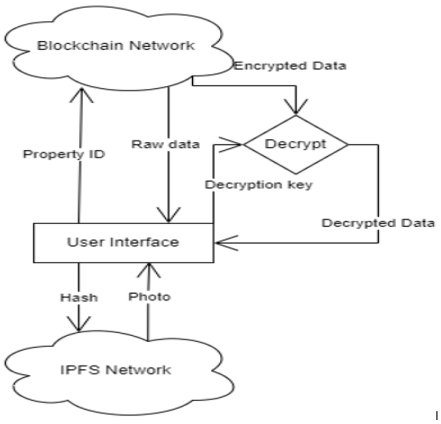


Figure 2. *Flow of information from verifier to the network*

At first basic public information will be shown, such as the type of real estate, area or description, address or location. In case these properties are enough the third party won't need a decryption key. Otherwise, the owner authorizes decryption using its decryption key. In this case private details are shown such as: Owner, Co-owners, Cadastral Zone / Coordinates, price etc. Should be noted that this information will be in accordance with the current state of North Macedonia laws. After retrieving data from blockchain, we can connect immediately to the IPFS network and retrieve its images.

4.2 Issuer Interface

This part of the software will be used by the issuing institution. In this interface, the certificate will be issued and sent to the network. After the certificate has been issued, the institution is responsible for sending the encryption key to the owner.

Initially, the user fills all the fields with the information of the ownership certificate that is required. After that, some of these fields are encrypted using the specified encryption key specified by the user or randomly generated, as it is shown in Fig. 3.

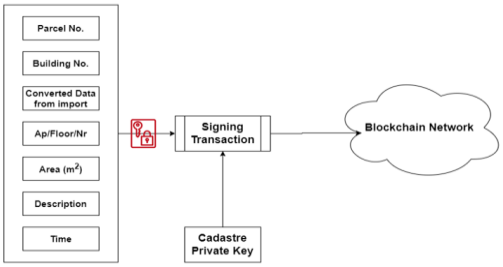


Figure 3. *The flow of information from the verifier to the network*

Once filled in, the transaction is initiated using the private key, and once confirmed it is added to the blockchain. Should be noted that this information is encrypted.

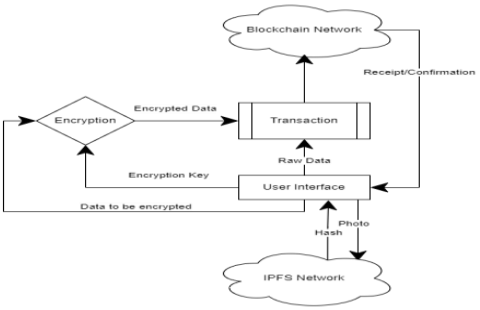


Figure 4. *The flow of information from issuer to respective network*

Along with the rest of the data, a transaction is created. The transaction takes one parameter, which is the address encryption key that will be used to issue the certificate. Once the certificate has been issued the user needs to wait for the transaction receipt. This transaction contains data such as transaction address, gas used,

included block, etc. Unlike the previous case, we first connect to the IPFS, upload images, and then take their hashes. These hashes are included as part of the transaction.

5. Conclusion

In Blockchain technology as a new decentralized peer-to-peer infrastructure supports openness, transparency, accountability, identity management and trust. It has received extensive attention recently and it is applied in many fields. We believe that using blockchain technology in public administration will make a more efficient administration. The trust, transparency, and accessibility of services to the citizens will be increased by using this technology. By safely improving and automating processes in compliance with privacy and confidentiality regulations, blockchain-based solutions will strengthen the bond between citizens and the government.

In this paper we proposed to use blockchain as a mechanism to be used in public administration in the Land Administration System (LAS) ***to manage real estate properties***, in order to improve efficiency and security and to address problems like: tracking usage of Real Property, corruptions of certificates, ownership rights. This system is based on Ethereum EVM, where the main execution will take place, where the smart contract will be deployed and where the main dataset will be stored. IPFS will be used to store files such as photos or scanned documents and will be attached to the certificate in the blockchain. The system we propose aims to enable much more sophisticated systems for issuing and verifying certificates of real estate property entirely on blockchain. This includes the issuance of several certificates as per state guidelines, and verification from other third parties using decryption keys. The user is required to specify only two fields, property ID and decryption key. These services can be accessed from every device that has been connected to the internet. In each case, we can deploy the project to a private or public blockchain. We have considered that the actual implementation should not be too complex compared to the actual implementations, as well as match the costs of maintenance as closely as possible.

As future work, first we will be focused on Blockchain development and smart contract deployment. Additionally, we will work on (1) technical changes, such as IPFS orchestration, increasing the number of key distribution methods, tweaking the environment based on PoC results, lower resource usage, dockerization, 1-click node deployment as well as on (2) quality-of-life improvements, such as QR code integration, customization panel, offering printable (hard copy) certificate, better UI/UX.

REFERENCES

[1] Petrov D. *et al.* The Impact of Blockchain and Distributed Ledger Technology on Financial Services. International Scientific Journal "Industry 4.0", Vol IV, Issue 2, pp. 88-91, 201, Web ISSN 2534-997X, Print ISSN: 2534-8582.

[2] Mechkaroska D., Popovska-Mitrovikj A., Dimitrova V. Secure Big Data and IoT With Implementation of Blockchain. In International Scientific Journal "Security $ Future", Vol. II, Issue 4, pp. 183-185, 2018, Web ISSN: 2535-082X, Print ISSN: 2535-0668.

[3] Wani, Sh., Imthiyas, M., Almohamedh, H., Alhamed, K.M., Almotairi, S., Gulzar, S. Distributed Denial of Service (DDoS) Mitigation Using Blockchain – A Comprehensive Insight. *Symmetry*, pp. 227, Vol. 13, No. 2, 1st January 2021, DOI: 10.3390/sym13020227, Published by MDPI.

[4] Pereira, S. N., Tasnim, N., Rizon, R. S., Islam, M.N. Blockchain-Based Digital Record-Keeping in Land Administration System. In *Proceedings of International Joint Conference on Advances in Computational Intelligence*, May 2021, Online ISBN: 978-981-16-0586-4, Print ISBN: 978-981-16-0585-7, pp. 431-443, DOI: 10.1007/978-981-16-0586-4_35, Published by Springer, Singapore.

[5] Ameyaw, P.D., Vries, W.T. Transparency of Land Administration and the Role of Blockchain Technology, a Four-Dimensional Framework Analysis from the Ghanaian Land Perspective. *Land 2020*, 491, DOI: 10.3390/land9120491, Published by MDPI, Available: https://www.mdpi.com/2073-445X/9/12/491.

[6] Aliti, A., Leka, E., Luma, A., Apostolova, M. A Systematic Literature Review on Using Blockchain Technology in Public Administration. In *Proceedings of 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022, Opatija, Croatia, Published by IEEE, DOI: 10.23919/MIPRO55190.2022.9803797.

[7] Ferdous, M.S, Chowdhury, M.J.M., Hoque M.A, Colman, A. Blockchain Consensus Algorithms: A Survey. *arXiv:2001.07091v2* [cs.DC], February 2020, DOI: 10.48550/arXiv.2001.07091, Available: https://arxiv.org/pdf/2001.07091.

[8] Nguyen, G.T, Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems (JIPS)*, Vol. 14, No. 1, pp. 101-128, February 2018, Print ISSN 1976-913X, Online ISSN: 2092-805X, DOI:10.3745/JIPS.01.0024.

[9] Matzut, R., Pennekamp, J., Buchholz, E., Wehrle, K. Utilizing Public Blockchain for the Sybil-Resistant Bootstrapping of Distributed Anonymity Services. In *Proceedings of the 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS '20)*, May 2022, Taipei, Taiwan. Published by ACM, New York, USA, DOI: 10.1145/3320269.3384729.

[10] Zhou, H. Fard, A. M., Makanju, A. The State of Ethereum Smart Contracts Security: vulnerabilities, Countermeasures, and Tool Support. *Journal of Cybersecurity and Privacy 2022*, ISSN: 264-800X, 2, pp. 358-378, Published by MDPI, DOI: 10.3390/jcp2020019.

[11] Norvill, R., Pontiveros, B.B.F., State, R., Cullen, A.J. Visual emulation for Ethereum's Virtual Machine. In *Proceedings of Conference: NOMS 2018 – 2018 IEEE/IFIP Network Operation and Management Symposium*, pp. 1-4, DOI: 10.1109/NOMS.2018.8406332.

[12] McMurren, J., Young, A., Verhulst, S. *Addressing Transaction Costs Through Bockcchain and Identity in Swedish Land Transfers*. October 2018, Available at: https://blockchan.ge/blockchange-land-registry.pdf.

[13] Shang, Q., Price, A. A Blockchain-Based Land Titling Project in The Republic of Georgia, Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations*: Technology, Governance, Globalization 2019, , Vol. 12, Issue 3-5, pp. 72-78, Online ISSN: 1558-2485, Print ISSN: 1558-2477 DOI: 10.1162/inov_a_00276.

[14] Sladic, G., Milosavljevic, B., Nikolic, S, Sladic, D., Radulovic, A. Blockcahain Solution for Securing Real Property Transaction: A Case Study for Serbia. *ISPR International Jourrnal of Geo-Information* 2021, 10, 35, DOI: 10.3390/ijgi10010035, Published by MDPI.

[15] Torun, A. Hierarchical Blockchain Architecture for a Relaxed Hegemony on Cadastre Data Management and Update: A Case Study for Turkey. In *Proceedings of UCTEA International Geographical Information Systems Congress 2017*, 15-18 November 2017, Adana, Turkey.

[16] Stefanovic, M., Przulj, D., Ristic S., Stefanovic, D. Blockchain and Land Administration: Possible Applications and Limitation. In *Proceedings of the 5th International Scientific Conference on Contemporary Issues in Economics, Business and Management (EBM 2018)*, Kragujevac, Republic of Serbia, 9-10th November 2018, Published by IEEE.

[17] Muller, H., Seifert, M. Blockchain, a Feasible for Land Administration?". In *FIG Working week 2019 Geospatial information for a smarter life and environmental resilience*, Hanoi, Vietnam, April 22-26, 2019, Available at: https://www.fig.net/resources/proceedings/fig_proceedings/fig2019/papers/ts01i/TS01I_seifert_mueller_10110.pdf.

[18] Khan, S., Shael, M., Majdalawieh, M., Nizamuddin, N., Nicho, M. Blockchain for Governments: The Case of Dubai Government. *Sustainability 2022*, 14, 6576, DOI: 10.3390/su14116576.

[19] Desai, H., Kantarcioglu M., Kagal, L. A Hybrid Blockchain Architecture for Privacy-Enabled and Acccountable Auctions. In *2019 IEEE International Conference on Blockchain (Blockcchain)*, 2019, pp. 34-43, Atlanta, USA, DOI: 10.1109/Blockchain.2019.00014.

[20] Nyaletey, E., Parizi, R.M., Zhang, Q., Choo, K.K.R. BlockIPFS – Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability. *2019 IEEE International Conference on Blockchain (Blockchain), 2019*, pp. 18-25, DOI: 10.1109/Blockchain.2019.00012, Published by: IEEE, Online ISBN: 978-1-7281-4693-5, Print ISBN: 978-1-7281-4694-2.

Technological development: Thermal vision as a phenomenon

Pavel Zahradnicek[1*], Jan Hrdinka, Jan Zezula, Ludek Rak
University of defence, Brno, Czech republic[1]
pavel.zahradnicek@unob.cz

Abstract: *The article deals with technological development, especially with thermal imaging. The authors are convinced, that this technology can progressively and qualitative influence operations of security forces and crisis response teams. The article is divided into 3 main parts, where first chapter generally describes thermal imaging, second chapter deals with current applications and last chapter sets the perspectives for future.*
Keywords*: CAPABILITIES, EFECTIVENESS, SECURITY, TECHNOLOGICAL DEVELOPMENT, THERMOVISION.*

1. Introduction

Technological trends [1] disruptively influence not only security environment, but also all PMESII [2] areas. New technologies, instruments and procedures have impact on capabilities development and creating of strategies [3]. These strategies are constructed by instruments with their specific characteristics, units and various procedures, influenced by leaders.

One of the phenomenon of nowadays is thermal vision. This kind of technology is not so new and disruptive as itself, but trend of miniaturization push this technology as overall useful and comfortable for single operator. Wide scale of thermal vision applications from low quality devices to very advanced and miniaturized devices offers opportunity to apply this technology.

Thermal vision is based on visualization of difference between temperature of object and surroundings [4]. Generally, it is possible to divide thermal vision into following categories:

- Personal cameras and mobile cameras;
- cameras for recognition and thermal scopes;
- Single thermal cameras and integrated cameras in fused system.

The topic of effectivity from user perspective was several times explored. Simple comparisons, for example [5], favors thermal visions, rather than pure daily optics, daily camera or night vision in worsened conditions. Darkness, fog, snow etc. sets a barrier between target and observer, leveraging using thermal vision. Therefore, based not only on scientific, but firstly on empiric basis is strongly recommended combination of devices, what allows orientation in area.

2. Application in field of security

Security and rescue forces use thermal vision as a fitting asset of response teams.

Police teams by searching areas and objects are identifying lost and hidden individuals and groups. There is visible also fresh body liquids (esp. blood) on the ground and is possible to track escaping individuals.

Fire fighters identify not-visible centers of fire, identify location of victims of fires and also hidden people. Planning and conducting of firefighter's intervention is more precise and safe.

Medical urgent teams, working in worsened (war) conditions are having the possibility to improvingly identify changes of temperatures and abnormalities in tissues.

The army application is the core topic of this article. Thermal vision systems are installed as sensor part of fixed wings, rotary wings and vehicles. Especially in aircraft are combined with other technologies and the introduced output for operator is integrated picture, which is not visible by separate technologies. ISR units and Special Forces are equipped by reconnaissance and target acquisition devices, using also thermal vision. Not so often are equipped by personal scopes and googles. The combination with other systems allows not integrated picture of surroundings, but by operator distinguished outputs, what can stand for specifics, object or enemies. This advantage sets for protective measures, as anti-thermal vision camouflage [6, 7], what is new trend in field of warfighting function protection. Basically every type of sensor can be thermal and the picture can be transferred into monitoring system as example can be mentioned engineer robots or unmanned aerial vehicles.

Current Ukrainian conflict turned up the impact of thermal vision as a component of maneuvering units. Despite the fact, that these applications were commercial and sometimes low-cost, the tactical advantage was on side of forces using thermal vision. Small local battles of infantry units during night time favorited Ukrainian units, operating with personal thermal vision, night vision and drones with thermal vision. Especially in forests and urban areas was because of technological advantage recognized and impacted an enemy. Clashes between sniping units are also influenced by thermal vision. In fact, who shows body part - does not matter on size, is identified, can be hidden. Impact of using of technology, based on conflict lessons learned, is not only quantitative, but also has strong impact on morale, what is also part of combat potential influencing ratio of strength.

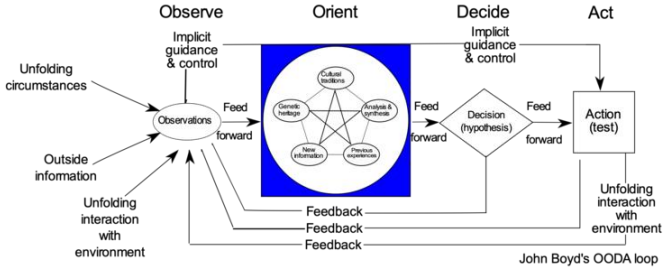
Thermal vision supports military capabilities development and mostly at these of main capabilities areas [8]: Project, Engage, Protect, and Inform.

3. Perspective from operational viewpoint

The miniaturization continues and it is only problem technical development and of time, when will be fusion of technologies integrated onto level of individual soldier. The usage will be wider and more common. Integrated sensors will be part of unmanned systems, sensors and individual soldiers, depending on their needs, for example googles and scopes.

In relation to autonomy, there exists future capacity to link fusion of sensory technologies and algorithms, what enable construction of very precise view of situation and effective support of common operational picture. Adding relation to signal and connection, the picture can be distributed to necessary entities, esp. commanders. This leverage Boyd´s OODA loop at all levels of command and control [9, 10].

Picture1: *Boyd´s OODA loop*



Source: The OODA Loop and the Half-Beat

4. Way outs for applied research

In Czech army, there is not breaded thermal imaging in structure of manoeuvre units (meaning combat units of army, not reconnaissance or SF/SOF). The authors are convinced, that this kind of technology can, in case of correct amount and training, influence combat effectiveness of manoeuvre units. For this reasons they prepared set of experiments, answering following questions, correlating on low-tactical level:

- How can thermal vision influence deployment of combat units?
- Which tactical activities are proper to support with thermal imaging and why?
- How will increase combat potential and capability to engage?
- How are the principles of using thermal vision and how to protect against enemy using this technology?

Firstly data we measured and evaluated, using imager InfiRay Eye II E6Pro V3 for short distances. During the data measuring were focused results and also approach of trainees. Firstly dataset of results is following:

- Up to 200 m is possibility to detect, recognise and identify all details of person. Is possible to recognise basic sign of friend or foe.
- For detection, it is possible to use it for opened area observation up to 1000 m.
- Commercial application are also for applying for infantry units.
- In tree lines and bushes, there is not capacity to recognise man (soldier) and animal. So the imager only "warns", that in area finds something.
- The eyes of observer can be defocused, in combat environment it can cause inability to shoot, for decades of seconds.
- From individual perspective, creates overview esp., during night, conducting reconnaissance and defence activities (mostly static). Knowledge of surrounding, makes soldier more informed and oriented, capable to decide for appropriate action.
- The light from rear lens is visible in night vision. It is important to equip imager for military use by automatic switch off when drawing from eye.

Next measurement will be focused on dynamic tactical activities and also using ARCHER TBX 8 on middle and longer distances. Using live simulators (SAAB) will be measured difference of effectiveness of units equipped and not-equipped by thermal vision.

All the hard data will be transformed to constructive simulator Masa Sword and compared from perspective of capabilities on battalion level, what can generate change of combat potential.

5. Conclusion

Thermal vision can influence results of battle in all phases of OODA, based on empirical knowledge, current subjective experience from operations and also primarily results from measurements. Manoeuvre units worldwide, are underestimated by equipping with this kind of materiel, which can be crucial for fulfilling the task and surviving on the battlefield.

References

1. STO. Science & Technology Trends 2020-2040: Exploring the S&T Edge. In: Www.nato.int [online]. Brussels, 2020 [cit. 2022-09-10]. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdfA. Mecke, I. Lee, J.R. Baker jr., M.M. Banaszak Holl, B.G. Orr, Eur. Phys. J. E 14, 7 (2004)
2. STOJAR, Richard. Bezpečnostní prostředí: sektorová analýza a implikace pro ozbrojené síly ČR 2021. Brno: Univerzita obrany, 2022. ISBN 978-80-7582-459-2.
3. PROCHÁZKA, Josef a Pavel NEČAS. Přístupy k tvorbě bezpečnostních a obranných strategií. Banská Bystrica: Univerzita Mateja Bela v Banskej Bystrici, Fakulta politických vied a medzinárodných vzťahov, 2020. Fakulta politických vied a medzinárodných vzťahov. ISBN 978-80-557-1656-5.
4. BALÁŽ, Teodor, VU, Duc Hieu. INFRARED SIMULATION OF STATIC PERFORMANCE OF THERMAL CAMERA SYSTEM. In: 22nd International Scientific Conference ARMAMENT AND TECHNICS OF LAND FORCES 2016. Liptovský Mikuláš, SR: Academy of the Armed forces of Gen. M. R. Štefánik, Liptovský Mikuláš, 2016, s. 193-201. ISBN 978-80-8040-537-3.
5. MORAVEC, Tomáš. Historie a současnost prostředků pro pozorování za ztížených podmínek a jejich využití u bezpečnostních složek. Praha, 2022. Bakalářská práce. AMBIS.
6. NATO STO. About the NATO Science and Technology Organization (STO). Sto.nato.int [online]. 2022, 2022 [cit. 2022-09-10]. Dostupné z: https://www.sto.nato.int/Pages/default.aspx
7. RACEK, František, BALÁŽ, Teodor, KREJČÍ, Jaroslav, JOBÁNEK, Adam. Evaluation of validity of observer test for testing of camouflage patterns. In: Target and Background Signatures IV. Bellingham, Washington, USA: Society of Photo-Optical Instrumentation Engineers (SPIE), 2018. ISSN 0277-786X. ISBN 978-1-5106-2172-5. doi:10.1117/12.2325101
8. THE LONG TERM PERSPECTIVE FOR DEFENCE 2035. In: Army.cz [online]. Prague, 2019 [cit. 2022-10-25]. Dostupné z: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/dv-2035-aj.pdf
9. BOYD, Cameron, Robert COLLIER, Daniel SKINNER, et al. Characterisation of Combat Identification Technologies. https://shoalgroup.com/wp-content/uploads/2017/06/Boyd-et-al-2005-Characterisation-of-Combat-Identification-Technologies-IEEE-2005.pdf, 2005.
10. The OODA Loop and the Half-Beat. In: Thestrategybridge.org [online]. 2020 [cit. 2022-10-26]. Dostupné z: https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat

Principle of Operation and Advantages of a Sensor for Fog Contamination Detection

Ognyan Ivanov[1,2,*], Petar Todorov[1,2], José Luis Pérez-Díaz[3], Tihomir Tiankov[1]
Institute of Mechanics, Bulgarian Academy of Sciences, Block 4, Acad. G. Bonchev St., Sofia -1113, Bulgaria[1]
Georgi Nadjakov Institute of Solid State Physics, Bulgarian Academy of Sciences, 72 Tzarigradsko Chaussee Blvd., 1784 Sofia, Bulgaria[2]
Escuela Politécnica Superior, Universidad de Alcalá, 28805 Alcalá de Henares, Madrid, Spain[3]
ogi124@yahoo.com

Abstract: *During out work in a project related to European security, we have created various devices. One of them is a sensor for control of contaminations in the composition of fogs, which is first of its kind in the world. The development of such a sensor is important because in this project, artificially generated fogs with special additives are used for decontamination, and it is crucial to control the quantity of impurities in these fogs. In this work, different aspects of the operation of this sensor, its advantages and design considerations are discussed.*
Keywords*: FOG, SENSOR, ELECTROMAGNETIC ECHO EFFECT, SECURITY*

1. Introduction

The project "Device for Large Scale Fog Decontamination" with acronym COUNTERFOG is a project funded by the European Commission under the FP7-Security Programme. Its main purpose is to build systems for quick and efficient counteraction against contaminations of the atmosphere of various nature. These can be any sort of dispersed CBRN (chemical, biological, radiological, nuclear) agents, that is why fog spraying was chosen as the decontamination method. Fog has the ability to collect any particles from the air and collapse them to the ground, thus minimizing the harmful impact on humans that may be present in the contaminated area. In order to control the presence of pollutants, both in the atmosphere and in the decontaminating fog, respectively the systems for decontamination, our team has created numerous devices for control of the presence of harmful substances [1]. One of them is a sensor with a liquid layer operating on the basis of the electromagnetic echo effect (EMEE). The former name of the effect is the "surface photo-charge effect" (SPCE) [2]. The method is contactless and quite fast, provides real-time analysis, and can be considered universal [3-5]. The EMEE generates signals that are highly sensitive even to imperceptible changes in the composition and properties of the object under study- gas, liquid, or solid. Some information about this sensor has already been published [6]. Here we will give more details about the principle of operation of the sensor, ways to optimize its performance and its main advantages.

2. Principle of operation of the sensor with a liquid layer

The EMEE sensor for detection of contaminations in the composition of fogs needs to have a layer of liquid inside of it. The liquid is of the same origin as the one used for generation of the decontamination fog (Fig. 1).

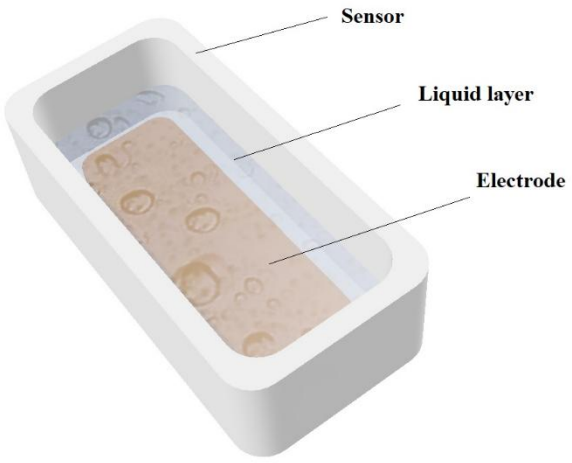


Fig. 1 *Schematic representation of the sensor for detection of contaminants in fog.*

When the fog droplets are in contact with the liquid layer, the EMEE signal is generated in the solid-liquid interface (between the electrode and the liquid). The signal does is not influenced by the main compound of the fog. However, when impurities are added, there will be a deviation in the amplitude of the signal.

The principle of operation of such a sensing structure and the measurement setup are shown in Fig. 2. The liquid is stored in a tank and fed by micro pumps (7) to the sensor (1), which is sprayed with fog by the fog generator (6). A power supply (3) powers a laser (2) and the beam is modulated by a frequency generator (4), which also feeds a reference signal to a lock-in nanovoltmeter (5) that measures the signal. The ready state of the sensing element is determined when a signal without liquid is received. On alert, a controlled filling of the sensor begins until the steady level is reached. After the liquid is present, the sensor is operational. The signal generated from uncontaminated fog is known. If a different signal is received, then the difference with the reference signal ΔV will inform us about the presence and the increase of any dangerous compound in the fog.

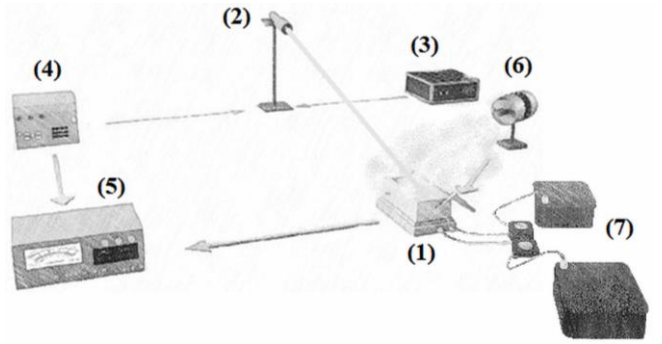


Fig. 2 *Measurement setup of fog contaminations by an EMEE sensor with a liquid layer.*

It has to be kept in mind that exact values about the increase/decrease of a certain compound in the vicinity of the sensing element can be obtained only for materials for which we have calibrated the system. Without calibration, we cannot know the increase of a random contaminant in absolute values. Yet, for our purposes, this is not so necessary. We can also work with relative values. The reasons for that are the following:

- In the initial hours (which are most essential for decontamination) the material of the attack can be unknown. And still, the neutralizing system has to react immediately. We cannot wait for the determination of the attacking agent.
- The purpose of the decontamination is the removal of the contaminating agent. Conducted experiments so far show that the sensor will react to it. It can be traced when the EMEE signal amplitude reaches its maximum deviation point from the initial condition, when there was no agent present. This way we can know when peak contamination

level is reached. Also by comparison, we can check when the signal returns to its initial state – without contaminant, which is actually the most valuable information for us. Between the two states, we will be able to make a relative assessment of the level of contamination. Even if we have calibrated the system and we measure the contamination in absolute values, the obtained results will also have relative accuracy. The reason is that fog is a dynamic constantly changing entity in every region of its volume. What we have measured at time t_1 for a given point, most certainly will not be the same at moment t_2 (for example, after a minute has passed).

It has to be noted that after each measurement, the liquid will be contaminated and it will have to be replaced. This means that the sensing element will have to be flushed with liquid from the tank by miniature pumps. There are be two exactly defined open-valve times for liquid flow – for flushing and filling of the sensor. The sensor is connected to a second tank for waste liquid. The operational sequence is the following: we pump liquid in and make a measurement. When the measurement is over, we flush with clean liquid. Next, the sequence is repeated – we load the sensor, measure and flush. And so on repeatedly. For better accuracy, we can control the liquid volume while measuring. The amount of liquid is about 5-10 millilitres.

We must note that the longer we wait, the more the signal from the sensor will increase. The admixture in the fog might decline, but in the liquid layer, it will be accumulated and the signal will grow. This is why, for example, we measure for 2 minutes, wash with clean liquid, load with fresh one, and measure for 2 minutes again, clean again and so on. In such a case, we will have a current measurement every 3 minutes (it takes about 1 minute to flush and fill). The period of this cycle has to be kept constant in order to avoid the error coming from admixture accumulation in the liquid.

Under real circumstances, we won't be able to calibrate the system for all types of contaminants. We will measure in relative values and we will monitor for the peak level of the harmful mixture. Next, we will monitor for its disappearance, at which point the signal will be zero (sensor reading will be zero, because only clean fog will have remained, which does not generate a signal). This will mean that the decontamination has finished. With the repetitive cycles of cleaning and filling, we will also solve the problem of raising the level of the liquid due to precipitation of fog in liquid form over the sensing element. A change in the level of the liquid can result in a measurement error.

We should also point out that when having a structure with a liquid layer, a better sensitivity is expected in contrast to a direct interaction fog–solid body. This is due to the fact that for the fog–solid interaction, the main signal comes from the predominant matter in the fog, based on which we have to capture small changes coming from the admixtures. In this case, we have the fog on one hand, generating a signal V_1, and an impurity on the other, creating another signal V_2. Since the quantity of the fog is much higher, in the general case V_1 will also be much stronger than V_2. The two signals will be combined. It is not easy to separate those signals since the fog changes constantly. Using the structure with a liquid layer, the predominant substance of the fog will not create a signal. Then V_1 will be zero and we will measure only V_2. Still, we have to keep in mind that with the liquid layer structure, the substance we are looking for is dissolving in the liquid and this may affect sensitivity.

The usage of a thin layer of liquid from the same kind as the one used for fog generation has different advantages. In this case, the sensing element does not react to the predominant fog compound. It only reacts to admixtures. Since the admixture is also present in the fog, we will still have fluctuations. The inconsistent volume of fog interacting with the sensor will also mean inconsistent amount of impurity interacting with the active surface of the sensor. Those fluctuations are averaged by the liquid layer for a period we define. This way the problem is solved to a satisfying extent.

If we use a structure with direct solid–fog contact, we will have to create a mechanism to prevent the condensation. In this case, we will probably also reject the admixtures absorbed in the fog to some extent, which will reduce the sensitivity.

3. Main advantages of a structure with a liquid layer

The main advantages of a structure with a liquid layer over the interface include:

- The problem with condensation on the sensor surface, which obstructs the measurements, is solved.
- The problem with surface pollution is solved, which is also an impediment to measurements.
- The sensitivity is increased by zeroing the signal from the predominant fog compound. It is taken into account that if the sensor is sensitive to the main composite of the fog, in the general case this compound will generate a much stronger signal. This is so because it is contained in greater amounts and on the base of that strong signal we will have to capture very small changes generated by the admixture.
- More realistic measurements can be taken. The density of fog varies constantly. The signal will be different depending on the quantity of fog that has interacted with the surface. We cannot be sure if the alteration of the signal is due to change in the mixture percentage or density of the fog. The liquid layer eliminates the influence of the main fog compound, so that only the impurity formed in the mist can influence the results. Naturally, if the density of the fog changes, the density of the impurity will also change. However, this is compensated greatly by the averaging, which the liquid provides.

A minor inconvenience is that during the measurements the sensor needs to be periodically filled in and out with small liquid volumes but this can easily be achieved by incorporating micro pumps in the setup.

4. Conclusion

In terms of the realization of the sensor, different structures have been developed and tested. Our aim is to create a stand-alone device, which can work automatically. The active surface should be integrated into a small vessel with an appropriate inclination where the contact with the liquid should be established. This vessel should be in a metal shield for protection against electromagnetic interferences because the generated EMEE signals are too weak. A balance needs to be found between requirements for electromagnetic shielding and the necessity for maximized sensor contact with the fog. Different technical requirements have to be followed. The protective shielding should have a cover that opens automatically. The working structure, the pumps, the laser module, the tanks and the electronic devices should all be placed in a suitable manner as one whole assembly.

Acknowledgements

This work has been funded by FP7-SEC-2012-1 program of the EU Commission under grant number 312804 and the Grant No BG05M2OP001-1.002-0011-C02 financed by the Science and Education for Smart Growth Operational Program, and co-financed by the European Union through the European structural and Investment funds.

References

[1] O. Ivanov, K. Simeonov, P. Todorov, Z. Stoyanov, D. Antonova, K. Kostadinov, Registration approach of viruses by using the electromagnetic echo effect, *2021 IEEE International Conference on Manipulation, Manufacturing and Measurement on the Nanoscale (3M-NANO)*, 2021, doi:10.1109/3M-NANO49087.2021.9599760.

[2] O. Ivanov, P. Todorov, I. Gultepe, Investigations on the Influence of Chemical Compounds on Fog Microphysical Parameters. Atmosphere, 11, 3, 2020, 225.

[3] O. Ivanov, Sensor applications of field-matter interactions, In *Encyclopedia of Sensors*, American Scientific Publishers, C. A. Grimes, E. C. Dickey, M. V. Pishko (editors), 9, 2006, 165-197.

[4] O. Ivanov, M. Kuneva, Quality control methods based on electromagnetic field-matter interactions, *Application and Experience of Quality Control*, O. Ivanov (editor), INTECH, 2011, DOI:10.5772/15857, 509-536.

[5] O. Ivanov, A. Vaseashta, L. Stoichev, Rapid, contactless, and non-destructive testing of chemical composition of samples, *Functionalized Nanoscale Materials, Devices and Systems for Chem.-bio Sensors, Photonics, and Energy Generation and Storage*, Springer, 2008, 331-334.

[6] O. Ivanov, S. Karatodorov, J. L. Pérez Díaz, Novel Electromagnetic Sensor for Contaminations in Fog Based on the Laser-induced Charge Effect, *Proceedings of IEEE SENSORS 2017*, CFP17SE, IEEE, 2017, ISBN: 978-1-5386-4056-2, 1509-1511.