

INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

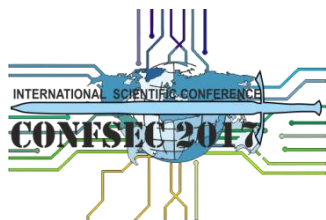
ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

YEAR V, ISSUE 2/2021



**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 / 2021

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 University 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
Vesselin Demirev, Assoc. Prof.	Technical University Sofia	BG
Vladimir Zakhmatov, Prof.	Academy of Ecological Safety, Kiev	UA
Zelimir Kesetovic, Prof.	University of Belgrade	RS

CONTENTS

THEORETICAL FOUNDATIONS OF SECURITY

Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes

Valaeri Panevski 42

NATIONAL AND INTERNATIONAL SECURITY

Contemporary Low Slow and Small (LSS) threat from the air defence view

Zoltan Krajnc1, Erika Vallus 46

Practical approaches for collecting intelligence information

Ilin Savov 49

Examples of nuclear security measures for nuclear facilities

Dimitar Dimitrov 51

Emotional intelligence in small unit's leadership

Vladimir Statev 55

Tactical efficiency in the process of handling and usage of firearms – important security related precondition for carrying out the police duty

Jonce Ivanovski, Aljosa Nedev 58

INFORMATION SECURITY

Steganographic algorithm using the different color components of a 24-bit image

Veselka Stoyanova, Ilian Lilov 61

TECHNICAL FACILITIES FOR ENSURING SECURITY

Means and ways of destruction of explosives and materials

Damyanova Liliya 64

Adaptive methods for detecting passive signal from an underwater object

Nikolay Gueorguiev, Alexandar Kolarov, Ilian. Iliev 67

Non-lethal technologies for forced stopping potentially dangerous vehicles and vessels

Adelina Tumbarska 71

Evaluation of protective action of poisoned gas substances of new generated activated carbon for gas mask application

Liliya Manoilova , Kamelia Ruskova 75

Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes

Valaeri 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
paneovski@ims.bas.bg

Abstract: At its core, business continuity management (BCM) is a process that identifies potential threats to an organization and the impacts on business operations that they could cause if they happen. This process provides a framework for building resilience of the organization and the ability to respond effectively. BCM can help organizations to reduce the negative effects and to protect business reputation under adverse circumstances, whether internal or external, to reduce downtime and recovery costs.

Like continuity, sustainability focuses on maintaining the processes and procedures that help businesses survive unexpected threats. Recognizing that businesses operate in an environment of constant change, sustainability focuses on how best to preserve the value in these complex environments.

But effective BCM process can happen through synergy of administrative and organizational activities (strategies and plans) and operation of flexible, intelligent security systems (ISS). The innovative solutions for the development of the systems are closely related to the requirements formulated in the separate stages of the process of building the BCM of the organization, incl. sustainability, providing warning and prevention of the threats, prevention of terrorist acts and thus ensuring the safety of people and the competitive advantage of business. Understanding the value of connecting different security systems and how they can be integrated is a key component in developing more intelligent security.

The link between risk management and BCM plays a significant role here. Risk management strategies (risk avoidance, risk acceptance or risk mitigation - by risk sharing or risk transfer) are responses to a “preliminary event” of perceived and assessed risks. Most BCM strategies and tactics focus on the processes that must occur after an event or disaster. The goals of these processes are to return the business to normal operation as efficiently and effectively as possible. Namely the relationship between the process of building BCM and ISS development is the subject of this publication.

Keywords: Business Continuity Management, Intelligent Security Systems Development

1. Introduction

The current demands of the world economy have changed things for business. Organizations must now return online as soon as possible after a disaster or risk losing business or reputation. Thus, business continuity management (BCM) is crucial.

But what is BCM in essence? It is a holistic management process that identifies potential threats to an organization and the impacts on business operations that those threats, if implemented, could cause. At the same time, BCM provides a framework for building an effective response that protects the interests of key stakeholders, reputation, brand and value creation activities.

Sustainable business management, including at risk events (natural disasters and man-made crises) is focused on raising awareness; developing a set of strategies and training the members of the organization for roles and responsibilities in crisis.

Businesses need to have plans in place for everything from a hurricane or flood to a bomb threat, an active shooter and an employee strike. Despite the development of different types of probable risk events, the organization needs clear communication channels and management chains to allow the best possible response to the situation in its development [1,2,3,4].

But in order to successfully implement the BCM framework, it is necessary to build, operate and manage an Intelligent Security System [5,6,7,8,9] (as a set of physical protection systems operating in a cybersecurity environment, with a high degree of integration) of the organization and its integration into the overall business management system.

Last but not least, the following restrictions are introduced for the correct presentation of the topic:

- interruptions due to technological reasons are not taken into account, as they are set in advance in the technological documentation of the equipment of the organization;

- the security requirements set by the national operators of the organization are not taken into account, because applying the national and international requirements and standards, in accordance with the specifics of its mission, goals and tasks the relevant elements of the security systems are established and maintained.

2. Business continuity management - framework

2.1 Business continuity management – ISO approach

Various national approaches are known in international theory and practice in the field of business continuity management, but all of them are based on ISO 22301 - Security and resilience - Business continuity management systems - Requirements. In line with and in support of better and correct implementation of BCM, a series of guidelines have been developed, the main ones being as follows

- ISO 22313 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;
- ISO 22316 - Security and resilience — Organizational resilience — Principles and attributes;
- ISO 22317- Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA);
- ISO 22318 - Societal security — Business continuity management systems — Guidelines for supply chain continuity;
- ISO 22330 - Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity;

➤ ISO 22331 - Security and resilience — Business continuity management systems — Guidelines for business continuity strategy.

2.2 Basic key elements of BCM

BCM programs must include a number of key elements to ensure that the organization is well positioned for success and that planning documents are properly developed and regularly updated and improved to lead to success.

The key elements of BCM programs include, but are not limited to:

- **Management:** The structure and the team created for the development and management of the activity.
- **Use of good practices:** The ways in which the current processes of management and planning of the organization's BCM are compared with expert approaches and industry standards.
- **Continuity strategy:** It is a detailed plan that assesses the possible risks to an organization and how it can be recovered if those risks become a reality.
- **Documentation of the plan:** Excerpts from the plan in terms of volume and content to which all participants have access.
- **Tactical execution:** The ways in which the organization plans to recover from certain types of incidents.
- **Training:** The types of staff training for the correct understanding of the Business Continuity Plan and its role in it.
- **Testing:** Creating simulations of a crisis event and testing the reaction of staff in the implementation of the business continuity plan.
- **Maintenance:** Introduce changes to the plan, if necessary, in order to improve its effectiveness.
- **Monitoring:** Comparing the implementation of current standards and expert advice with the way the plan works.

2.3 What are the risks to the business continuity?

Also called business continuity events, business continuity risks are the most common events that can lead to disruption of the organization's business (natural and man-made crises). Identifying these risks is a vital part of business continuity planning, namely: terrible weather; natural disasters (tornadoes, floods, blizzards, earthquakes, fires, etc.); physical security threat; appropriation (theft) of a product of the organization; supply chain problems; threats to staff and employee safety; incidents at the organization's facilities; destruction of equipment or property of the company; power outages; server crashes; failures in public and private services (communications, transport, safety, etc.); environmental disasters, including spills of hazardous materials; network outages; human error / human hazards; stock market crashes; cyberattacks and hacking activity.

Each of these events can lead to major challenges for an organization, such as danger or injury to staff and others, equipment damage, brand injury and loss of income and net worth. Business continuity management and planning address and reduce the impact of these contingencies.

2.4 BCM Lifecycle

Successful BCM helps organizations identify their key products and services and the threats to them. It also helps to quickly restore functionality by helping to protect market share, brand, image and reputation. To be successful, BCM must be seen as an integral part of the ongoing processes of the overall management of the organization. The involvement of senior management is critical to the success of BCM because of its impact on the allocation of resources and the culture of the organization and is essential to the life cycle of BCM.

The BCM life cycle (fig. 1) is a summary of best business practices based on the core requirements of ISO 22301[10]. These practices offer a solid foundation for sustainability while offering the flexibility to adapt to changes in the organization.



Figure 1: BCM lifecycle (based on ISO 22313)

Managed by the leadership of the organization, the key activities for the BCM life cycle can be formulated, as follows:

- Conducting business impact analysis and risk assessment;
- Development of a business continuity strategy;
- Establishment and implementation of business continuity procedures;
- Exercise and test procedures regularly before the risk event occur.

3. Framework for possible integration

3.1 Business impact analysis and Risk Assessment for physical protection systems requirements development

Using formulation in item 8.2.2 “The organization shall use the process for analysing business impacts to determine business continuity priorities and requirements” [10], the organization shall identify the resources and assets for which security building is required and the inclusion as a priority for support.

The planning of the readiness of the organization for each type of event that has been found to have a negative impact on the business is done with the help of *Business impact analysis*. This provides a way to predict how an event will affect business and to formulate risk reduction strategies, including the construction of physical protection systems (peripheral and risk areas). Understanding which assets will be affected, what processes need to change, and what additional security and protection systems need to be built and maintained allows organizations to reduce costs and losses from downtime.

At the same time, in accordance with item 8.2.3 “The organization shall implement and maintain a risk assessment process” [10].

We shall not forget that the organization's risk management is a process that is:

- intrinsic to the economic object (organization);
- carried out by managers at all levels in the organization;
- applied as a first step in determining the development strategy of the organization;

- applied throughout the organization and for each of its levels, including the adoption of a package of opinions on organizational risk;
- designed to identify potential events that, if they occur, will affect the organization, as well as to manage risk within a reasonable propensity to take risky actions;
- able to provide reasonable security to the organization's management.

Last but not least, according to item 8.2.3 Risk assessment [11] to "... select an appropriate method for identifying, analyzing and evaluating risks..." [11], we need to turn to ISO 31000 [12], through which we define the principles for risk management and related work guides.

As a result of the risk assessment and BIA, the management of the organization receives information about the assets, the impact on which the probable risk events may cause business interruption for a longer period and lead to significant losses, including reputation and a long recovery period (if it is possible to recover at all). This is a starting point for building a physical protection system (PPS) (development of the required structure and composition), as an element of the intelligent security system. (fig. 2).

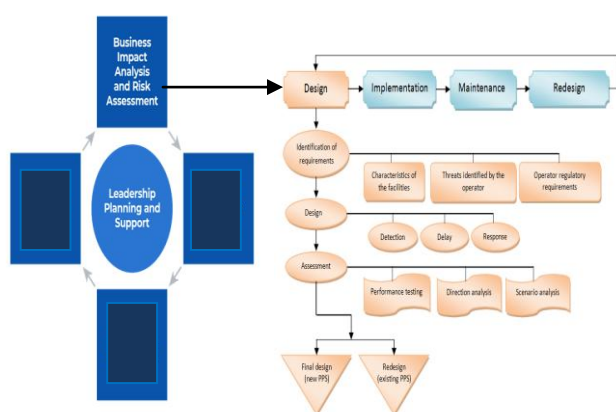


Figure 2: BIA and development of a physical protection system

3.2 Exercise and Test and requirements development for Redesign of PPS

Business continuity exercises are an important and ongoing initiative. The plan should be tested regularly using pre-defined strategies and scenarios. Testing focuses may vary depending on what details, conditions, frequency, business functions, or supporting information processing need to be tested. The testing strategy should include test objectives and related measurement indicators, scenarios, summaries, planning and improvements. It is the emerging need for improvements in business continuity management that will give an input signal to the need and scope of redesigning existing physical security systems and changing the integration scheme in the overall flow of business security management.

Based on appropriate scenarios that are well planned with clearly defined aims and objectives the responsible authorities develop teamwork, competence, confidence and knowledge for those who

have roles to perform in relation to disruptions. As a result post-exercise reports are developed which contain outcomes, recommendations and actions to implement improvements.

Last but not least, in accordance with item 8.5 "The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions" [10] organization should propose changes and improvements, including physical protection systems (fig. 3).

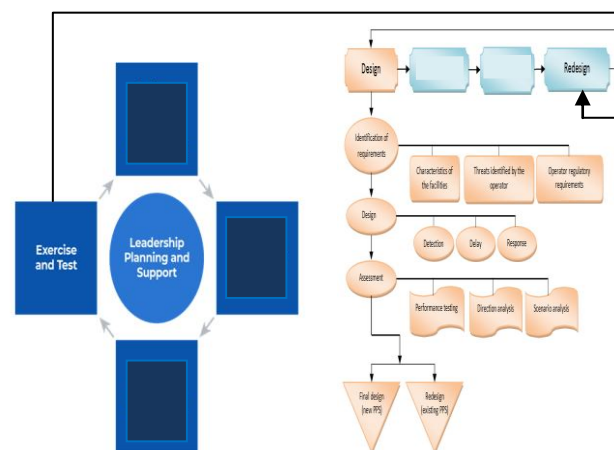


Figure 3: Exercise and Test and redesign of a physical protection system

This is where the link between the key activity "Exercise and Test" of the BCM life cycle and the "Redesign" phase of the PPS life cycle takes place (phase 3).

In Phase 3, an assessment shall be made to determine whether the system meets the requirements for change, namely:

- Confirmation of the functioning of the PPS in accordance with the requirements set in the process of its design and development;
- Identification of possible shortcomings of the system in the design or its implementation, which must be considered in order to provide adequate corrective actions;
- Analysis of possible improvements that may be needed to overcome the deficiencies and improve the functionality of the system;
- Re-evaluate the effectiveness of the PPS on an annual basis to take into account any changes in the objectives, functionalities of the system or the requirements to it.

4. Conclusion

This approach is only an initial step towards developing a proposal for dynamic contact between the business continuity management process and the construction and development of intelligent security systems. Here it is crucial to know and properly apply the standards of the International Organization for Standardization (ISO), the Technical Committee - TC 292 "Security and resilience", as currently 41 pcs. are active. Also, the models of intelligent security systems work together with the elements of the security system of an organization, built in accordance with the requirements of national operators and license holders (according to the specifics of the organization), international and European organizations in the field and not lastly, the technical regulations for the operation of the equipment.

The use of the elements “Business impact analysis and Risk Assessment” and “Exercise and Tes” for requirements for design and redesign development helps to treat the act of threat as a set of risk factors that may affect the assets of the organization, each of which is able to change the security and protection system of elements of the organization. The appropriate technical level of the elements of the physical protection system and their integration into the overall security system of the organization allows precise distribution of functions between management and staff of the organization related to the timely planning of the necessary means to build and develop security in general.

ACKNOWLEDGMENTS

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” (SESG), co-financed by the European Union through the European Structural and Investment Funds.

Literature:

- [1] Dimitrov D. L., “STANDARDIZED APPROACHES TO THE INTEGRATION OF CRITICAL INFRASTRUCTURE MANAGEMENT SYSTEMS”, PROCEEDINGS, SECURITY, VOLUME III., Scientific technical union of mechanical engineering “Industry - 4.0”, 2019, ISSN:ISSN 2535-0315 (Print), ISSN 2535-0323 (Online), p.p. 239-241;
- [2] Dimitar Dimitrov, “COMPERATIVE EVALUATION OF MODELING AND SIMULATION TECHNIQUES FOR INTERDEPENDENT CRITICAL INFRASTRUCTURE”, International Scientific Journal „Security & Future“, Issue 4/2019, Scientific Technical Union of Mechanical Engineering, 2019, ISSN:ISSN: 2535-0668 (print), 2535- 082X (online), p.p. 128-132;
- [3] Pehlivanski V. “Tests in the process of designing protection systems”, monograph 2020, ISBN 978-619-188-359-2;
- [4] Lichkov N., Pehlivanski V., Lyaskov N., Penev N., "Method for simultaneous registration of seismic oscillations registered by several sensors", Sb. reports of the XVIII International Scientific Congress “Machines. Technologies. Materials”, 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, pp. 79-82;
- [5] Gueorgiev N., Boychev Y., Kosev V., “Investigation of seismic oscillations caused by one type of heavy wheel equipment”, Sat. reports of the XVIII International Scientific Congress “Machines. Technologies. Materials”, 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, 27-30;
- [6] Gueorgiev N., Boychev Y., Kosev V., “Investigation of seismic oscillations caused by one type of heavy chain technique”, Sat. reports of the XVIII International Scientific Congress “Machines. Technologies. Materials”, 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, 23-26;
- [7] Litchkov N. G., Boychev Y. D., Kosev V. I., “Analysis of the frequency characteristics of a class of seismic signals”, Proceedings of the International Scientific Conference on Security “CONFSEC 2020”, 4, 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 113-116;
- [8] Nikolay Gueorguiev, Yavor Boichev, Konstantina Belotelova, Ivan Ivanov, “FREQUENCY CHARACTERISTICS OF SEISMIC PIEZOELECTRIC SENSORS UNDER ONE-DIMENSIONAL MECHANICAL ACTION”, Journal of Theoretical and Applied Mechanics, Sofia, Vol.49 (2019), ISSN: 0861-6663 (Print), 1314-8710 (Online) pp. 130-141. Bulgarian

Academy of sciences, National committee of theoretical and applied mechanics, 50, 2, 2020, ISSN: 0861-6663 (Print), 1314-8710 (Online), 130-141. SJR (Scopus):0.28;

- [9] Yavor Boychev, Nikolai Dyulgerov, “Preparation and properties of composites with ultrafine-grained structure”, 2021, ISBN: 978-619-245-100-4, 120;
- [10] ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements;
- [11] ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;
- [12] ISO 31000:2018 - Risk management — Guideline.

Contemporary Low Slow and Small (LSS) threat from the air defence view

Zoltan Krajnc¹, Erika Vallus²
 University of Public Service, Budapest, Hungary¹
 zoltan.krajnc@uni-nke.hu, vallus.erika@mil.hu²

Abstract: This article analyzes the air defense relevance of LSS-type threats. Summaries possible attack scenarios. The air defences have to face new types of challenges in addition to the traditional threat like so-called the LSS (Low Slow and Small) threat by micro, mini drones (including so-called COTS drones) and small UAS systems. The properly heterogeneous sensor and intervention systems need to be integrated if we are to create effective air defences against LSS-type threats. The layered air defence have to can integrate almost all effectors with their sensors and other sensor systems into flexible and effective C2 system.

Keywords: LSS-THREAT, AIR THREAT, DRONES, TRENDS OF AIR DEFENCE CAPABILITIES, CONTEMPORARY CONFLICTS

1. Introduction

According to the Bonus Military Balance 2019 content analysis [1], the west countries (the developed world, including leading NATO member states) neglected the full development of air defences in the post-Cold War decades. The focus of the developments has essentially been focused on two areas: ballistic missile defence (mainly theater missile defence) and the air defences of expeditionary forces. (defence against not a peer or near-peer competitors)

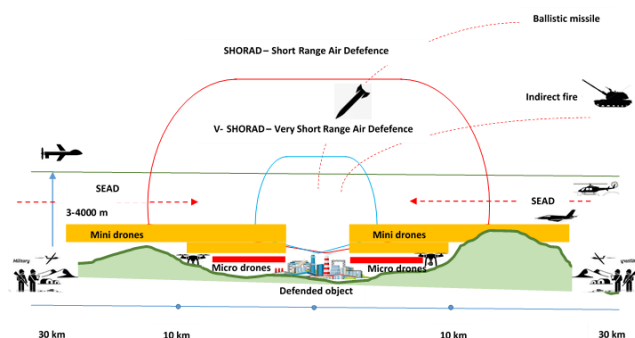


Fig. 1 Scenarios of LSS attack on defended object

Based on the experience of recent years and the analysis of the conflicts of our time, it is easy to see that air defences have to face new types of challenges in addition to the traditional threat. (fixed and rotary-wing platforms, ballistic missiles, cruise missiles, uninhabited aerial vehicles of all classes, precision-guided munitions, rockets, artillery, and mortar rounds as well)

Table 1: Classification by Strategic Concept of Employment for Unmanned Aircraft Systems in NATO (Class I).

	Weight	Operational altitude	Range	Payload
Micro	≤ 2 kg	50-100 m	0.6	≤ 0.5 kg
Mini	≤ 20 kg	1000 m	10-20	≤ 10 kg
Small	weight ≥ 20 kg	1500 m	50 km	≤ 50 kg

What are these challenges again? This has recently been called the LSS (Low Slow and Small) threat by experts and is essentially understood by experts as micro, mini drones (including so-called COTS¹ drones) and small UAS systems. In my article, I am going to summarize the characteristics of this threat and the possibilities for improving air defences.

2. Show the topic, describe the scientific problem

2.1 Typical UAS missions

In recent conflicts and crises, where UAS application has been observed, UAS systems have performed the following combat tasks:

- ISR (Intelligence, Surveillance, and Reconnaissance) missions;

- ISR missions combined with long range fire (artillery support);

- Direct attack (air strike with explosions);

- Swarm direct attack (massive, synchronized air strike with explosions);

The differentiated mission (combat task) of LSS targets depends on your military technical capabilities. Small-category devices are practically identical to pilot-led aerial attack devices. Integrated into COMAO (Composite Air Operations), they are usually designated for a deception, ISR or EW mission. Devices belonged to mini and micro class are typically not used as part of COMAO. Their duties are typically ISR, or attack usually for propaganda and disruptive purposes

2.2 Problems with types LSS-targets

For LSS targets, the difficulty can be perceived in all four segments of active air defence: detection, tracking, identification and intervention (destruction) as well. Very hard to detect and track small UAS in land cutter and with slow speed and hover.

For effective detection have to use heterogeneous types of sensor systems and so-called effectors (hard and soft weapon systems). Planners should take into account the fact that can be also collateral damage to the intervention.

Table 2: Vulnerability of Air Defence Units from different types of drones

	Distance from object	Effector with counter drone capabilities	Sensor
Counter micro (nano) drones	≤ 500 m	There is no effective solutions (small weapons, jammers, etc.)	Electro optical;
Counter mini drone	≤ 2 km	High Power Laser; "Hunter-killer" drone; Gun/Smart munition;	Light tactical radars; Electro optical;
Counter small drone	≤ 5 km	SHORAD missile; High Power Laser; High Power Microwave;	3D tactical radars; Electro optical;

2.3 Short analysis of application of LSS technology in contemporary conflicts

Ukraine

The ongoing conflict in eastern Ukraine is already showing an extensive development in the use of drones in analyzed category, affecting the official Ukrainian armed forces and pro-government non-state (civilian) groups, organizations and separatist forces alike.

¹ COTS - commercial off the shelf

According to military observers and content on a large number of social media and video-sharing sites, the Ukrainian government and pro-government groups use such drones in significantly greater quantities in their crisis management operations than the opposing parties. These sorties mainly consisted of general reconnaissance, surveillance and often artillery adjust firing.

As an interesting fact, we can observe that the Ukrainian government, sensing the limited possibilities and extent of obsolescence of the armed forces' reconnaissance systems, has turned to commercially available non-military drones, similar to the strategy of terrorist organizations. With these initiatives, pro-government forces are attempting to provide Ukrainian security forces with additional information in their fight against the separatists. A major initiative is the People's Project.com Ukraine's military and civilian crowd funding project, which provides substantial instrumental and human resources support to Ukrainian government forces, including several UAV drone projects.

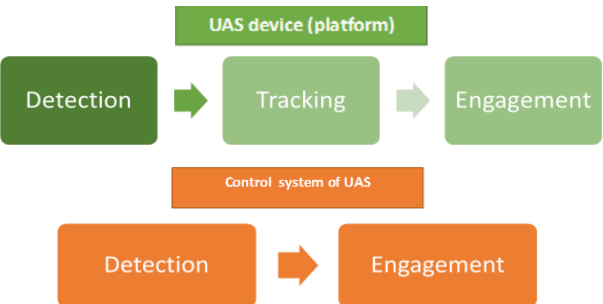
There are kind of "warfare-military start-up" activities, i.e. private companies are making innovative developments, drone modifications, even upgrades combined with redesigns, all aimed at expanding operational capabilities: increased range and payload, increased interference protection, development of control systems, and so on. Separatist forces, like the methods of terrorist organizations, see small drones as essentially armed platforms, in addition to reconnaissance and surveillance missions, and the use of "larger" military unmanned aerial devices of Russian origin can also be observed.

Many images have been posted on social media showing explosives (grenades) being used as a kind of bomb on drones, and have often been used. This is probably the first time we have observed the use of counter drone weapons systems (electronic jamming devices) in armed conflict.

Syria

There have also been a significant number of small drone applications in the armed component of the crisis in Syria, including significant deployments related to non-state actors. The source cited 38 different unmanned systems in 2015 and 2016, including a significant amount of heavily armed, modified hobby drones. [2]

Fig. 2 Process of counter UAS and control system



ISIS drone activities

The Islamic State's "drone strategy" is relatively well described. The overall concept of the use of small commercial drones has evolved gradually. The initial applications focused essentially on discovery and information gathering. Later, in the battle for Mosul, which began in October 2016, drones were used with a more nuanced, differentiated target system. They were used in large numbers against the pesmerga and the Iraqi Security Forces both in open terrain and in urban operational environments, where the fact that ground personnel operating among civilians, mosques and houses of sympathizers made it even more difficult to combat drones.

By analyzing the objectives of drone operations, it is clear that the priority has been given to maximal loss/destruction in the enemy's human, technical, infrastructure, mental resources and

effective support for propaganda objectives. To meet these priorities, three forms of drone deployment combat were used: reconnaissance/surveillance operations to obtain relevant information; direct attack of designated targets with improvised explosive devices, bombs (strike measurement); coordination and support of suicide bombings in order to cause maximum casualties.

3. The potential answers of air defence systems

Classic and even extended air defences are not capable of effectively countering all potentially imaginable earlier mentioned threats. In future air and air defence operations, it seems clear that a new type of threat needs to be new responded to.

Table 3 Effectors

Types of effectors	Technology
Guns and Ammunitions	
(Lower cost) Missiles	
Directed energy weapons (DE)	High Power Laser (HPL)/Medium Power Laser (MPL)  High Power Microwave (HPM) /Medium Power Microwave (MPM) 
Hunter-killer UAVs	
Novel effectors	

Conventional aerial target detecting, tracking and destruction with conventional radar, fire control systems and missiles (ammunition) is not enough. For detection often do not requires a reflected radar wave, but for example signals from the control unit. The intervention does not necessarily have to attack the UAS platform, success can be achieved by paralyzing the control system. (Fig 2.) This short example above shows that properly heterogeneous sensor and intervention systems need to be integrated if we are to create effective air defences against LSS-type threats.

Here's a look at what technologies-based weapon systems can be considered as so-called effectors. (Table 3)

To sum up layered air defence have to can integrate almost all effectors with their sensors and other sensor systems into flexible and effective C2 system.

3. Conclusions

According to a well-sounding saying, the 20th century vehicle was the car, while the 21st century's vehicle would be the drone. Drones allow us to separate the device from humans, so our devices can be operated without a direct human presence (remote monitoring, remote control, autonomous operation and a combination thereof). This trend is also true of warfare. They are an increasing segment of air warfare on the unmanned aircraft platform (UAVs, drones), although initially only replaced manned aircraft: e.g. RQ-4 Global Hawk unmanned reconnaissance aircraft flew instead of pilot-led aircraft in surveillance-reconnaissance operations, or MQ-1 Predator multitasking unmanned aircraft Hellfire missiles were used to strike instead of classic fighter bombers during crisis management in Afghanistan.

Practical examples have shown that cheap drones and improvised bomb-load modifications cannot provide the real, destructive efficiency expected of conventional weapon systems. It is easy to see that this cannot be a realistic expectation, but it does bring a range of benefits that terrorist organizations cannot disseminate. We can also include material issues, since it depends on many things, but in simple terms we can say that from a few hundred thousand forints we can build a system capable of terrorist attack from free commercially available devices, including improvised explosive devices. In addition to relative cheapness, a significant argument is that it allows for a mass-modified application, which, also due to the quantitative factor, can cause significant disruption to the operations of conventional forces, in the daily lives of the population.

Due to advances in technology and mass production, increasing price standards have already made drones a potential destructive tool in the mid-1990s (Aum Shinrikyo, Japan). This beginning was followed in less than two decades by drone operations, which can be considered almost mass use. As presented in our paper, based on the drone application strategy followed by the Islamic State, we can filter from planned and carried out deployments the experience that arming drones could be carried out even with small industrial options. The strategic concept of the use of small drones developed gradually, with initial actions focused on detection and information gathering later followed by drone applications with a more differentiated target system.

In our view, the illegal, terrorist use of small drones has only entered its initial phase. Available with ever-evolving technical capabilities, drones will enable the development of ever-increasing combat capabilities, and the Internet will provide an unlimited, uncontrollable framework for technological transfers already today. "Swarming," the use of drone swarms, will be one of the biggest challenges in the coming days. This puts the mass application in a higher dimension, as it is still difficult to imagine that up to tens of drones simultaneously carry out an air strike in concert or in communication with each other, analogously with the so-called COMAO operation carried out by the classical Air Force.

3. References

1. The Bonus Military Balance 2019 content (<https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/xmb2019-bonus-content>) (downloaded: 31 Apr 2021)
2. Dan Gettinger: Drones operating in Syria and Iraq (<http://dronecenter.bard.edu/files/2016/12/Drones-in-Iraq-and-Syria-CSD.pdf>) (downloaded: 31 Apr 2021)
3. Larry Frieze, N.R. Jenzen-Jones, Michael Smallwood: Emerging Unmanned Threats: The use of commercially-available UAVs by armed non-state actors, Special Report No. 2, 2016, Armament Research Services (ARES), ISBN 978-0-9924624-7-5
4. Hezbollah's Terrorist Activity, 2000-2012 (<http://www.crethiplethi.com/hezbollah-s-terrorist-activity-2000-2012/lebanon/2013/>) letöltve: 2018. augusztus 3.
5. Balkan Serkan: DAESH's drone strategy technology and the rise of innovative terrorism, 2017, SETA Foundation for Political, Economic and Social Research, ISBN: 978-975-2459-23-6 (www.setav.org) (letöltve: 2018. augusztus 11.)
6. Mauro Labrano: Swarm drone attack in Syria points to new kind of warfare, <https://globalriskinsights.com/2018/01/swarm-drone-attack-syria-uav/> (letöltve: 2018. augusztus 13.)
7. Komjáthy Lajos József, Csengeri János A távirányított és pilóta nélküli repülőrendszerek alkalmazási lehetőségei a felkelők elleni műveletek során, Honvédségi Szemle, (2017/6.) Pp. 81-92. (2017)
8. Komjáthy Lajos József A műveleti környezet és körülményei változásainak hatása napjaink katonai tevékenységére, Hadtudományi Szemle X.:(3) pp. 63-77. (2017)
9. Krajnc Zoltán Csengeri János Hybrid warfare from military air perspective In:8. medzinárodná vedecká konferencia: "National And International Security 2017". 614 p. Liptovsky Mikulas: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. pp. 254-262. (ISBN:978-80-8040-551-9)
10. Krajnc Zoltán Csengeri János Early concepts and theories of employment of air power In: 12. medzinárodná vedecko-odborná konferencia: Management - Theory, Education and Practise 2016. 346 p. Liptovsky Mikulas: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2016. pp. 164-171. (ISBN:978-80-8040-536-6)
11. Csengeri János „Operation Allied Force” A NATO légi háborúja a dél-szláv válság megoldása érdekében 1., Repüléstudományi Közlemények, XXV:(1) pp. 114-125. (2013)
12. János Csengeri Material management and transportation procedures in air force logistic operations, In: Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie. 380 p. 2014. pp. 222-233. (ISBN:978-80-8040-496-3)
13. Patrick Tucker In Ukraine, Tomorrow's Drone War Is Alive Today, <https://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/> (downloaded 21 Apr 2021)

Practical approaches for collecting intelligence information

Ilin Savov

Academy of the Ministry of Interior, Sofia, Bulgaria

ilin_savov@abv.bg

Abstract: *The report examines and assesses the possibilities for obtaining information for the benefit of the security services. The main practical approaches and their specifics regarding the collection of intelligence information are highlighted.*

Keywords: SECURITY, INFORMATION, INTELLIGENCE, OSINT, TECHNICAL TOOLS

1. Introduction

Information has always played a decisive role in the history of civilization and has served as a basis for decision-making at all levels and stages of development of society and the state. In the history of social development can be distinguished several information revolutions related to radical changes in the field of production, processing and transmission of information, which led to radical transformations of social relations. As a result of such transformations, society has acquired in a sense a new quality.

We are witnessing a significant increase in the role, place and impact of information in the life of the individual, society, state. Information today has become a powerful real tangible resource, having even greater value than natural, financial, labor and other resources. Information has become a commodity that is sold and bought. Information in the present plays a paramount role as a non-traditional weapon, information wars arise, develop and end. The cross-border information network Internet is developing and entering our lives extremely fast.

The possibilities for production (creation), processing, storage and dissemination of information are becoming increasingly important. This is not just about the amount of information, ie. for quantity, but also for its qualitative side - structuring and its transformation into knowledge and cognition. In the field of national security, a large amount of information needs to be processed, which is why "the ability of the national information resource to control and form the most important information flows on a regional and global scale must be taken into account.

The development of information and communication technologies covers all spheres of society - economy, social life, culture, science and education, political life. Citizens and society are increasingly relying on reliable and reliable information on the Internet. The state annually increases the number of services and the amount of information it provides to citizens and businesses through the Internet.

This report will briefly look at traditional practical approaches to intelligence gathering.

2. Collection and systematization of intelligence information

Open source intelligence (OSINT) is one of the methods of obtaining information about special services. It includes searching, selecting and collecting information obtained from publicly available sources and its analysis.

According to Central Intelligence Agency (CIA) analyst Sherman Kent, who spoke back in 1947, politicians receive up to 80 percent of the information they need to make peacetime decisions from open sources. Later, General Samuel Wilson, head of the Intelligence Department of the United States Department of Defense from 1976 to 1977, noted that "90 percent of intelligence comes from open sources and only 10 percent is at the expense of the agency." [1]

Open sources include:

- Mass media - newspapers, magazines, radio, television;
- Public government reports, official budget data, collection and analysis of industry reports, press conference materials, various public statements, hearings, legislative debates and speeches;

- Information obtained from professional and academic reports presented at scientific conferences, symposia, professional associations, dissertations and theses and expert reports;

- Professional and academic reports, reports, articles;

- Visits to exhibitions and fairs;

- Internet, in particular social sites, video hosting, directories, blogs, forums

It is necessary to pay attention to another important emphasis on the directions in which the acquisition of information is important in terms of:

- the collection of political, economic and military information necessary for the assessment of the military-economic and moral-political potential of the countries-objects of intelligence activity;

- obtaining special intelligence information related to specific areas of economics, science and technology, military affairs. It is usually intended for a narrower circle of specialists and serves as a material in the development of strategic plans (for economic pressure, for any kind of "sanctions", etc.)

In the practice of all intelligence centers around the world, information obtained by intelligence agents is considered indispensable. This approach remains a crucial tool for overcoming the barriers erected by states to protect national interests. "On the way to getting the most important information ..." Sherman Kent wrote, theoretically justifying the importance of intelligence for the United States ... there are often insurmountable obstacles. They are deliberately created by other countries, and in order to overcome them, methods are needed that are often unfamiliar to the average person. These methods consist of obtaining information by illegal means." [2]

The benefits of intelligence are obvious. Everyone, except the carrier of information, can analyze it, summarize and draw conclusions, ie. to receive the necessary information from the set of indirect data. They are used to solve tasks that are impossible to accomplish, by staff members of the special services or by technical means, difficult or impractical, although this does not preclude their joint work.

Intelligence centers show great interest in the small weaknesses of man, caught in their field of vision and try to use his shortcomings or vices, to deceive him, scare, use, as the German expert J. Yosten writes.

The Internet can be considered an indispensable source of information. The data obtained from the network are used in the field of education, business, medicine, entertainment and recreation, etc. But the Internet is not just an informational Klondike. Cyberspace has long been an arena of network espionage, involving various intelligence agencies and special services working for government, business and the criminal world.

The question arises why the World Wide Web is a space for acquiring foreign secrets? The answer is simple and clear: because the Internet has everything. Everything - this is all information about public and state institutions, organizations, business structures and individuals.

Globalization provides unprecedented access to tools such as the Internet, satellite communications, electronic funds transfer, easy international movement, exchange of official documents and more. Unfortunately, these opportunities are becoming the main tools used by criminal groups and terrorist organizations to achieve their goals. The development of modern global processes makes it possible to connect geographically remote groups, better

coordination, easier communication and realization of information goals.

The Internet is used in various ways by terrorist organizations. They can be combined in two main directions.

The first direction shows that the Internet has become a useful channel of communication that allows terrorists and their followers to spread propaganda and instructions.

The Internet may not be used, but rather attacked by terrorists in the so-called cyber-terrorism. According to many researchers and politicians, who describe the connection between terrorism and the Internet mainly as cyber-terrorism or cyber-war (so-called attacks on communication and computer networks). No less threatening are the numerous Internet applications that terrorists take advantage of.

The information age influences not only the targets and weapons chosen by terrorists and criminal organizations, but also the ways in which these groups work and structure their individual units. Several of the most dangerous terrorist organizations use information technology (IT) - such as computers, software, telecommunications devices, and the Internet - to better organize and coordinate.

The rapid development of equipment and technology in recent decades has led to even faster development of technical means and systems in intelligence. Enormous resources are being invested in the creation of intelligence tools and systems in all developed countries. Hundreds of companies in many countries work in this field. This branch of business has long taken its place in the general system of Western economies and has its own solid legal basis.

All leading experts agree that the value of information in the use of special technical means (electronic surveillance, tracking and eavesdropping) in the investigation of certain forms of serious crime or terrorist acts is unquestionable. This method is extremely important for the protection of national security in modern conditions.

The method "obtaining information through special technical means and channels" covers a set of opportunities and practices.

Conventionally, the method of "obtaining information through special technical means and channels", according to the American classification, is divided into several separate groups:

- Audio surveillance:
 - Eavesdropping on telephone calls;
 - Control of calls made over the Internet (VoIP);
 - Control of conversations in the room.
- Visual surveillance:
 - Hidden video surveillance devices;
 - Built-in video system in vehicles;
 - Surveillance Drones.
- Tracking surveillance:
 - Global positioning systems (GPS systems);
 - Mobile devices;
 - Radio Frequency Identification (RFID) devices;
 - Biometric information technologies (retinal scanning of the eyes when visiting airports, etc.).
- Traffic surveillance:
 - Monitoring of computer information;
 - Monitoring the use of computer systems.

3. Results and discussion

The development of communication technologies on the one hand and their use by people with different interests, including for criminal purposes, has led to the paradox of the world community choosing which priority to be: security or insecurity, security or human rights.

The security dilemma organically stems from the peculiarities of the emerging modern world, including its systemic nature. Therefore, the dilemma of security of man and society is of scientific interest.

There is no doubt that the change of epochs causes a change in the security system: therefore, with the emergence of new dangers and threats, new factors of development, there is a need for a new security paradigm and its security system.

Above all, the definition of the dilemma of security of man and society with a set of values and ideals that change the external and internal environment is indisputable. There are different views here. For example, the basic idea of the US national security strategy is that the establishment of global and, in particular, American security is impossible without America's leadership in the world, without its economic and military superiority over other countries. Hence the strengthening of the role of the state in America's national security system. In other words, it is increasingly viewed through the prism of the triad "individual security - state security - international security" (this model has become particularly important in the light of the events of September 11, 2001). scheme the individual "relinquishes more and more of his care for his own security to the state."

4. Conclusion

Before us is the paradox of modern liberal civilization - the freedom and security of the individual are becoming increasingly dependent on the state, the pressure of the latter on the individual continues to grow, due to the emergence of new information technologies and technical systems that threaten the foundations of the earth. civilization. The dilemma for the security of the individual and the state here is that the distinction between the private and the public is becoming increasingly difficult, and this contributes to the legitimate conquest by the state of the bridgehead "freedom for the individual."

Today, stronger measures need to be taken to combat threats to national security and crime in Bulgaria. An example of this was given by the United States with its Patriot Act of 2001, characterized by a marked increase in the fight against terrorism and a range of restrictions on citizens' rights.

An essential and important ingredient in the fight against crime, creating risks and threats to national security and public order, is the control of traffic data and the use of their unsuspected possibilities for adequate counteraction to any crime.

Each country must proceed from the specific legal and criminal situation in the country, and not simply from abstract notions of "human rights". At the same time, the main condition for the protection of citizens' rights is a strong state power based on law.

5. References

1. **Greene, Kate.** Reality Mining. Sandy Pentland is using data gathered by cell phones to learn about human behavior. – In: *MIT Technology Review* February 19, (2008) <http://www2.technologyreview.com/news/409598/tr10-reality-mining/>
2. **Greenwald, Glenn.** NSA taps in to internet giants' systems to mine user data, secret files reveal. – In: *The Guardian* 6 June (2013). <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>
3. **Kent, Sherman.** Strategic intelligence for American world policy. Princeton University Press, (1966).
4. **Kondratiev, Alexander.** Based on open sources. - In: *Military industrial courier. MIC*, September 16, (2009), № 36 (302)
5. **Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015.** <https://www.congress.gov/bills/114/congress-house-bill/2048>
6. **Marks, Paul.** Pentagon sets its sights on social networking websites. - In: *New Scientist* [онлайн]. June 9, (2006) <https://www.newscientist.com/article/mg19025556-200-pentagon-sets-its-sights-on-social-networking-websites/>

Examples of nuclear security measures 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: *The lifetime of a nuclear facility extends from the earliest planning stages through to its decommissioning. It is important to consider nuclear security early in the design of new facilities and during partial redesigns or modifications, as it can result in nuclear security for these facilities that is more efficient, more effective and better integrated with other safety, safeguards, operational and other measures. Nuclear security measures are also important during commissioning and operation, they should not cease at decommissioning, as they are important in addressing the protection of the remaining quantities of nuclear material or other radioactive material, which has accumulated during the operations stage.*

KEYWORDS: NUCLEAR AND RADIOACTIVE MATERIAL, NUCLEAR FACILITY, NUCLEAR SECURITY, NUCLEAR SECURITY MEASURES

1. Introduction

Nuclear facilities have often been designed without giving sufficient consideration to nuclear security until late in the design stage or after operational and safety features had already been determined. Nuclear security measures were added later, often resulting in the application of measures that were not integrated or fully compatible with measures relating to safety, safeguards, and operations.

Moreover, implementing new or additional security measures after a nuclear facility is in operation may be difficult and costly. Considering security requirements early in new designs, partial redesigns and modifications can result in nuclear security that is more efficient and effective as well as better integrated with other measures in the facility.

Various requirements apply to a nuclear facility during all stages in its lifetime, including nuclear safety, nuclear security, safeguards and operational requirements. As stated in [1], "Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that security measures do not compromise safety and safety measures do not compromise security."

A balance should be achieved between these various requirements. Ideally, the measures implemented to meet these requirements should complement each other, but in some cases, the measures implemented may conflict with one another.

2. Eight stages in the lifetime of a nuclear facility

The lifetime of a nuclear facility is divided into the following eight stages: planning, siting, design, construction, commissioning, operation, cessation of operation and decommissioning.

2.1 The planning stage for a nuclear facility includes activities such as conceptual design and obtaining required approvals prior to receiving authorization to begin formal siting and design stages.

2.2 The siting stage for a nuclear facility generally comprises the consideration of candidate sites, taking into account various factors such as available infrastructure and workforce as well as geographical and security considerations. This would then be followed by a detailed evaluation of the candidate sites. The evaluation may culminate in a request for, and approval of, a selected site.

2.3 In some cases, the design stage is an iterative process - from conceptual design through to final design - that ultimately results in a request for approval to construct a nuclear facility. In other cases, generic designs may be developed and approved prior to the siting stage.

2.4 The construction stage comprises site preparation, the manufacture, acquisition and assembly of the components of the

nuclear facility, the installation of components and equipment, and the performance of associated tests.

2.5 The commissioning stage comprises the process of making systems and components of facilities operational, along with initiating associated nuclear security activities, and verifying that the systems, components and activities are in accordance with the design and have fulfilled the required criteria.

2.6 The operation stage includes all routine and emergency operations of the facility once it is commissioned.

2.7 The cessation of operation stage describes a planned condition at a nuclear facility in which facility operations have ceased either permanently in preparation for decommissioning or for an extended period of time for major modifications, maintenance or repair.

2.8 The decommissioning stage includes the administrative and technical actions taken to remove the nuclear material and other assets from the facility.

Nuclear security measures can be removed from the facility when no nuclear material and other radioactive material remain and there is no longer the potential for unauthorized removal of nuclear material or an act of sabotage that causes unacceptable radiological consequences.

Although not explicitly defined as a stage, there are periods during the lifetime of a nuclear facility when it could be undergoing some type of modification during one of the stages. This typically occurs during the operation stage but may occur in other stages as well. These modifications could lead to a need for increased or altered nuclear security measures.

One such example is if the operator of a site with one nuclear power plant were to receive approval to construct a second power plant on the same site while continuing operation of the original three.

During construction, part of the site would be in the design stage through to the commissioning stage, while the other three would remain in the operation stage. Ultimately, when the new plant enters operation, the facility would enter a stage in which all four power plants were in the operation stage.

A second example is if, during the operation stage of a nuclear facility, modifications affecting physical protection measures were to be completed, such as changing a security boundary, addition of new target locations, removal of a target location, or installation of a new perimeter intrusion detection system. While the facility remained in the operation stage, the modifications to the physical protection equipment may be designed, constructed, tested and implemented.

3. Security measures during each stage

Below, the major nuclear security actions for each stage of the lifetime of a nuclear facility for the country, the competent authority and the operator are set out. These actions apply to new facilities as well as existing ones, although existing facilities may already have completed some of these actions.

In addition, some actions assigned in this section to the country could be delegated to the competent authorities, as appropriate. All aspects of nuclear security, including information security and computer security [2, 3], should be maintained during all relevant stages in the lifetime of a nuclear facility.

STAGE 1: Planning stage goals

Measures to address applicable regulatory nuclear security requirements for the new nuclear facility should be identified during the planning stage.

Major decisions will be made during this stage, and the importance of nuclear security should be recognized and reflected in these decisions.

Nuclear security goals at this stage:

- (a) Ensuring that the nuclear security requirements are met that are set out in the legal and regulatory framework, as applicable to the proposed facility and the type and quantity of nuclear material and other radioactive material expected to be in use or storage at the facility;
- (b) Ensuring the integration of nuclear security requirements with operational goals and safety requirements in the facility design specifications;
- (c) Identifying nuclear security roles and responsibilities and assigning them to the various competent authorities and organizations involved in nuclear security at the facility;
- (d) Establishing a framework for communication among all relevant stakeholder organizations (e.g. those responsible for nuclear safety, nuclear security, safeguards and facility operations);
- (e) Identifying and developing nuclear security competencies (e.g. human resources and technical capabilities) needed to implement nuclear security measures;
- (f) Raising awareness of security issues among all relevant stakeholder organizations.

STAGE 2: Siting stage goals

The location of the nuclear facility is identified during the siting stage. The siting of a nuclear facility has the potential to increase or decrease its vulnerability to external security threats as well as to increase or decrease the potential consequences that could result from malicious acts.

During site selection, nuclear security considerations should be evaluated alongside safety and other considerations, such as seismic activity, geology, meteorology and hydrology.

Nuclear security goals at this stage:

- (a) Any local or regional threats that could impact the facility;
- (b) Security interfaces and interdependencies with existing nearby nuclear facilities;
- (c) Topography that may enhance or increase the vulnerability of the security of site;
- (d) Potential impact of radiological releases to the environment or populated areas (e.g. population centres, critical infrastructure, airports and other transport assets, and international borders);
- (e) The availability of sufficient response forces to respond in a timely manner to a nuclear security event;

- (f) Free space for site reconfiguration, including expansion, if security needs increase.

STAGE 3: Design stage goals

Measures required to meet applicable regulatory nuclear security requirements should be integrated into the overall design during the design stage. Potential conflicts between safety and security measures should be identified and minimized during the design stage, and measures should be implemented in a manner to strengthen synergy between these two areas where possible.

For example, access control measures for sensitive areas in the facility need to account for both safety and security considerations.

Nuclear security goals at this stage:

- (a) Developing nuclear security designs that meet regulatory requirements for nuclear security and accounting for the national design basis threat or representative threat statement as well as the preliminary facility analyses;
- (b) Characterizing and evaluating the nuclear facility to determine the required protection levels for the facility for the protection of nuclear material and the possible radiological consequences of sabotage;
- (c) Planning for nuclear security areas in the facility (e.g. limited access area, protected area, inner area and vital area) in order to provide defence in depth;
- (d) Identifying locations and types of critical nuclear security asset, such as the central alarm station and guard stations;
- (e) Identifying and resolving conflicts between regulatory requirements for nuclear security and those for other disciplines as early in the design stage as practicable.

STAGE 4: Construction stage goals

During the construction stage of a nuclear facility, the operator should take measures to ensure that the facility nuclear security measures are implemented as designed during the various stages of construction.

At or near the end of construction, nuclear security measures should be tested to determine that they are installed and operate in a manner that addresses the applicable regulatory requirements and the design basis threat or representative threat statement.

Nuclear security goals at this stage:

- (a) Ensuring that the construction and installation of nuclear security measures meet design requirements;
- (b) Preventing the introduction of contraband to the construction site as well as any tampering with facilities or equipment that could aid in the execution of a malicious act after the facility becomes operational;
- (c) Isolating construction activities from other operational facilities (e.g. those located on the same site) and addressing interim security vulnerabilities which may be introduced to nearby facilities during the construction stage;
- (d) Conducting preparatory activities, such as establishing an organization or organizations that will be responsible for nuclear security at the facility during and after construction, training security personnel and developing plans and procedures for nuclear security at the facility;
- (e) Conducting testing of physical protection equipment and other systems and components that contribute to nuclear security following installation to ensure that they meet functional, operational and performance requirements.

STAGE 5: Commissioning stage goals

During the commissioning stage, the operator should demonstrate that the facility as constructed meets the design specifications,

including that the combination of nuclear security measures in place meets the applicable regulatory requirements.

This stage also includes administrative and technical actions taken to introduce the nuclear material into the facility. [4]

Nuclear security goals at this stage:

- (a) Validating that the facility's nuclear security plans, operating procedures, assessment procedures, contingency and emergency procedures adequately address applicable regulations, the design basis threat or representative threat statement;
- (b) Verifying that all physical protection equipment and other systems and components that contribute to nuclear security functions are in place and meet the design requirements;
- (c) Implementing compensatory nuclear security measures to provide protection for the material until the nuclear security measures are fully operational if nuclear security measures are not fully implemented upon arrival of the nuclear material into the nuclear facility;
- (d) Familiarizing all facility personnel with nuclear security processes and procedures;
- (e) Developing a commissioning protocol to provide evidence that the nuclear facility, as constructed, meets the design specifications and complies with applicable regulatory requirements for nuclear security;
- (f) Describing and evaluating the nuclear security measures described in the nuclear security plan through assessments, including performance testing;
- (g) Establishing a formal process to evaluate the impacts on nuclear security from proposed operational changes, changes in nuclear safety measures or facility modifications prior to their implementation;
- (h) Establishing a formal process to evaluate the impacts on facility operations and on nuclear safety from proposed changes to nuclear security measures prior to their implementation;
- (i) Identifying and correcting deficiencies in nuclear security processes and procedures.

STAGE 6: Operation stage goals

During the operation stage, sustained, effective nuclear security should be maintained. The elements of nuclear security are described in a nuclear security plan, the development of which was mentioned in the previous two stages. [5]

The nuclear security plan should form the basis for oversight by the competent authority and is part of the license or authorization of the facility. Any major modifications to the facility's nuclear security measures should be subject to review and approval by the competent authority.

Nuclear security goals at this stage:

- (a) Ongoing evaluations of nuclear security measures through inspections and performance testing, including exercises;
- (b) Maintaining a formal process to evaluate the impacts on nuclear security from proposed operational changes, changes in nuclear safety measures or facility modifications prior to their implementation;
- (c) Maintaining a formal process to evaluate the impacts on facility operations and on nuclear safety from proposed changes to nuclear security measures prior to their implementation;
- (d) Ensuring that any compensatory measures are implemented to address non-compliance with requirements or failure of nuclear security measures;
- (e) Maintaining a strong nuclear security culture;

(f) Responding to changes in the threat environment, as appropriate, through changes to the nuclear security system;

(g) Implementing sustainability and quality assurance programmes.

STAGE 7: Cessation of operation stage goals

As long as a risk of unauthorized removal of nuclear material or of sabotage leading to unacceptable radiological consequences remains, nuclear security measures should continue to be implemented on the site, although they should be tailored to the changing nature of operations on the site.

This applies whether the facility has ceased operation permanently, in preparation for decommissioning, or for an extended period of time for major modifications, maintenance or repair.

Nuclear security goals at this stage:

- (a) Modifying nuclear security measures in situations where nuclear material inventories are relocated, removed, increased or otherwise changed, as needed;
- (b) Accounting for impacts on nuclear security of reduction or reassignment of personnel resources;
- (c) Supporting cessation activities by bringing in new entities and personnel to the facility, including contractors, as appropriate;
- (d) Evaluating possible changes to nuclear security measures to account for changes to the facility that may impact the potential for sabotage;
- (e) Reconfiguring security areas following changes to the facility configuration to ensure that adequate nuclear security measures continue to be in place, as appropriate;
- (f) Evaluating process operations equipment and structures to identify quantities of nuclear material or other radioactive material accumulated in hold-up during the operations stage.

STAGE 8: Decommissioning stage goals

The decommissioning stage involves activities that will ultimately lead to the removal of all nuclear material and other radioactive material from the facility. However, as long as a risk of unauthorized removal of nuclear material or of sabotage leading to unacceptable radiological consequences remains, nuclear security measures should be maintained.

The application of these measures should be based on a graded approach, taking account of the category of nuclear material and its potential for sabotage leading to unacceptable radiological consequences.

Nuclear security goals at this stage:

- (a) Re-evaluating nuclear security requirements as the inventory of nuclear material and the potential radiological consequences associated with sabotage change;
- (b) Re-evaluating process operations equipment and structures to identify hold-up quantities of nuclear material or other radioactive material accumulated in them during the operations stage;
- (c) Balancing safety and security objectives during decommissioning, for example, it may be required to delay decommissioning for dose reduction purposes (safety) versus the immediate removal of nuclear material and/or sensitive information for security purposes;
- (d) Reducing nuclear security measures during the period while nuclear material and contaminated equipment is being removed from the nuclear facility, while continuing to meet regulatory requirements based on a graded approach;
- (e) Ensuring proper disposal of sensitive information and security related equipment;

(f) Managing changes in the workforce or organizations that impact nuclear security at the facility, such as workforce reductions;

(g) Encouraging personnel to remain vigilant with regard to security awareness and nuclear security culture during decommissioning.

5. Conclusion

There are well known risks associated with the use of nuclear material and nuclear facilities. From a nuclear security perspective the two primary risks are those associated with unauthorized removal of nuclear material, for potential use in a nuclear explosive device, and with sabotage of the material and/or facility resulting in Unacceptable Radiological Consequences (URC).

The management of these risks is the primary basis for nuclear security in relation to nuclear material and nuclear facilities. If a country has made the decision to accept nuclear material and nuclear facilities within its borders, it is also accepting the responsibility to protect those materials from unauthorized removal and the facilities and materials from sabotage resulting in a release of radionuclides.

The country's physical protection regime should be reviewed and updated regularly to reflect changes in the threat and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of nuclear material and nuclear facilities.

6. Acknowledgement

The issues discussed in this report are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum communication, intelligent security systems and risk management (Quasar) ", which has received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

Bibliography

[1]. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

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

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

[4]. Пъневски В. С., "Възможни специфични изисквания към проектирането на мехатронни системи за сигурност и защита на критична инфраструктура", Сборник доклади от Научна конференция „Актуални проблеми на сигурността“, 22-23 октомври 2020 г., 6, Издателски комплекс на НВУ „Васил Левски“, 2020, ISSN:2367-7465, стр. 84-90;

[5]. Panevski V.S., "POSSIBLE APPROACH FOR DEVELOPING A MODEL OF INTELLIGENT SECURITY SYSTEM APPLICABLE IN ITS DESIGN IN THE QUASAR CENTER OF COMPETENCE", SECURITY & FUTURE, 4, 2, Scientific Technical Union of Mechanical Engineering "Industry-4.0", 2020, ISSN:2535-082X, стр. 47-50.

Emotional intelligence in small unit's leadership

Vladimir Statev

“Vasil Levski” National Military University, Veliko Tarnovo, Bulgaria
vladimir.statev@gmail.com

Abstract: Emotional Intelligence is a concept that dates back to the last decade of the 20th century when it started gaining momentum. Today its theories and practices are widely accepted and are applied by thousands of managers across the World. If we assume that business managers and military leaders and commanders often have similar problems in their field of work concerning subordinates then we need to look into the possibility of military leaders applying Emotional Intelligence as their civilian counterparts do.

Keywords: EMOTIONAL INTELLIGENCE, MANAGEMENT, SMALL UNIT, SELF-AWARENESS, SELF-REGULATION, EMPATHY, MOTIVATION, SOCIAL SKILLS

1. Introduction

Emotional Intelligence is not a new concept. It dates back to the last decade of the 20th century. Arguably the most iconic author on the subject is Daniel Goleman who claims that “...high IQ is no guarantee of success, happiness, or virtue, but until Emotional Intelligence, we could only guess why.” [1] Today theories and practices of Emotional Intelligence are widely accepted and are applied by thousands of managers across the World. That is a fact and it would not be so if they did not show sufficient results. But they do. So if we can agree that business managers and military leaders and commanders have similar responsibilities and duties when subordinate personnel is considered and as long as we stay within the boundaries of routine operations, we can assume that managers and military leaders and commanders will often have similar tasks and problems in their field of work. And if that is the case, then a logical question arises – Can Emotional Intelligence be applied by military leaders as successfully as their civilian counterparts? In the following pages, we will try to answer that particular question.

2. Problem discussion

A small military unit's leader such as a platoon leader or a company commander can be compared to a person hired in the middle management class in almost any business organization. That is the case if we take under consideration the number of personnel/employees the military leader/manager has direct responsibility for. By accepting that there are many similarities between managers and military commanders in the daily interactions with subordinates and that such a parallel is based on a reasonable amount of equivalency between the two professions, we reach the point where we need to see how the prominent features of a successful middle management personal and small military unit's leaders can be compared.

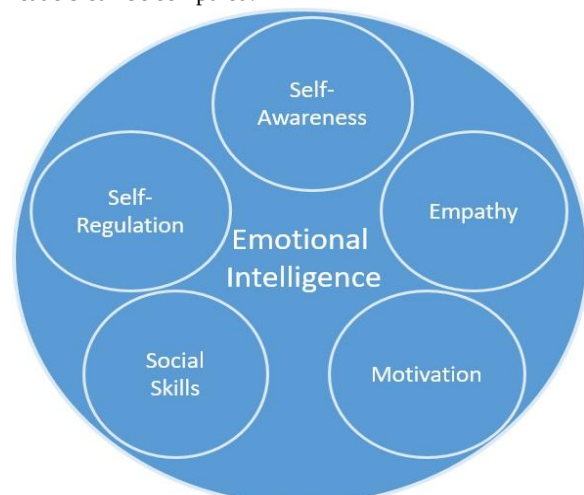


Fig. 1 Components of Emotional Intelligence.

2.1 Self-Awareness

People who possess the quality of Self-Awareness have a deep understanding and hold over their own emotions, their strong sides, weak points, needs, and emotions. These people are neither too critical of the actions of others nor are they too much of an optimist when it comes to people's behavior. The self-aware type of person is mostly a honest one – with themselves and with the people they interact with. People who are self-aware understand where they are headed and why. They would not make compromises with their values and go against their ideals. They know that this would create internal struggles ahead and cause problems later.

Most importantly, self-aware leaders know how their inner workings and feelings affect themselves and what effect they have on the individuals surrounding them. For example, if a person is self-aware, they would know that closing deadlines bring out their worst characteristics, put time in more detailed planning, and finish the task in advance rather than letting the deadline creep in. This method can be applied by business managers as well as military commanders as long as both categories of decision-makers know themselves and the way their minds function in difficult or unfamiliar situations.

It is proven that the mood of the leader is transmitted to their subordinates. [2] So if the leader military or not, permits the situation to negatively affect their feelings, this would affect the physiological climate of the team or unit they are in charge of. Which will then lead to loss of productivity. Loss of productivity may result in failure, which in business costs money and in warfare costs lives. This is why Self-Awareness is the first trait that we discuss when talking about Emotional Intelligence and its correlations with leadership.

2.2 Self-Regulation

Emotions are generated by our brains based on a number of internal and external factors. So they are a product of the biological process and viewed as such are inevitable. This however does not mean that we cannot control them. In the context of Emotional Intelligence, Self-Regulation is described as an internal dialog that a person has with themselves. A person who leads this kind of dialog is afflicted by a bad temper or emotional impulse as often as all people are. But an individual who possesses the skill to communicate with themselves in such a way controls their emotions and feelings, and even uses them in their favor. They are in control and make the conscious decision of what face they are showing to the outside world and do not let emotions force their hand.

Let us imagine a situation where a manager is a witness of how a team of their employees makes a poor presentation in front of the board of directors of the enterprise. If the managers do not possess the ability to self-regulate, they can and most certainly will start to shout and might even break a piece of furniture as soon as the directors walk out of the conference room. For comparison, a manager who can self-regulate will note the poor performance in a calm manner, then they would take time to consider their emotional status and the reasons for this failure. They would ask themselves questions such as “Is this a result of lack of efforts?”, “Are there external factors in play?” and “What is their part in this affair?” After finding the answers, a good manager would bring the team

together and they would discuss the consequences of the poor performance, analyze the problem and present a working solution.

We can easily imagine a similar situation where we have a platoon on the firing range, demonstrating their skills in front of the brigade commander and the position their platoon leader would find themselves if the troops perform lower than expected. But why is Self-Regulation so important for a good leader? People who self-regulate are reasonable and are capable of building a suitable working environment based on trust and equity. Such an environment reduces friction and increases productivity and performance. Self-regulation travels down the ladder and chain of command. If the leader is known for their calm demeanor, the subordinates are prone to act accordingly in any situation, which is important when it comes to business ventures and it is crucial in military operations.

2.3 Motivation

Motivation is a common trait among efficient leaders in all fields of work. A leader who possesses that characteristic can be distinguished from the rest. Such individuals aim at surpassing all expectations – those of others and their own. When talking about Motivation, we need to talk about the cornerstone on which it is built – achievements. Most people are motivated by external factors such as money, status, or impressive title or rank. On the other hand, those who have it in them to lead, are motivated by their desire for achievements for the sake of the achievements themselves.

How can we identify those who are motivated by their strive toward the achievement and not by the reward? The first thing we should note is their behavior and dedication to the work. Those people who seek challenges tend to seek self-improvement. They are proud of what they have achieved and try tirelessly to find ways to do things better. The second thing that marks an individual as achievement-driven is their tendency to ask questions regarding the ways things are done and the models that are followed. Critical thinking and the desire to implement new methods and apply new approaches in their work is what sets these people apart from the reward-motivated.

To better illustrate this point, we would review the actions taken by a manager in a cosmetics company. The manager was frustrated by the time it took for the numbers from the active sales personnel to be collected and processed. The manager created an automatic system that remained the sales personnel to send the data at the end of each business day. That decreased the time it took for the information to be gathered and analyzed from weeks to hours, which was a great improvement by any standard.

Today the military forces across the World implement all kinds of automatic systems, but that does not mean that perfection has been achieved. That inevitably applies when considering the lower echelons. The lower you are in the chain of command, the more concrete the regulations you have to follow are. The lack of freedom when managing a unit blocks the potential improvements that small unit leaders may bring to increase the effectiveness of the system.

Another trait that shows that a person aims at success is that they constantly try raising the bar and measure their progress. Everyone who is self-aware and motivated would be aware of their limits, but they would not be satisfied by achieving mediocre goals. It is only natural that such people track and note their own progress, but also that of their team or unit so that they can compare and measure it. Individuals who lack Motivation on the other hand, often have no idea how their work compares against that of their peers and people occupying similar positions.

An interesting fact is that a person with a high level of Motivation does not lose focus when facing hard times or meets with failure. When dealing with such negative outcomes, some managers would blame the circumstances or take it as their personal

fault. But motivated leaders take it as a challenge and a chance to prove themselves by turning the course of events in their favor.

The last thing that indicates the level of motivation a person possesses is their loyalty to the organization or unit. People who do the work only because they extract satisfaction from the results or what they have achieved, tend to stay in the same structure or organization even when offered a better paying position in another company.

We can claim with confidence that Motivation is typical for a strong leader because if a leader is constantly raising the bar and pushing themselves to perform better and achieve greater results, they would do the same with their subordinates and given the chance – with the organization itself. The desire to out-perform and to track progress is contagious. It spreads and by doing so raises the standards and the overall success of the organization.

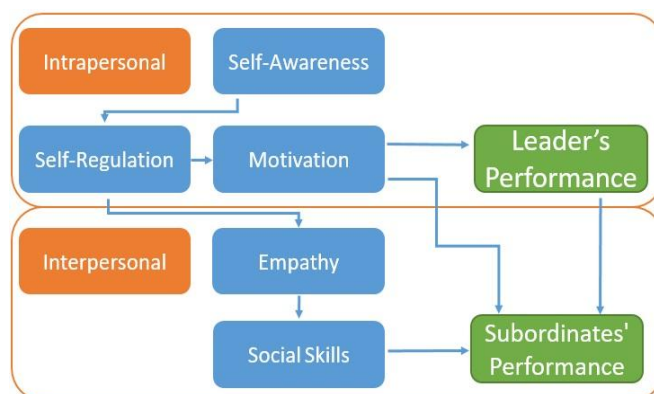


Fig. 2 Connections between the components of Emotional Intelligence and performance.

2.4 Empathy

Empathy is something we associate with the relations we have with family and friends. It is not commonly correlated with workplace relations. The general public would not consider empathy as an attribute of any leadership, it just does not belong in the business world.

But empathy should not be mistaken for sentiment. It does not mean that a leader should take the emotions and feelings of subordinates as their own or will try to please everyone. This would be a living nightmare and every action or decision would be next to impossible. Empathy means considering the feelings and emotions of subordinates as one of the factors in the decision-making process, which will lead to better and more intelligent decisions.

A real-life example of Empathy in action presented itself when two real-estate firms declared a merging. This led to the doubling of employees' positions. One section chief gathered their subordinates and held a melancholic speech highlighting the fact that many would soon be dismissed. The section chief of a similar structure in the other company openly declared their concerns and guaranteed their subordinates that they would do what they can to provide information as soon as possible and promised fair treatment during the merging.

The difference between the actions of the two sections chiefs was rooted in Empathy. The first one was preoccupied with their own feelings and doubts and failed to consider those of their subordinates. The second chief tapped in the emotions of their employees and responded in the best possible way. It is no surprise that the second chief managed to keep most of their section intact, while the other ceased to exist after the merging of the firms was completed. This happened not because a higher authority made such a decision, but because the employees felt the lack of support and clarity from the position of the direct supervisor made the employees choose to leave the firm before the merging even started.

Similar situations may occur in a military unit, for example, if the unit is regularly tasked with difficult and high-risk missions, while other units of the same battalion are not. This can cause tension which would most likely have a negative effect on the emotional status of the personnel. If the leader does not take into account the feeling and emotions that the troops are dealing with while planning the next operation, they might find themselves with a unit that is no longer a team, but people put together by a formality. Unlike firm employees, military personnel can't quit their job whenever they like, but if the climate in the unit is not suitable and they do not feel appreciated they can try to transfer to a different unit or leave the service at the earliest opportunity.

"When employees believe they are being treated fairly – when they feel heard when they understand how and why important decisions are made, and when they believe they are respected – their companies will benefit." [3] Leaders' Empathy is one of the things that hold groups together and what makes individuals feel an important part of something bigger. Taking time to listen to subordinates and understanding their emotional needs can yield long-term benefits such as developing a sense of belonging that is of extreme importance when facing difficult situations or the hardships of military service.

2.5 Social Skills

Understanding social skills might seem simple enough. Generally speaking, social skills are often viewed as acting in a friendly manner or being polite to people, but as a component of Emotional Intelligence, they are more than that. Not that individuals with developed Social Skills frequently have negative interactions with others, but the way they are communicating and the positive messages they send are pointed and with purpose. Considering this aspect as part of the behavior of managers and leaders, one can be sure that good working relations help in convincing the superiors, the peers, and the subordinates and making them more likely to agree with one's point of view or proposition.

People with good Social Skills tend to have a wide circle of contacts and the ability to find common ground with others thus creating relations. This way of thinking and acting is not just socializing, it aims at crafting a network that could be used when needed. Successful leaders understand that working alone is not only difficult but if one is pursuing a goal, achieving it without the support of the people involved in the work process is almost impossible.

Social Skills are a result of practicing and applying other components of Emotional Intelligence, so when giving examples of good Social Skills at action, they would seem familiar. When leaders use their Social Skills to better manage their teams – that is their Empathy working. The same thing applies when they use their Self-Awareness, Self-Regulation, and Empathy to persuade someone to accept their point of view. Relying on their Social Skills, managers know not only how to convince or affect someone, but the best time to do so in order to produce maximum result and create a well-performing team or unit.

In 1993, a chief of a planning department in a computer manufacturing company was convinced that the future of the company was the Internet. The chief used his contacts with employees in other departments and sections and created an informal virtual network that was not regulated by the company's top management. Then they proceeded with registering the company as a participant in the annual conference of the Internet industry. In less than a year, the head of the company created a new Internet department and the chief of the planning department was appointed to run it.

With the constant modernization of the Armed Forces and the new threats to national security, highly motivated small unit's leaders and commanders with good Social Skills would be the

perfect candidates for leading newly formed units tasked with testing new equipment or training for the execution of unconventional tasks or missions. Such commanders and leaders would aim at achieving results by increasing performance and pushing their subordinates hard towards success.

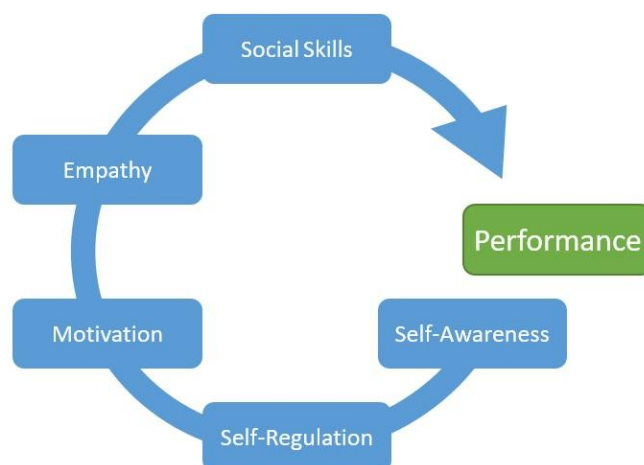


Fig. 3 Result of completing the cycle of Emotional Intelligence.

3. Conclusions

What Goleman says about the correlation between IQ and success may not be an axiom, but one can clearly see that there is reason in his theories on Emotional Intelligence. "We've known for years that Emotional Intelligence improves results – often by an order of magnitude." [4]

Based on the examples and suggestions given above, we can claim with a degree of confidence that a parallel between business managers working with people and military commanders and leaders serving in a tactical unit can be drawn. So if the civilian organizations can benefit from implementing the components of emotional intelligence in their affairs, so can the Armed Forces.

A small unit's commander who is self-aware and motivated, capable of self-regulation, exercises empathy and possesses social skills can achieve more than their peers and create a healthy working environment for their subordinates.

By including topics connected to the practical applications of Emotional Intelligence in officer's training, we can observe its effects on the unit's performance in the not-so-distant future.

4. References

1. D. Goleman, Harv. Bus. Rev., *What Makes a Leader?*, (2004)
2. T.Sy, S. Cote, J. Appl. Psychol., **Vol 90**, *The Contagious Leader: Impact of the Leader's Mood on the Mood of Group Members, Group Affective Tone, and Group Processes* (2005)
3. J. Brockner, Harv. Bus. Rev., *Why It's So Hard to Be Fair* (2006)
4. D. Goleman, R. Boyatzis, A. McKee, Harv. Bus. Rev., *Primal Leadership: The Hidden Driver of Great Performance* (2001)

Tactical efficiency in the process of handling and usage of firearms – important security related precondition for carrying out the police duty

Jonce Ivanovski, Aljosa Nedev

University "St. Kliment Ohridski", Faculty of Security - Skopje, Republic of North Macedonia

E-mail: ivanovskijonce78@gmail.com; aljosanedev@yahoo.com

Abstract: *The police, during the performance of its duties, bears a huge responsibility before the general public, in relation to the professional performance of their duties, without causing disturbance of the general security and violating the basic human rights and freedoms. Forming the public opinion on the quality of police services is directly related to the manner in which legal powers are exercised, and in particular, the part related to the use of means of coercion. Firearms as the most extreme form of coercion are of great importance for the police work, because its use can cause serious injury or death, so it should be used only when there are absolutely no other options to solve the conflict between the police and the citizens. Given the different circumstances and conditions under which firearms are used, the police officers have a tremendous responsibility to anticipate, understand and apply all legal, security and tactical procedures and rules for the reasonable use of firearms. That is the main reason why the focus on this paper is on the tactical and security related procedures, which include a number of activities related to the process of preparation and taking up arms, the process of immediate use of weapons and the final process of disarmament.*

Keywords: POLICE AUTHORIZATIONS, POLICE OFFICERS, USE OF FIREARMS, TACTICAL PROCEDURES, SECURITY ASSESSMENT

1. Introduction

The police, as a state body, is authorized and in charge of maintaining public order and peace. This position of the police arises from the established powers, which are necessary for the performance of its basic function, which is to maintain internal security and preserve the constitutionality and legality of the social order [1]. Among most of the police duties, the authorization to use means of coercion stands out by its weight, because their application directly restricts, and in severe cases violates the constitutionally guaranteed human rights and freedoms, and especially the right to freedom of movement, bodily integrity and of life. The seriousness of the consequences that can result from the use of means of coercion, and especially from the use of firearms, categorizes the police profession as a high-risk and responsible profession, in which the lives of people on the one hand and the lives of police officers on the other hand can be easily endangered [2]. Therefore, the use of firearms by the police should be seen as an exception in its conduct, and not as a rule, because it is an authorization whose use almost without exception has serious consequences.

Due to the great importance and significance of the use of firearms in everyday police work, the assumption is justified that the use of firearms is an extremely serious and responsible activity that requires professional experience, knowledge and skills, but also great concentration in crucial moments (stress control, fear). That is why many studies have been conducted in which firearms are analyzed from different aspects (sociological, criminological, psychological, legal, tactical-security, educational, etc.), and thus various theses and questions about its legality, justification, usability, proportionality, limitation, efficiency, etc. [3] [4] [5].

2. Legal basis for the use of firearms

Firearms, as the most severe form of coercion, have stricter legal restrictions on their use than other means of coercion. This means that during the performance of their official duties, police officers may use firearms only in cases when otherwise and by using other means of coercion is impossible [6]:

- to protect their own life or the lives of other people;
- to prevent the commission of a crime for which a prison sentence of at least four years may be imposed;
- to prevent the escape of a person who have committed a crime for which a sentence of ten years or a heavier sentence may be imposed or a person for whom a warrant has been issued for such a crime;
- to prevent the escape of a person deprived of liberty due to a crime committed from the previous point or a person for whom a warrant has been issued for escape from serving a prison sentence for such crimes, and

- To prevent an attack on a facility or person being under protection.

Taking into consideration the legal basis, it can be said that any use of firearms is considered potentially deadly, as it can kill or seriously injure the participants involved in the attack or the individuals who accidentally found themselves at the scene of an armed shootout. In such complex and uncertain situations, the police practice shows that the decision for its application is always difficult and complicated because at the same time care should be taken not to endanger one's own life, the lives of other colleagues, citizens, but also the lives of people who are conducting the attack.

Firearms, as the most severe form coercion, is a serious challenge to the expertise, ethics and ability of every police officer, and therefore it is in the interest of the state to define the legal basis as accurately as possible so that citizens can experience the police as a figure of security and protection, not as an immediate and direct threat to their lives [7].

3. Tactical and security procedure during the use of firearms

3.1. General tactics and safety rules

When using firearms, the legal regulations should be well known. Furthermore, the police officers have a huge responsibility to anticipate, understand and apply all security and tactical procedures and activities as long as they are conducted reasonably and adequately. This implies the application of an appropriate tactical approach that is in accordance with the prescribed security procedures, as consequences can easily occur as a result of improper and inadequate use of firearms [8]. In practice, this means that in a very short period of time they have to perform a number of tactical activities and actions related to the process of preparation and taking up arms, the process of direct (physical) manipulation of weapons, the executive process of disarmament. While carrying out these three interrelated processes, police officers need to maintain a high level of concentration and demonstrate motor skills to quickly, efficiently and safely execute all crucial elements of the overall tactical process [9]. Depending on the conditions and the reasons why the firearm is used, one should always strive for the final outcome to be favorable, i.e. not to allow unnecessary damage, because the bullets can cause severe bodily injuries or take human lives. To prevent this from happening, police officers must make logical judgments and make decisions that are consistent with the current security environment, and therefore must strictly adhere to certain rules for the safe handling of firearms. We are talking about the application of four basic safety rules [10]:

Rule 1: Treat each weapon as if it were loaded. There should be no exceptions to this rule whatsoever, as it is always assumed that the weapon is loaded. If you come in contact with the weapon, you should check if there is ammunition inside. The check is performed

by removing the frame (charger), pulling (blocking) the cover in the rear position and inspecting the opening of the tube. In case you need to check a weapon that is unfamiliar how it works, it should be done only in the presence of a person who is trained to handle that weapon.

Rule 2: Never point a firearm at something you do not want to destroy. You should never allow the tube opening to pass through any part of your own body or any other body. Basically it is very difficult to find a completely safe direction, except maybe the back of the shooting range. In other words, firearms should be aimed at something that will absorb and retain the bullet in the case of an accidental firing.

Rule 3: Do not put your finger on the trigger until you intend to shoot with a firearm. Many police officers think that the finger should be constantly on the trigger so that they can fire the weapon faster, which is not true, because it can be fired equally quickly if the finger is outside the trigger frame. This rule is often violated in situations when the weapon is returned to the holster and therefore causes wounds and injuries to the body.

Rule 4: Be always sure about your target and what lies behind it. Before the weapon is used, the target must be clearly visible and positively identified. This rule requires police officers to be firmly convinced and confident that there are no random observers in the area around the threat and behind it, i.e. citizens. In most cases when firearms are used, the reaction time is very short, so it is crucial to properly assess the situation before making a final decision on action.

3.2. Preparation, pulling out, using and returning the weapon in the holster

Police officers carry weapons while performing their professional duties [11]. Firearms (semi-automatic pistol) as well as other equipment are on the service belt. The holster in which the weapon is placed is always on the side of the hand with which the shot is fired, while the holster with a spare frame is carried on the opposite side of the belt. This placement of the gun and the spare frame at all times should ensure their availability and the possibility of quick use regardless of the conditions in which it operates. When starting the procedure of pulling the weapon out of the holster, the main priority is to bring it to the firing position, i.e. to aim at the final target. To achieve this, several consecutive steps are required through which the tactical task will be performed efficiently and safely (Fig.1) [12]:



Fig. 1 Pulling out a gun from the holster

First step. The hand that shoots covers the handle of the gun, the thumb unbuttons the holster, and the finger that shoots is straight along the outside of the holster. The other hand comes in contact with the service belt to facilitate the extraction process. While performing these initial interventions with the gun, a preparatory firing position is taken and the threat is identified with both eyes.

Second step. The firing hand lifts the pistol out from the holster, then immediately directs the opening of the barrel at the auxiliary hand to make a firm grip with both hands. While establishing a proper grip with both hands, the gun is aimed at the ground at a 45-degree angle. In this position the auxiliary hand grabs the cover and pulls back (repeats) to charge the gun.

Third step. The hand that pulls the trigger and the other hand together point the gun directly at the target, i.e. to a position of complete alignment of the front and rear sight. During this process,

the finger that is supposed to pull the trigger is placed outside the frame of the gun.

Fourth step. Direct the opening of the gun straight towards the target (aim at the target) and pull the trigger with your finger. After firing, the gaze is kept on the threat for a short time to provide a realistic insight into the shot, and then the finger is removed from the trigger.

After pulling out the gun from the holster, the procedure for safe return of the weapon follows. In order to facilitate the process of putting the gun back in the holster, it is necessary to perform the sequence of steps in the opposite direction. When returning the pistol, it is very important to remove the finger with which the trigger is pulled at the same moment when the target is no longer a threat and to activate all safety mechanisms.

3.3. Tactical views on the use of firearms

The specific manner and conditions in which firearms are used impose the need to establish appropriate tactical attitudes for firing. To achieve accuracy and ensure timely feedback, police officers must have a stable and balanced firing position. This means that before the weapon is aimed at the target, police officers must involve the whole body, i.e. provide skeletal support (simultaneous involvement of multiple groups of joints), muscle contraction (synchronized work of multiple muscle groups), full body kinesthetics (harmonized work and body function) and natural target point (alignment and centering of targets after a shot) [13].

When firearms are used, tactical attitudes can be formed for shooting in a standing, kneeling and lying position. Which of these shooting positions will be used at a given time depends on the security circumstances and situation in which the police officers are. In a standing position, the most acceptable for tactical and combat shooting are the positions "isosceles triangle" and "vivar position" because they provide good stability, balance and maximum involvement of the whole body (Fig. 2) [14].



Fig. 2 Standing positions for shooting "isosceles triangle" and "vivar"

Tactical attitude shooting in the kneeling position can be from a low and high kneeling position. When a low shooting position is applied, then positions are formed on one or both legs by leaning on the knee with the arm, sitting on one or both heels, and when a high shooting position is used, then the body is kept upright all the time, regardless of the position of the shooting legs (Fig. 3).



Fig. 3 Squatting positions for shooting in low and high position

When the body is brought to a supine position, shooting positions can be performed by lying on the abdomen, side and back (Fig. 4).



Fig. 4 Lying postures for shooting the abdomen, side and back

3.4. Tactical movements with firearms

When the legal requirements for the use of firearms are met, police officers apply a variety of tactical movements in space in order to quickly, efficiently and safely overcome the resulting danger. If we take into account that when performing police tasks, most of the time is spent in tactical movement with firearms and less in shooting, then these movements must be well practiced, because it will enable a timely and quick reaction (taking a safe shelter, running, lying down, twisting, changing running direction, etc.). When performing a tactical movement with a firearm, the position of the body is constantly changing and adjusting depending on the configuration of the terrain, the degree of danger, weather conditions, equipment and in such changing circumstances, the movements are usually performed in a standing or lying position [15] [16].

If the tactical movement with a firearm is performed in a standing position, then it is performed with a straight line movement forward, backward and sideways and with alternating change of direction of movement in one side and the other (Fig 5). During the whole time this process is repeated, the weapon is raised to shoulder height and it is ready for use.



Fig. 5 Tactical movement with a firearm in a standing position

In the supine position, the tactical movement with a firearm is performed in several ways, with crawling lowly on the abdomen, side, back and crawling of the forearms and palms (Fig. 6). When crawling in the supine position, the weapon is held with the stronger hand in the direction of the determined target.



Fig. 6 Tactical movement with a firearm in a supine position

4. Conclusion

In most of their work, police officers use their powers to act in police interventions in cases where there are reasons for suspicion that a crime has been committed or the public order has been disturbed, and it often happens that in those interventions they use means for coercion. Due to the nature and severity of these situations, which can be extreme and extremely tense, the need to use firearms inevitably arises. Given that this means of coercion directly endangers the rights and freedoms of all human beings, proper and professional action should enable the narrowing of the space for discretionary decision-making, and increase the tactical and security efficiency that is crucial to exclude illegality and criminal liability of the police. Therefore, in the daily police action, the knowledge of the legislation regarding the use of firearms should help for a timely tactical response that includes the

application of a number of activities and actions with weapons in order to protect the personal safety of police officers and protect the life and health of the policemen and citizens.

5. References

1. Закон за полиција, Службен весник на Република Македонија, 114/2006.
2. Ivanovski J, Nedev A. Usage of coercion means for protection of the personal safety of police officers, International Scientific Conference, The Balkans between Past and Future: Security, Conflict resolution and Euro-atlantic Integration, 1, 2013, 279-290.
3. Žaberl M. Policijska uporaba strelenega orožja in načelo sorazmernosti, Varstvoslovje, 4, 2002, 340-346.
4. Ivanovski J, Rajkovchevski R. Testing the police model for the handling and use of firearms against non-police subjects, International Journal of Police Science & Management, 3, 2015, 1-6.
5. Gligorov S. Affection of some biomotor tests under the success on some situation problems at selected subjects of special police forces in Republic of Macedonia, Physical culture, 1, 2004, 113-116.
6. Krstevska K. Upotreba sredstva prinude prema makedonskoj regulativi, Časopis za pravnu teoriju i praksi: Pravni život, 2009, 795-806.
7. Мурговски Б. Меѓународните стандарди и компатибилноста на националните законски основи за употреба на средства за присила и огнено оружје, Годишник на Факултет за безбедност, 1, 2009, 151-163.
8. Ивановски Ј. Тактика на полициско постапување при употреба на средства за присилба, Скопје, Факултет за безбедност, 2019.
9. Officer Survival Guide - 11 Officer Defense Tips & Tactics files.policemag.com/documents/police-magazine-officer-survival-guide.pdf [15.3.2021].
10. Maršić M, Ljubić T, Britevac A. Evaluacija dvije metode nastave za sigurnost rukovanja vatrenim oružjem, Policija, sigurnost, 1-2, 2008, 16-26.
11. Правилник за начинот на вршење на полициските работи, Службен весник на Република Македонија, 149/2007.
12. How to Shoot a Handgun (with Pictures)-wikiHow http://www.wikihow.com/Shoot-a-Handgun#Learning_Basic_Handgun_Skills_sub [21.2.2021].
13. Basic Pistol Shooting Techniques.indd - Law Enforcement Services, LLC [w.lawenforcementservices.biz/Basic%20Pistol%20Shooting%20Techniques.pdf](http://www.lawenforcementservices.biz/Basic%20Pistol%20Shooting%20Techniques.pdf) [21.3.2021].
14. McLaughlin C. The Weaver system techniques for handgun combat, International Defence Review, 3, 1988, 267-270.
15. Suarez G. The tactical advantage: A definitive study of personal small-arms tactics, Paladin Press, Colorado, 1998.
16. Shooting from Cover and Concealment https://fortress.wa.gov/cjtc/www/1/level_i_section_8_manual_revisions.pdf [12.2.2021].

Steganographic algorithm using the different color components of a 24-bit image

Veselka Stoyanova¹, Ilian Lilov²

National Military University, Faculty of Artillery, AAD and KIS, Shumen, Bulgaria¹

National Military University, Veliko Tarnovo, Bulgaria²

veselka tr@abv.bg

Abstract: The article deals with the steganography system which hides text inside images without losing data in components of RGB model. The secret message is hidden in the cover image using Least Significant Bit (LSB) algorithm. The comparative results for the proposed algorithm are very promising for blue components of image. To evaluate steganography system properties are used the measures like Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PRSN), Mean Squared Error (MSE) and Structural Similarity Index for measuring (SSIM). The aim of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it is hidden the same information, but in a different color channel, to determine which color channel shows the most invisibility to others and is it advisable to be used in the transmission of confidential information.

Keywords: STEGANOGRAPHY, LSB, RGB, IMAGE

1. Introduction

Development and improvement of information and communication technologies create the establishment of a global digital environment, they offer new opportunities for the restoration of personal, business and institutional communication and interaction, predetermining various limitations.

A matter of ensuring the secure and hidden transmission of information with extremely up-to-date and subject to much research.

Steganography is the art and science of hiding messages inside a digital medium in such a way that only the sender and the receiver, can view the hidden message [7],[8]. However, the *steganographic capacity* is the maximum number of bits that can be embedded in a given cover image with a negligible probability of detection by an adversary[9]. Therefore, the embedding capacity is larger than the steganographic capacity [10]. Steganography modification principle [2] is used to implement the functions of embedding and retrieving data in the cover image, where the pre-existing cover images are changed during the process of embedding. An algorithm is used for insertion into the LSB (Last Significant Bit) for hiding information in image [1], [2], [7]. Through the LSB method is obtained embedding of the message bits in the last significant bits of the color components of individual pixels of the image. It is symmetrical, which means that for embedding and extracting a message, identical operations are performed in the same order. The effect of the algorithm is based on the fact that the secret information is stored in the last significant bits of the pixels of an image, without causing visible differences in its view [1]. It's even a way to transmit information between different groups with dangerous ideas for national security [6]. Steganalysis is used to detect the stego objects and extract the secret messages.

Fig. 1 illustrates some essential factors in Steganography.

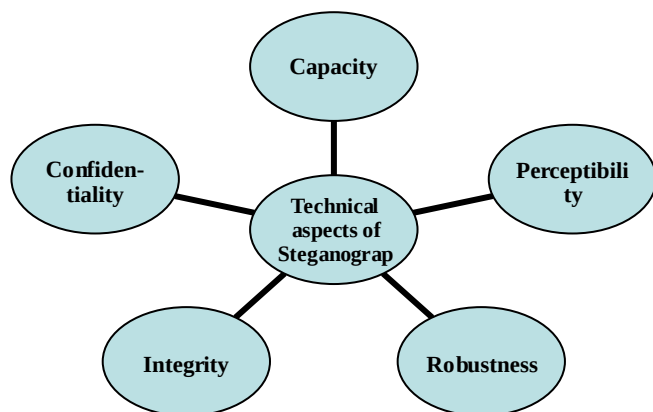


Fig.1 Some factors that we should consider while evaluating a Steganography algorithm

2. Steganographic algorithm using the different color

Color images have 3 color channels that can be interpreted in different ways. After preparing the cover image to hide confidential information in it is necessary to select an algorithm by which to perform the hiding. An RGB image has three channels: red, green, and blue. The algorithm allows to manipulate the individual color channels independently, hiding information separately in each of them or realizing combinations of the three possible color channels. This algorithm reduces the maximum capacity of the hidden information in cases where only one of the color channels (red, green or blue) or a combination of two of them is used. Fig. 2 shows a scheme of hiding information in all three color channels.

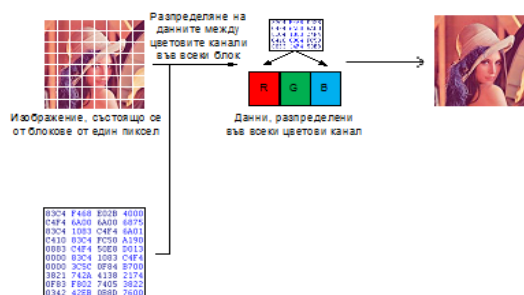


Fig. 2 Hide information in the three color channels

If 1 byte of information can be hidden in three pixels when using all three color channels, the same amount of information will be hidden in eight pixels if only one color channel is used. Fig. 3 shows how to hide one byte of information only in the blue color component.

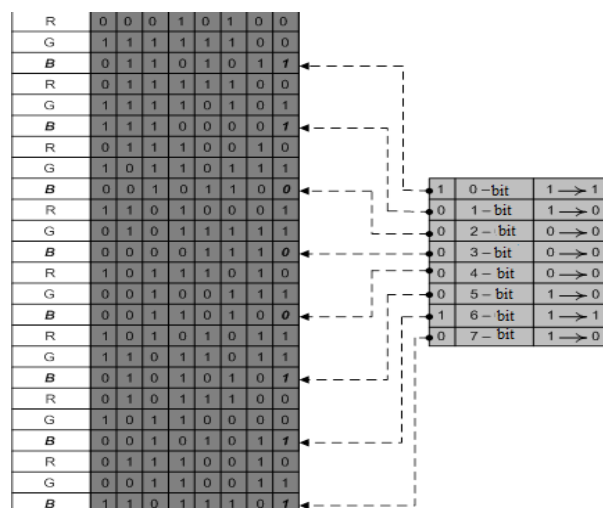


Fig. 3 Scheme for hiding information in the youngest bits of the blue color channel

If this algorithm is combined with an algorithm that allows more than one lower bit to be used in the color channel of the pixel, such a reduction in the size of the hidden data will not be observed. In this case, the capacity to hidden information in an image will increase proportionally, but this will be at the expense of its quality.

The aim of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it has hidden the same information, but in a different color channel, to determine which color channel shows the most invisibility to others and it is advisable to be used in the transmission of confidential information.

The characteristics studied are represented by formulas (1) and (2), the PSNR is based on values obtained for the MSE:

$$(1) \quad MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2,$$

Where m and n are the width and height of the image; $I(i, j)$ and $K(i, j)$ are relevant pixels with coordinates (i, j) in the original stego-image.

$$(2) \quad PSNR = 10 \cdot \log_{10} \left(\frac{max^2}{MSE} \right) = 10 \cdot \log_{10} \left(\frac{max}{\sqrt{MSE}} \right),$$

where $max = 255$ for 8 bit images[1].

The SSIM index (Structural Similarity Index for measuring) is similar to the MSE and the PSNR, but is designed to improve them both. As an indicator it measures changes in brightness, contrast and structure of an image. In [3], the brightness, contrast, and the value of structural similarity are represented. Average value for the SSIM index

$$(3) \quad SSIM(x, y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [s(x, y)]^\gamma,$$

Where $\alpha > 0$, $\beta > 0$ and $\gamma > 0$ are parameters which determine the relative importance of the three components in the value of the $SSIM(x, y)$. In the article was accepted equal importance of brightness, contrast and value of structural similarity, i.e. $\alpha = \beta = \gamma = 1$ and $C_3 = C_2/2$.

3. Experimental results.

The proposed algorithm can work with BMP, PNG and TIFF file formats of images without size limitations. Since it does not have a block for pre-compression, the maximum amount of information that will be embedded in the image is determined depending on the size of the carrier file minus the information in the header file (service information), while also allocating bytes for the generated code of the password.

By implementing a program system for embedding/ extracting text messages many tests with different size messages and images have been carried out. The studied algorithm is based on the LSB method applied and tested on BMP image formats. Test results of the qualitative characteristics MSE, SNR, PSNR, SSIM and E are analyzed. Visual analysis of the compared images shows lack of visual differences in visual control. Histogram analysis and the results of the qualitative characteristics are obtained by MATLAB.

The amount of the stego-file is the same as that of the carrier file. A stego-key can be typed in the algorithm

We have tested the proposed algorithm for around 20 different cover images of BMP format. Every pixel contains 24 bits (for 8-bit representation) each one as 8 bit components in pixel. In the proposed method, all the three components have been used for data embedding. First, each color component from a pixel is separated and three separate $M \times N$ matrix is obtained. The purpose of the study is to determine whether there is a change in the qualitative characteristics of the stego image, when it was hidden the same information, but in a different color component, to determine which of them shows the greatest invisibility to others and it is advisable to be used in the trans. Table 1 presents the results for the studied quality characteristics in hiding 60 kB information. One of the least

significant bits is used to hide the information and these settings are combined with the selection of the three color components of the individual pixels of the *Parrots.bmp* image alone or in combination.

Table 1: Investigated quality characteristics when hiding 60kB text in Latin, using a different combination of color components in the pixels in the image *Parrots.bmp* use the one LSB

Nº	LSB	Color component	MSEavr	SNR	PSNR	E
1.	1bit	RGB	5,05765e-4	64,5345	71,2806	7,6201
2.	1	Red	1,344 e-4	74,2082	80,9543	7.6200
3.	1	Blue	1,3413 e-4	74,3955	81,1416	7.6200
4.	1	Green	3,477e-4	74,2205	80,9666	7.6201
5.	1	RG	7,579 e-5	74,2400	80,9861	7.6200
6.	1	RB	7,587 e-5	74,3261	81,0722	7.6201
7.	1	RG	0.000072	74,3534	81,0995	7.6200
8.	1	BG	0.0004199	64,8525	71,5986	7,6201

Table 1 shows the comparative results with three different color components and RGB combination using the one LSB. The results in Table 1 correspond to those presented in Fig. 4 and fig. 5, from which it can be easily established and concluded that the blue color channel has the best performance in combination with the use of only one low bit.

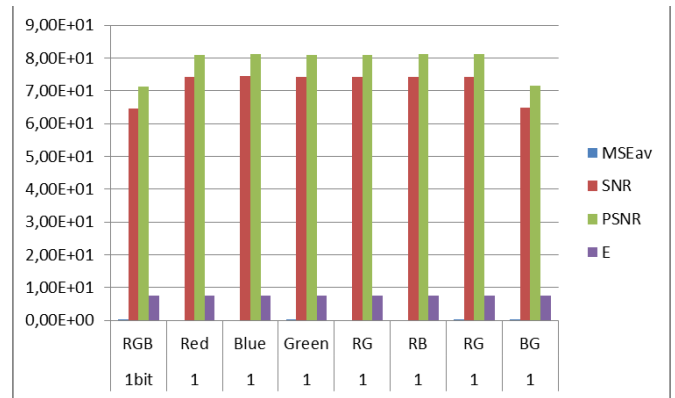


fig.4 Diagram of quality characteristics for evaluation of the hiding of 60kB text in Latin, in different color channels in *Parrots.bmp*

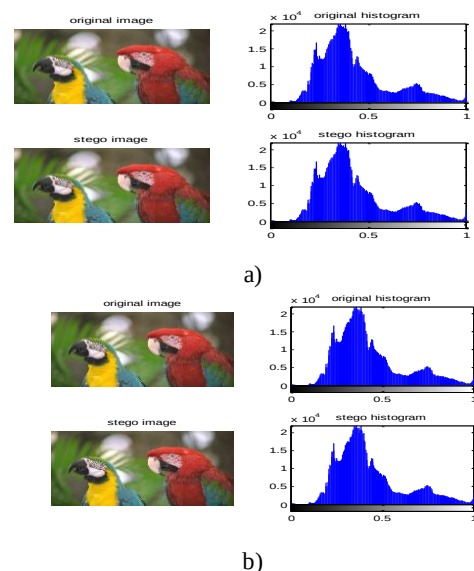


fig.5 Presentation of original and stego image of *Parrot.bmp* and their histograms, with embedded a) 40kB and b) 60kB information

Table 2 shows the comparative results with three different color components and RGB combination use the two LSB.

Table 2: Investigated quality characteristics when hiding 60k B text in Latin, using a different combination of color components in the pixels in the image *Parrots.bmp* use the two LSB

№	LSB	Color component	MSEavr	SNR	PSNR	E
1.	2	RGB	0.0004786	64,1356	70,8817	7.6201
2.	2	Red	3,3002 e-4	70,9295	77,6756	7.6200
3.	2	Blue	4,2566 e-4	70,7788	77,5249	7.6201
4.	2	Green	3,0825e-4	71,1253	77,8714	7.6200
5.	2	RG	1,756 e-4	70,8061	77,5522	7.6200
6.	2	RB	1,756 e-4	70,8809	77,6270	7.6200
7.	2	RG	0.0001801	70,8915	77,6377	7.6200
8.	2	BG	4,884 e-4	64,6990	71,4451	7.6201

Fig. 6 presented PSNR between cover image and stego-image, and corresponding to the results in Table 2.

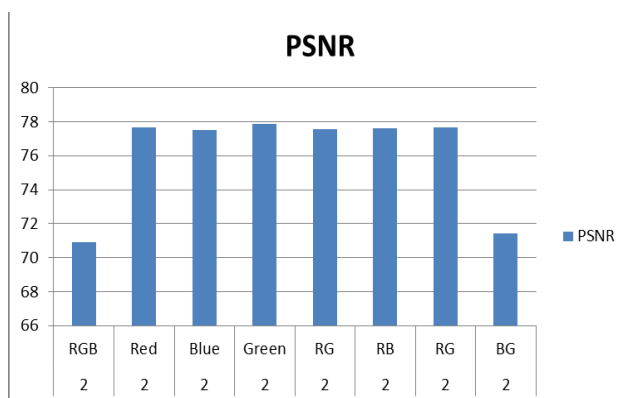


fig.6 Diagram of PSNR for evaluation of the hiding of 60kB text in Latin, in different color channels in *Parrots.bmp* use the two LSB

From above experimental results, it is apparent that each stego-image is almost analogous to corresponding cover image and shows better imperceptibility. That is deterioration of the quality of images due to the embedding of the secret messages cannot be distinguished.

Steganalysis intends to find the secret information that carries some stego-information by attacking the security of the used steganography algorithm[9]. Best images to hide information in them are Bitmap 24 bit images since they are considered as the largest and highest quality image file types. When an image has a high image quality and capacity, the information can be easily hidden[11].

4. Conclusion

Data hiding is a challenging and most important task in the field of information security.

The results from the research can be summarized in the following conclusions about the characteristics of the studied steganography algorithm:

It is noticed that the blue color channel has the best qualities compared to the other two (red and green) when using the one LSB, although the difference is only one in the indicator, it is with about 0.2% better values. But when we use the two LSB it is noticed that the green color channel has the best qualities compared to the other two (red and blue).

The research was carried out using different dimensions of the hidden data. It should be noted that files larger than 60 kB can hardly be hidden in just one color components.

It could be recommended when using the algorithm with different color channels, which is applied mainly to blue color, examining the best characteristics of the stego image.

Moreover, proposed method extracts the hidden secret message efficiently without using the range tables

5. References

1. Stoyanova,V. and Zh.Tasheva, *Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images*, Machines. Technologies. Materials.Vol. 9 (2015), Issue 7, pg(s) 65-68., <https://stumejournals.com/journals/mtm/2015/7/65>
2. Cole, E., „*Hiding in Plain Sight: Steganography and the Art of Covert Communication*“, Wiley Publishing, Inc., Indianapolis, Indiana, (2003)
3. Wang Z., A .C .Bovik, H. R. Sheikh, and E. P. Simoncelli. “*Image quality assessment: From error measurement to structural similarity*,” IEEE Trans.ImageProcessing,vol.13, Jan.(2004)
4. Tasheva, Zh., and A. Tasheva. “Combining cryptography and steganography in software system for hiding confidential information.” Journal Science Education Innovation, Association Scientific and Applied Research Vol. 1, 2013, pp. 84-92 (2013)
5. Димитров, Д., *Използване на полюсни модели за формиране на базисни функции*, Сборник научни трудове, Шуменски университет, т 2, с.394 – 397, Шумен, 2009, ISBN:978-954-577- 549-6.
6. Atanasov, A., *Бежанската вълна от Сирия – заплаха за националната сигурност*, II International Scientific Conference ConfSec18, Borovec, Year 2, ISSUE 1(3) ISSN 2603-2945 (print), ISSN 2603-2953 (online)
7. H. Abdulrahman, M. Chaumont, Ph. Montesinos, B.Magnierhttps, Color Image Steganalysis Based On Steerable Gaussian Filters Bank, IH&MMSec: *Information Hiding and Multimedia Security*, Vigo, Spain. pp.109-114, Jun (2016), [ff10.1145/2909827.2930799fm /hal.archives-ouvertes.fr/hal-01374101/document](https://hal.archives-ouvertes.fr/hal-01374101/document)
8. G. Kumar and A. Rana, “*Data hiding techniques in digital multimedia*,” International Journal of Engineering Science Invention Research and Development, vol. 1, pp. 333–337, 2015.
9. A. Soria-Lorente and S. Berres, A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information, volume 2017, <https://doi.org/10.1155/2017/5397082>
10. S. Sachdeva, A. Sharma, and V. Gill, “*Colour image steganography using modified JPEG quantization technique*,” International Journal of Latest Research in Science and Technology, vol. 1, pp. 1–5, 2012.
11. A. Nejahi, F.Z. Boroujeni, *The Improvement of Steganography Function Based on the Least Significant Bit in RGB Color*, American Journal of Software Engineering and Applications, Volume 5, Issue 3-1, May (2016).

Means and ways of destruction of explosives and materials

Damyanova Liliya ¹

Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences, 67
Shipchenski Prohod Street, 1574 Sofia, Bulgaria
lilydamyanova@gmail.com¹

Abstract: The report discusses the main tools and methods for destroying explosives and materials. A comparison of blasting methods is made. The requirements for ensuring safe working conditions during the destruction of explosives and materials are considered.

Keywords: DESTRUCTION OF EXPLOSIVES, BLASTING METHODS, SAFE WORKING CONDITIONS

1. Introduction

The buildings for production and storage of explosives and materials are subject to numerous requirements in terms of construction of buildings, quantity of explosive materials, as well as distances from sites to neighboring buildings and facilities. These requirements arise from the risks and hazards, as well as from the damage that would occur in the event of an unwanted explosion of explosives and materials. [1,2,3]

The conditions and procedures for production, marketing, acquisition, storage and use, scrapping and destruction of explosive substances, pyrotechnic devices, weapons, as well as utilization of weapons and ammunition are regulated by the Law on Weapons, Ammunition, Explosives and fireworks products (WAEFP).

Utilization of weapons is a process of irreversible transformation by dismantling, in which the respective arms are crumbling to the constituent its elements, which then are fit for use for the purpose. Disposal of ammunition is a process of irreversible transformation via destroying of individual constituent elements with the subsequent use of waste propellant, explosive substances, empty packaging, ferrous and non-ferrous metals.

The report examined the main means and methods to dispose of explosive substances, pyrotechnic devices, weapons and ammunition themselves and need to respect the basic rules for safety in activities related to their destruction. [4.5]

2. Basic ways of exploding ammunition, explosives, materials and pyrotechnics

In practice these are established methods for blasting of WAEFP:

- through and preparation of militants and their transportation;
- Detonation with detonator capsule and fire-conducting cord (fire explosion);
- Blasting with detonating cord;
- Blow blasting with an electric detonator (electric blasting)



Fig. 1

-Blasting with non-electrical systems (capsule detonators waveguide). (figure 1)

The training of militants is carried out at the site of the blasting. The boxes are made on the surface, in special booths or sheds or in special chambers.

Waterproof or waterproof explosives are used to work in flooded conditions.

2.1. Detonating with a detonator capsule and a fire-conducting cord (fire explosion);

Detonation with detonator capsule fire cord (fire explosion) is allowed only in cases where no other method of detonation can be applied.

The blast uses an ignition tube that can be used for underwater detonation. In the process of production of WAEFP it is planned to use a clamping device, a special rope, a detonator. This method is applicable for detonation of both single and mass charges.

Sections of fire cord are prepared with length that provides sufficient time for the lighting of all sections and for moving the blastings on a safe distance or shelter without use of vehicles

Fire blasting is prohibited:

1. in case of blasting works in underground conditions;
2. in case of blasting of more than one drilling charge;
3. in case of detonation of charges covered with protective devices;
4. when shooting boreholes and blasting holes;
5. when the withdrawal of the detonator is difficult

2.2. Detonation with detonating cord;

When detonating with a detonating cord, the sections are joined together only in the ways specified by the manufacturer in the instructions for use (Fig. 2).



Fig. 2

2.3 Detonation with electric detonator (electric detonation);

The electric method for activating an explosive charge is effective for detonating a whole group of charges at a specific time. The use of electric blasting is carried out in an environment in which there are no stray currents, leakage currents and in the vicinity of electrical equipment, cables and other sources of electricity and hazardous electromagnetic radiation. There should be no additional safety measures such as switching off the power supply, measuring the level of strays and leakage currents, use of electric detonators with high electrical resistance, etc. (figure 3)



Fig.3

The initiation of the blasting net by a detonating cord may be performed with a detonator capsule, an electric detonator, or other means of detonation.

Electrodetonators shall be detonated by means of detonating devices providing a direct current with a pulse force and energy not less than that specified for the respective type of electrodetonators in the standard or instruction manual.

The main wires are connected directly to the terminals of the detonator without the use of additional wires.

All electrical equipment, cables, sockets and other power supply wires located within the danger zone where the electric blasting network is installed shall be disconnected from the moment the militants are trained until the detonation is completed.

3. Methods for destruction of explosives and materials

The methods for destruction of explosives and materials are chosen depending on the type of explosive and its quantity.

In practice there are two basic methods for destroying in bang substances, ammunition for weapons and pyrotechnic products, namely:

- by blasting;
- by incineration.

By blasting to destroy explosive substances which do not have lost the ability to be detonated - projectiles, mines, aerial bombs, martial parts for missiles, front parts of reactive grenades and fuses, lighters, capsules, electric detonators, and other means for blasting explosive substances.

Through combustion is destroyed explosive substances lost their ability to detonate - propellant, pyrotechnic means and compositions and munitions for weapons with a caliber up to 15 mm.

The method of disposal of explosives and materials must comply with the most appropriate method specified in the instructions for use. The destruction of explosive materials must be carried out in compliance with the requirements for explosion and fire safety and environmental protection.

For the destruction of explosives and materials, a site shall be established, which shall be provided at a safe distance, but not less than 1000 m from settlements, industrial and construction sites or warehouses for explosives. The site and 10 m around it are cleared of combustible materials so that there is no danger of subsequent fire.

3.1. Destruction by blasting

Blasting destroys capsule detonators, electric detonators, detonating cord delay devices and other means of detonation, firing explosive devices, explosives and detonating cords that have not

lost their detonation properties, as well as exuded nitroester explosives. (figure 4)

Explosives are detonated by electric detonators or non-electrical systems and with the help of munitions of suitable explosives.

When detonation minutes capability of destroying explosive materials is reduced, they detonate in the pits, as they are placed directly on the explosive material and the pits are backfilled with sand or soil. In the same way, the detonator cord delay devices, detonators and explosive devices are destroyed.

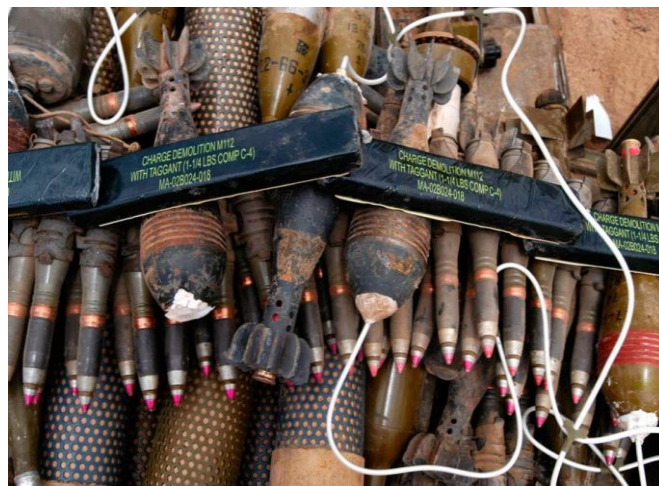


Fig.4

3.2. Destruction by incineration

The destruction of explosives is necessary to comply with the weather, it is not appropriate burning explosives in rain, wind, fog and reduced visibility.

Combustion destroys fire-conducting cords, cartridges for group or single ignition of fire-conducting cords, explosives, which have lost their detonation properties, waveguides, gunpowder, pyrotechnic compositions and products thereof.

It is not appropriate to destroy detonators, electric detonators, detonator cord delay devices and other detonators by burning capsules.

Explosives, blasting cords, ammoonitions for block or a single ignition of the safety fuses and pyrotechnics are burned separately on fires of combustible materials. The explosive cartridges are spread on the stake in a row so that they do not touch. (figure 5)



Fig. 5

4. Safety when using explosives and detonation operations

Explosives, according to the degree of danger are divided into five groups:

First group - Explosives with nitroesters content over 15% / dynamite /, hexogen, tetryl, nitropenta, octagen. When working with explosives from this group, activities with frozen and exuded explosives are not allowed.

Second group - Ammonium nitrate explosives, TNT, mixtures of TNT with nitro compounds, explosives with nitroesters content up to 15%, phlegmatized hexogen, detonating cord and others.

Third group - gunpowder, pyrotechnic compositions, fire-conducting cord and means for its ignition.

Fourth group - blasting cap, retardants for detonating cord and other means of blasting.

Fifth group - explosives, piercing hail products.

Only specially trained people are involved in the production and use of explosives and materials. Persons who come into contact with the listed substances must study the safety measures and take action in accordance with the given commands. [6, 7, 8]

Commands include:

- preparation (the substance is preparing for ignition);
- fire (ignition pipe ignites);
- distance;
- feedback (this signal is given after the explosives and charges have been detonated or neutralized).

Explosives with different hazard groups are stored and transported separately. [9, 10, 11] The joint transportation/transfer /of explosives is allowed in compliance with the following requirements:

a / the means of detonation shall be placed in the front of the vehicle in special tightly closing boxes;

b / the packages with the explosives are separated from the boxes with the means for detonation in a way, excluding their contact;

c / the packages with explosive materials shall be fastened in such a way as to prevent shocks and friction during their transportation.

Each batch of explosives is accompanied by instructions for use, which contain data on the class, hazard group, conditions of use, warranty period, rules for safe operation during storage, use and destruction. [12]

The explosives should be used, stored and destroyed at respects than the requirements specified in the instruction manual.

Explosives are not allowed to be thrown, dragged, overturned, hit or rubbed.

5. Conclusions

In order to ensure the safety of people, facilities and buildings, it is necessary to know the means and methods of destruction of explosives and materials. The main issue related to the exploitation of explosives and materials is not only their production process, but also the process of their destruction.

To reduce the risk of an unwanted explosion during the operation of explosives, it is necessary to strictly follow the manufacturer's instructions, as well as the destruction to be carried out by qualified personnel who are trained for this activity.

The results are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum Communication, Intelligent Security Systems and Risk Management (Quasar) ", which received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

6. References

1. Ordinance № RD-02-20-1 of 19.1.2017 on planning and design of constructions intended for production, storage and trade of weapons, ammunition, explosives and pyrotechnic articles (Promulgated, SG No. 11) from 31 January 2017, effective from 01.03.2017).
2. Panevski VS. The need to manage the continuity of critical infrastructure. 2019, ISBN: 978-619-188-284-7, 156
3. Panevski VS. Improving the management of business continuity of critical infrastructure by optimizing the functionality of physical protection systems. Publishing House of BAS "Prof. Marin Drinov", 2020, ISBN: 978-619-245-026-7, 192 4, 3, NTS in Mechanical Engineering, 2020, ISSN: 2535-0315, 194-197.
4. Petkov S., Petkov P., Tumbarska A .. Dynamic deformation of the cladding and the body of cumulative charges. Journal of Engineering Sciences, LVI, 3, IMSTCA-BAS, 2019, ISSN: 1312-5702, DOI: 10.7546 / EngSci.LVI.19.03.03, 24-32 National Academic Publishing House
5. Tumbarska A. Trends in the development of non-lethal weapons with kinetic (impact) action. Proceedings of the International Scientific Conference "Technology. Technologies. Education. Security
6. Yaneva S., Petrov V., Requirements for ballistic resistance of bulletproof vests arising from various international standardization documents, Sixth National Conference with international participation "Metallurgy, Hydro- and Aerodynamics, National Security '2017" 29-30.05.2017, Proceedings, ISSN 1313-8308, pp. 374-378
7. S. Yaneva, STAB RESISTANCE OF BULLETPROOF VESTS. A CONCEPTUAL MODEL OF TEST BENCH, Proceedings of VII International BAPT Conference "Power Transmissions 2020", 10-13.06.2020 Borovets, Bulgaria, Publisher: Scientific-Technical Union Of Mechanical Engineering - Industry 4.0, ISBN 978-619-7383-18- 8, pp.122-126
8. S. Yaneva, BALLISTIC RESISTANCE OF BULLETPROOF VESTS LEVEL IIIA. DEVELOPMENT OF TESTING METHODOLOGY, Proceedings of VII International BAPT Conference "Power Transmissions 2020", 10-13.06.2020 Borovets, Bulgaria, Publisher: Scientific-Technical Union Of Mechanical Engineering - Industry 4.0, ISBN 978-619-7383-18-8, p.127-131
9. Marinov G., Yaneva S .. Requirements for ballistic stability of armored vehicles, arising from GOST R 50963-96 and STANAG 4569. Comparison and analysis. Proceedings of the International Scientific Conference "Technology. Technologies. Education. Security ", 3, 4, NTS in Mechanical Engineering, 2019, 310-313 .
10. Lichkov N. G, Dimitrov DL, Mihail Hristov, Stoyanov I .. Classification of chain technology as a source of propagation of surface seismic oscillations in different types of soils .. Proceedings of the International Scientific Conference on Security "CONFSEC 2020", 4, 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 21-24 National Non-Academic Publishing House
11. Lichkov N. G, Dimitrov DL, Mihail Hristov, Stoyanov I .. Classification of wheeled vehicles as a source of propagation of surface seismic oscillations in different types of soils .. Proceedings of the International Scientific Conference on Safety "CONFSEC 2020", 4 , 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 17-20 National Non-Academic Publishing House.
12. Ivanov I, Marinov G, Current requirements to the safety means for the participants in fire extinguishing for critical infrastructure sites, 2019, III INTERNATIONAL SCIENTIFIC CONFERENCE Borovets, Bulgaria. ISSN (PRINT) 2603-2945 ISSN (ONLINE) 2603-2953, YEAR 3, ISSUE 1 (5), DECEMBER 2019, 155

Adaptive methods for detecting passive signal from an underwater object

Nikolay Gueorguiev, Alexandar Kolarov¹, Ilian. Iliev²

¹ Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences, 67 Shipchenski

Prohod Street, 1574 Sofia, Bulgaria, e-mails: niki0611@abv.bg, aleksandar_kolarov@abv.bg

² Naval Academy "N. Vaptsarov", Varna, Bulgaria e-mail: i.iliev@nvna.eu

Abstract: In order to determine the total spatial and temporal scale of the propagation of anthropogenic sources of noise, it is necessary to identify them, which can be achieved by comparing underwater and sea surface observation data. For this purpose, it is necessary to determine the direction to the noise object in a function of time. In the development of a passive hydro-acoustic system positioned on the seabed for the detection, classification and determination of the direction to an underwater object, an adaptive processor shall be designed, examined and experimented to dynamically determine the weighting factors of a two-element antenna grille according to the criteria of the minimum of the average square error and the maximum of the signal noise ratio.

Keywords: ADAPTIVE PROCESSOR, LINEAR ANTENNA ARRA, UNDERWATER MONITORING, NOISE, SPECTROGRAM.

1. Introduction

The planned measures in the Program of Measures to the Marine Strategy for Environmental Protection in the Sea Waters of the Republic of Bulgaria envisage the monitoring under indicator D11C1.1 in fulfillment of the requirements of the RDMS to be performed on the basis of the analysis of data and information to be collected in the national "noise" register. The register will describe all human activities that generate impulse sounds in the sea area of the Republic of Bulgaria. Data on noise emissions from different types of ships will be collected from ship manufacturers / owners or specialized information systems (eg national AIS system, etc.), as well as from measurements by underwater noise monitoring stations. Data and information on anthropogenic activities will be collected continuously throughout the year and the noise register will be periodically updated. As a result of human activities in the marine environment, various types of fields are excited such as sound, light, electromagnetic, thermal, hydrodynamic, etc. Of all these fields, the sound field is distributed over the longest distances from the source [3,4]. That is why great attention is paid to the assessment of the energy impact of sound waves on marine species. A harmful underwater sound field is one in which exposure causes temporary or permanent damage to the fauna of the marine ecosystem. In theory, when such a field is created as a result of human activity, it is referred to as harmful anthropogenic noise. Anthropogenic noise is recognized as a serious stress factor for most marine mammals, many marine fish, crustaceans and other marine organisms. In addition to legally regulated activities that create anthropogenic noise in marine areas, short-term sound anomalies are possible, such as the sound of leaking gas in the event of a pipeline breach, or an uncharacteristic level of anthropogenic noise in protected or prohibited areas and water activities, noise from the use of bottom trawls for fishing, etc., which may cause significant harmful effects. Their timely registration and response to the authorities authorized by law can significantly reduce the harmful consequences [5].

2. Assumptions and ways to solve the problem

As an element of an underwater monitoring system in the national marine areas, Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences /IMS-BAS/ has developed a prototype of "Audio recording system for underwater monitoring with rapid notification of detected sound anomaly" /ARSUM/ (Fig. 1), designed for recording, classification and recording of sounds from biological sources (marine mammals, fish, shrimp, etc.), anthropogenic noise - pulsed (as a result of seismic surveys, laying pylons for wind farms and platforms on the seabed, use of pulsed sonar, underwater communications, underwater explosions, etc.) or long-term (caused by shipping, dredging, leaks in underwater gas and oil pipelines, actions of power plants, acoustic signals from artificial radiation [6]. When detecting, recording and classifying a sound anomaly (eg sound of a leaking gas in the event of a pipeline breakage, noise

from the use of bottom trawls for fishing or an uncharacteristic level of anthropogenic noise in protected or prohibited areas and for certain activities in the water area and etc.) a fragment of the information is recorded, with a duration sufficient for the classification of the event [7]. This fragment is transmitted wirelessly in an autonomous beacon from the device kit, where it is overwritten. Upon completion of the information transfer process, the radio beacon floats and transmits the critical information via radio to a shore, ship or air base station acting as an operations center. It is then used as a radio beacon to indicate the location of the event.

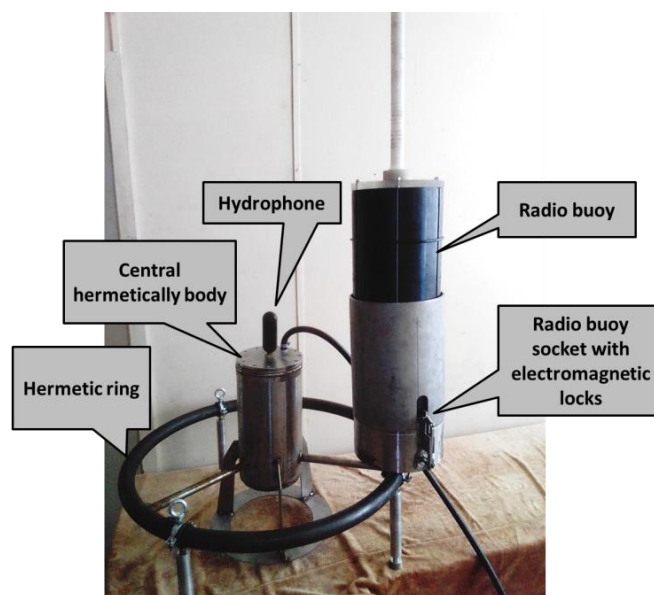


Fig. 1 General configuration of an experimental sample of ARSUM

When conducting tests with "Audio recording system for underwater monitoring with rapid notification of detected sound anomaly" it was concluded that its effectiveness is significantly increased when in addition to the information about the presence of classified noise in the area of the device is determined and the direction to it, and subsequently the vector of motion of the noise source is determined, even with tolerances in accuracy [8].

For this purpose, an experimental model of the product was developed, and in place of the hydrophone was mounted a linear antenna array of two hydrophones (for experiments - 2 microphones) - Fig.2.

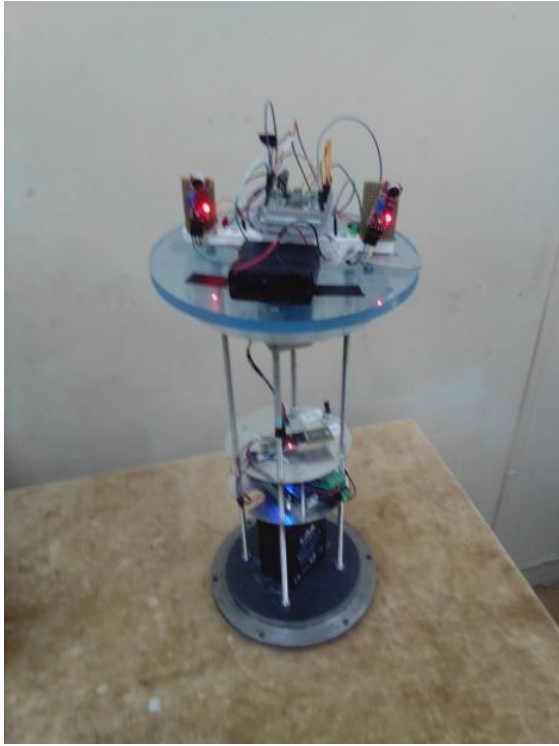


Fig.2 Electronic equipment located in the central airtight body

In order to achieve good accuracy characteristics, it was necessary to make a comparative assessment of applicable adaptive methods of beamforming using a linear antenna array for broadband signal processing [9].

3. Results and discussion

Two methods for adaptive beam formation based on the two-element linear antenna array shown in Fig. 3.

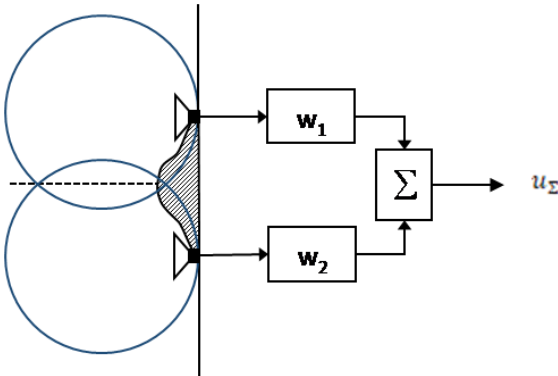


Fig.3 Two element ULA.

Adaptive beamforming methods calculate the weights w_1 and w_2 based on statistics of the signal received from the individual elements.

The first method, called "Sub band MVDR Beam former", forms the spatial beam by the method of minimal dispersion in the distortion of a broadband signal, using the technique of processing in sub bands. This type of diagram formation is also called the Capon method of beam formation [1, 2].

The second method "Sub band Phase Shift Beam former" processes the broadband signal in sub bands by introducing phase delays.

The aim of the study is to analyze their ability to detect a broadband signal against the background of their own noise and interference. The comparison of the two methods is performed by computer implementation of the algorithm shown in Fig. 4.

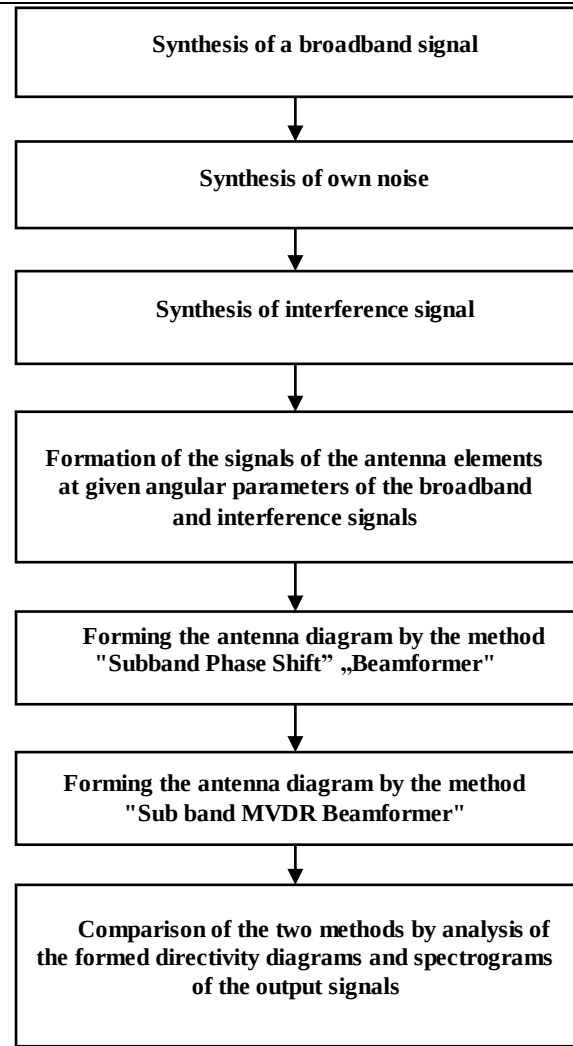


Fig.4 Algorithm for simulation of adaptive diagram formation by the methods "Sub band Phase Shift Beam former" and "Sub band MVDR Beam former"

In the simulation model, as a broadband signal (Fig. 3), a signal with linear frequency modulation with length 2 s, carrier frequency 2 kHz and frequency deviation 1 kHz is used, whose angular position relative to the perpendicular to the phase center of the antenna is 20°. The intrinsic noise of the antenna is Gaussian with a rms value equal to 0.3 of the amplitude value of the broadband signal.

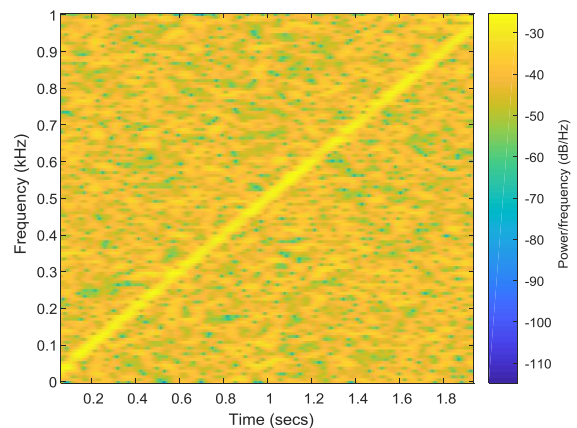


Fig.5 Spectrogram of noise signal and noise at the output of an antenna element

In the model, two interference signals with amplitudes twice as large as the broadband signal with angular positions of 10° and 30° are superimposed on the broadband signal and noise - Fig. 6.

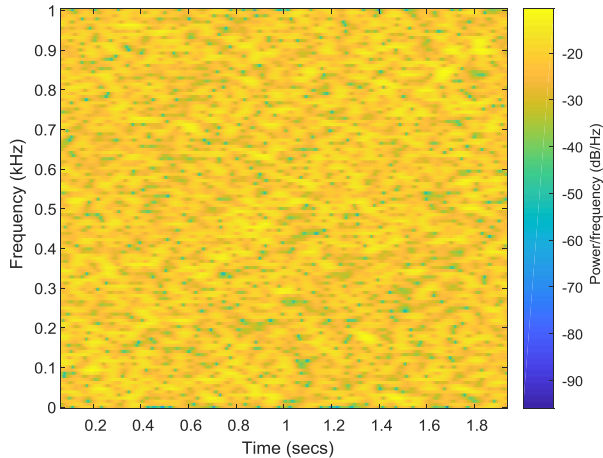


Fig.6 Spectrogram of a broadband signal with superimposed noise and two interference signals

Two non-directional microphones with a frequency band from 20 Hz to 20 kHz located at a distance of 10 cm are used as elements of the antenna array. The processing of the received signals is performed in eight frequency bands with medium frequencies 1000, 1250, 1500, 1750, 2000, 2250, 2500, 2750 Hz. For the purposes of the research the formation of the beam in a frequency band with medium frequency 1 kHz is analyzed. The obtained radiation patterns as a result of the operation of the two beamformers are shown in Fig. 7.

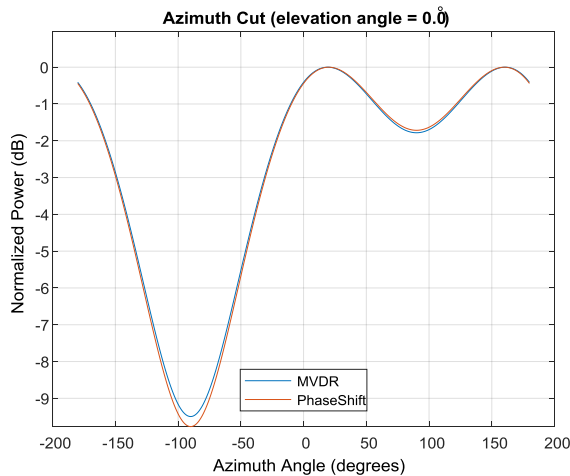


Fig.7 Directivity pattern formed by "Sub band Phase Shift Beamformer" and "Sub band MVDR Beamformer".

The main maximum of the directivity diagram is electronically directed in the direction of the 20° signal.

In the absence of an interference signal, the quality of operation of the two beam generators is identical. The advantage of "Sub band MVDR Beamformer" is manifested in the presence of interference. In this case, the average value by which the level of the output signal from the "Sub band MVDR Beamformer" beam generator exceeds the level of the "Sub band Phase Shift Beamformer" beam generator is 3.02 times.

Spectrograms of the output signals from the two beam generators are shown in Fig. 8 and Fig. 9.

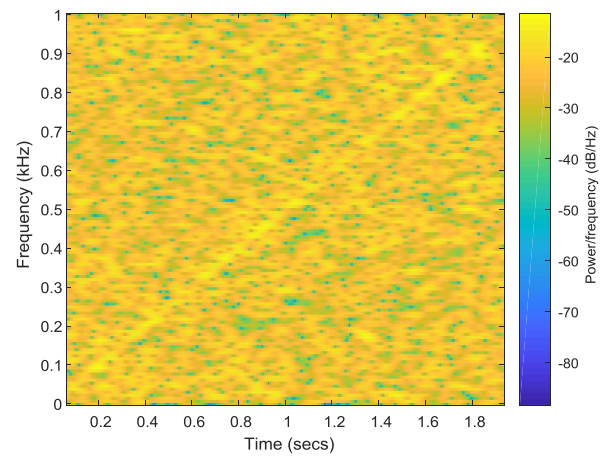


Fig.8 Spectrogram of the output signal of the antenna during interference in beam formation by "Sub band Phase Shift Beamformer"

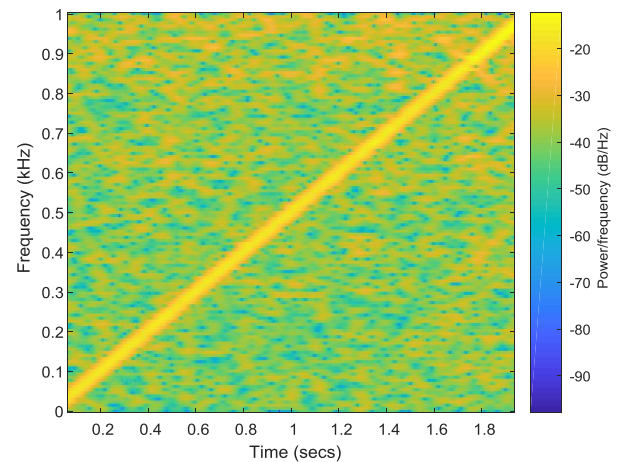


Fig.9 Spectrogram of the output signal of the antenna in case of interference during radiation formation through "Sub band MVDR"

5. Conclusion

The effectiveness of the actions taken by the authorized bodies in response to information received from the "Audio recording system for underwater monitoring with rapid notification of detected sound anomaly" is significantly higher when data on the directions to the detected and classified events are included. The need to determine the direction of the noise object as a function of the time of the passive sonar system requires to study and experiment an adaptive processor for dynamic determination of the weights of the two-element antenna array according to the criteria for minimum square error and maximum noise ratio of the signal.

Beam formation is used to amplify the signal against the background of noise. In real systems, the presence of interference signals received on side sheets leads to a strong masking of the signal by the target of interest [9]. In this case, the use of the method of minimum dispersion in signal distortion allows to form zeros in the directional characteristic in directions that coincide with the interference signal.

6. Acknowledgements:

The results can be used in the implementation of Work Package 2 "Intelligent Security Systems" of Project BG05M2OP001-1.002-0006 – Creation and Development of a Centre of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar), funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth 2014-2020".

7. References:

1. Van Trees, H. *Optimum Array Processing*. New York: Wiley-Interscience, 2002;
2. I. Iliev, "Hydroacoustic Measurements", "N. Vaptsarov Naval Academy", Varna, 2016, ISBN 978-954-8991-84-1;
3. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat I, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36341-2;
4. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat II, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36339-9;
5. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat III, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36340-5;
6. M. Todorov, On the models of interaction of dug pipelines, International Conference UACEG 2009, October 29-31, 2009, ISSN 1310-814X;
7. Ilov G., Germanov T., Zhelev J., Kirov B., Denev D., Mihova L., Varbanov R., Totsev A., Todorov M., Ivanov Iv., "Guide to Geotechnics", Eurocode 7, KIIP , 2011, ISBN 978-954-92275-8-1;
8. M. Todorov, "Cyclic Soils Properties", Seventh International Structural Engineering and Construction (ISEC-7), Hawaii, June 18—23, 2013, ISBN-10: 981-07-5354-2;
9. Samuel Shephard, Simon P. R. Greenstreet, GerJan J. Piet, Anna Rindorf, and Mark Dickey-Collas. Surveillance indicators and their use in implementation of the Marine Strategy Framework Directive. ICES Journal of Marine Science 2015, doi:10.1093/icesjms/fsv131;

Non-lethal technologies for forced stopping potentially dangerous vehicles and vessels

Adelina Tumbarska

Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. Angel Balevski"
at the Bulgarian Academy of Sciences, Sofia, Bulgaria

E-mail: y.toumbarski@ims.bas.bg

Abstract: The development of means for stopping vehicles and vessels that pose a potential threat of criminal and terrorist activity is one of the priorities in the non-lethal technologies research today. This paper summarizes and discusses the results of a study on the current state and prospects of technologies and systems for forced stopping different types of vehicles and vessels.

Keywords: NON-LETHAL WEAPONS, VEHICLE STOPPERS, VESSEL STOPPERS

Introduction

In the operations of military and law enforcement forces, it is often necessary to establish checkpoints, roadblocks and barriers, the purpose of which is to protect people and facilities in a certain perimeter or region from various threats, including vehicles carrying explosive devices. Pursuing of criminals or suspects in cars is also common in police practice, often endangering other traffic participants and passers-by. Small and medium-sized vessels pose an increasing threat to shipping and naval operations due to their use for terrorist and pirate attacks. Besides, they are often used for committing contraband, trafficking people and drugs and other crimes. With the increased access to modern equipment recently the danger of using unmanned land, floatable, underwater and flying platforms for crimes and terrorism has significantly increased.

In connection with the prevention or neutralization of such threats, significant efforts are being made in many countries to develop effective means of stopping dangerous vehicles and vessels. Efforts are focused mainly on finding solutions that increase the range and provide a smooth stopping by controlled deceleration, at a safe distance, in order to ensure the safety of passengers and minimize damage to the suspected vehicle/vessel.

This paper summarizes the results of a study on the current state and prospects in the development of non-lethal means of stopping different types of vehicles and vessels. These results are part of an extensive study of non-lethal technologies conducted within the Science and Education funded project "Quantum Communication, Intelligent Security Systems and Risk Management" (QUASAR), funded by the EU Funds for Smart Growth.

Results and Discussion

Several groups of non-lethal technologies offer opportunities for development of effective and safe means for stopping vehicles and vessels: mechanical, electrical, directed energy and chemical.

Mechanical technologies

The technologies in this category are represented by mechanical obstacles and entanglement systems for restricting and stopping the movement of various types of vehicles, the best developed of which at the moment are those for stopping cars.

Traditional car stopping systems are intended for pneumatic tires deflation and range from relatively simple means to stationary structures with mechanical control and manually placed spiked stripes. For mobile systems, the emphasis is on the ability for quick placement and minimizing the risk through structures that ensure a smooth release of air from the tires.

Means of impeding the movement of the enemy have been used since ancient times. One of the oldest non-lethal weapons are the spikes used to slow down the movement of infantry, war horses, camels and elephants, known as 'caltrop', coming from a plant with a similar shape (a type of water chestnut). The construction of these devices has undergone some improvement over the millennia, however the concept is unchanged - they all end with 4 spikes

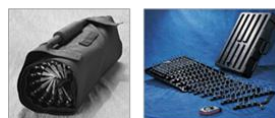


located on top of an imaginary equilateral triangular pyramid. When thrown to the ground they always stand in such a way that one spike is directed upwards, and the other three provide solid support. Today, caltrops are used by

both the military and the police to inflate pneumatic tires of all kind

of vehicles. The photo on the left shows tube-shaped caltrops designed to puncture self-adhesive car tires, which have been used for decades by special forces and law enforcement agencies in the USA. The opening in the center allows air to escape, even if the other end of the pipe is compacted by soft soil. Modern caltrops are made of high quality steel with a powder coating for corrosion protection. The design shown in the right allows for connecting the caltrops through a cord in groups of up to 500 pieces and more. [1] Causing immediate, irreparable and catastrophic damage to pneumatic tires, they are very effective as barriers for vehicles.

Spiked strips are effective and widely used means of preventing or stopping the movement of cars. Usually a strip consists of metal blades with a length of 35 to 75 mm, directed upwards. The spikes can be solid or hollow, with the cavities designed to detach from the strap and remain stuck in the tires, allowing air to escape more smoothly. For example, the stopping strips developed under the US Non-Lethal Weapons Program are manually positioned and have hollow spikes that cause



tires to fall within 10 s. [2] Similar devices are used by various US units to protect forces, checkpoints and access points. In many mobile constructions, like those of the company 'Magnumspike' (pictures down) [3], the metal spikes are placed on a folding metal structure stored in briefcase or on a base of rigid polymer which is rolled into a roll.

Manual installation of such systems, especially on roads and highways with heavy traffic, is connected with serious risk for the



safety of service personnel, so the recent developments are focused on systems ensuring remotely controlled deployment. One of these innovative products is 'PSEMC's NightHawk system' [4] which is portable and reusable. It fits in a small suitcase, which is placed by the road and is remotely controlled from a safe distance via wireless connection. The strip is positioned for less than 2 s, and after the vehicle has passed through it, it is retracted through the remote control into the briefcase for the same time, without endangering other vehicles and leaving spikes on the road. [5] Police departments in the US already have a number of such systems in use and report an impressive success rate.

There are also different variants of permanent obstacles that are built into the road or mounted on it, representing sections with a base of steel or high-strength polymer, and spikes. This type of strips has a mechanical control, through which the spikes are raised or lowered. Most obstacles have spikes pointing in one direction, but there are also strips with the ability to change the direction. This type of obstacles is used at entrances and exits of highways and parking lots, but can also be very useful in protecting the perimeter of critical infrastructure sites.

Devices that can stop cars regardless of the type of their tires are also an effective non-lethal solution for obstructing the movement of vehicles. Such systems have structures made of ropes or nets of high-strength materials that grip the front of the car or entangle its wheels, allowing the 'arrest' of vehicles of different sizes. Some of these nets are combined with spikes for greater effect, and many of them have strength and construction that allow multiple use. These

systems are of two types: vertically arranged - for capturing the front of the car and horizontal nets for tangling the wheels.

The devices of the first type are quite diverse in construction. The photo on the left shows the barrier network of the Swedish company 'SCAMA'. [6] The U.S. Non-Lethal Weapons Program includes a 'General Dynamics' Portable Barrier to Vehicles (right), a pre-deployed, mechanically activated reusable system. It is able to



stop a small vehicle traveling at speeds of up to 45 miles per hour. In stand-by mode, the capture module is located in a container that does not obstruct traffic. When activated, the net rises in less than 2 seconds, forming a soft barrier that 'arrests' the car and passengers. The system is used by various forces in the USA, recently it has been deployed in portable and permanent installations in many other countries. [7]

One example of horizontally placed nets is the VLAD lightweight vehicle stop device. It is a portable, detachable strip with disposable metal spikes that can be deployed in less than 1 minute to pierce and lock the front wheels of a small vehicle. It is also part of the US Non-Lethal Weapons Program, intended for use by different forces. [7] An electro-mechanical system for remote deployment of the net has also been



developed for protection of valuable assets, facilities and military bases. [8] An advanced quickly deployable system of this type is the X-Net of the British company 'QinetiQ'.

The unique design allows complete stopping of motor vehicles ranging from small cars to 10-ton trucks. The tire gripper uses a combination of metal spikes and strips of high-strength, dark-colored material which is difficult to be seen on the asphalt. When passing a car, the spikes get stuck in the tire, lifting the pad and wrapping it around the wheels and axle, immobilizing the car after only a few turns of the wheels. The net is strong enough to be removed and reused. The positioning device is remotely activated and the net is fully unfolded in about 1 s. [9] The system has been deployed by military, police and other units around the world.

For protection against threats on water, systems for stopping small to medium-sized vessels are being developed, mainly using ropes and nets to entangle the propellers of vessels with outboard engines. These systems rely on either pre-positioning the barrier or launching it while moving. The effectiveness of the latter depends exclusively on the precise positioning which is a difficult task especially at high-speed pursuing.

The RGES craft propulsion system was developed as part of the Non-Lethal Weapons Program and is used by the US Coast Guard. It is a net that can be pre-set (stationary), launched or thrown from the board of a vessel. It can tangle and stop the propeller of a vessel with an engine up to 250 hp travelling at speeds up to 50 knots. [7]



The device can contribute to the security of ports, protection of forces and pursuit of suspicious vessels. One of the versions has been developed for deployment as a barrier around a valuable asset or facility (such as ship, port, etc.).

A range of new vessel stopping systems is offered by the British company 'BCB International', using hand-held or vessel-mounted compressed air launchers. Specialized



ammunition is fired on the path of the vessel, placing a floating obstacle (rope or net) in front of it. When the boat passes over the obstacle, it gets entangled in the propeller and causes delay and stopping

without harming the vessel and the passengers. The systems are capable of 'arresting' vessels weighing up to 3 tons and speeding up to 45 knots per second. [10]

Electrical technologies

Over the last two decades, various concepts for stopping cars with the help of electricity have been studied however most of them have not been implemented in practice due to technical problems.

One of the few successful projects - the pre-deployable electric vehicle stopper (PEVS) - was developed within the Non-Lethal Weapons Program of the US DoD. Long-term efforts have been focused on improving the design and creating reliable, efficient and safe devices. [11] A prototype with a scalable effect, low cost and easy maintenance has been created in 2019 and undergone extensive testing. The developed technology allows the device located on the ground to 'hit' a vehicle with 500-600 thousand volts of electricity, which goes to the chassis and disrupts the engine functioning. Several minutes later the car can be started again. [12]

A new direction in the development of non-lethal technologies is the creation of wireless electrical weapons using 'channels' of electrically conductive media, such as liquid or ionized gas, instead of cable. Weapons using liquids (electrified water cannons) are designed to be used in riot control, while plasma weapons can also be used against equipment. The basic principle is the use of a laser beam to produce ionized gas, through which the electric charge can be transmitted to the target. Some of these weapons are essentially a combination of electric weapons and directed energy weapons, but the latter radiate energy from another source.

The American company 'Xtreme Alternative Defense Systems' (XADS) announced in 2004 the creation of the world's first electric weapon StunStrike capable of hitting targets at a distance of up to 15 m. The device shoots a stream of ionized gas at the target, which transmits a discharge with power capable of hitting a person or a car by disrupting its electrical system. It is intended for different ranges and applications, incl. detonating improvised explosive devices and approaching anti-tank grenades. The system is programmable, so it can be set to provide maximum security or fast effect depending on the needs. [13] This non-lethal weapon is created for use by police, special services and the military in urban conditions operations.

Another weapon that works with a laser-induced plasma channel (LIPC) is developed by 'Ionatron'. The interaction of air and laser light at a certain wavelength causes light to break down into 'fibers' which form a plasma channel that conducts energy like a virtual conductor. LIPC works in direct visibility, which allows the propagation of electrical impulses to be directed to a specific target. The 'Artificial flash' is intended to deactivate people or electronic circuits, including those of vehicles. [13]



Although the two last described weapons seem quite promising, no information about them published after 2008 can be found in the global network. Interestingly, according to a recent source - a marketing study for the period 2016-2025 [14], the companies created these weapons have currently joined their efforts on such technology under a contract with the US army and the equipment is expected to be available very soon. The source claims that voltage of 10^6 to 10^9 V could be passed through the plasma channel. So called 'Electrolaser' could find applications in short range weapons for police and army, and once the effect is scaled it can be used in aircraft and long range systems. It could easily immobilize a target vehicle or human and can be adjusted to be non-lethal or lethal through varying the voltage.

Directed energy technologies

Directed energy weapons cause damage to the target by emitting highly focused energy. It should be emphasized that the use of directed energy is considered to be the most promising direction in the development of weapons, including non-lethal ones, as these technologies offer a number of advantages over others, such as long range, accuracy, immediate delivery of the effect to the target and ability to regulate the effect.

The most promising kind of directed energy technologies for stopping vehicles is high-power microwaves (HPM). Weapons based on this technology are in principle lethal, however they have some non-lethal applications, one of which is deactivating vehicles' on-board computer systems in critical infrastructure protection, border and police checkpoints, pursuit and capture of suspects/fugitives in vehicles, traffic control, security of large-scale events, etc. Installed on a ship, such systems may be used to

obstruct or force the stopping of small vessels. Different device variants are being studied, as far as radio frequency pulses can be generated using different technologies. According to experts, these systems can provide minimal damage to the vessel and a negligible risk of injury to the crew compared to mechanical vessel stoppers.

High-power microwave weapons deliver an 'explosion' of energy designed to disrupt or destroy electronic equipment circuits. Weapons that operate in the range of radio waves and microwaves use electromagnetic pulses from two types of generators – narrow band and ultrawide band. The latter emit in a wide frequency range, but with low energy density and are convenient when it is not possible to accurately identify the characteristics of the object, in particular its operating frequencies. [15] In broadband weapons, the radiation is generated by an explosive or electromagnetic generator, while narrow-range weapons are electrically powered and aimed at specific targets. [16] Broadband weapons with directed energy are often called 'electromagnetic pulses' (EMP). According to some research, [17] short bursts of high-power microwave energy can be fatal to electronics without affecting people working with the equipment, but could have side effects on civilian electronic infrastructure, incl. hospital equipment and cardiac pacemakers.

The development of HPM weapons faces significant technical difficulties such as focusing the beams, reducing their energy per unit area with increasing distance, non-discriminatory impact (affecting all unprotected electronic systems within their range), absorbing the beams of conductive materials incl. from moisture in the air, relatively simple countermeasures, etc. [18, 19] In other words, the main challenge is to generate a sufficiently directed and sufficiently powerful pulse from a sufficiently compact source. For this reason, many are skeptical about the practical implementation of HPM weapons, but efforts are continuing in several countries.

One example of such device is the RF multi-frequency vehicle stopping system (RFVS) developed under the US Non-Lethal Weapons Program. The system provides multiple radio frequencies that interfere with the car's electronics and cause the engine to stop. [7] RFVS uses high-power magnetron tubes to generate intense RF pulses that prevent the motor from restarting while it is running. The effects on the target vehicle are short-term and generally reversible. Because, like all directed energy weapons, the system delivers energy at the speed of light, it does not need to be pre-deployed. Another advantage is the unlimited stock of 'ammunition' it has. Tests have shown high efficiency against more than 80% of potential targets, including both cars and large vehicles. [20]

In the last few years, there have been reports in the global net of several prototypes of car stoppers for police use that 'confuse' car electronics systems without destroying them. Such is, for example, the device developed by the company 'E2V', which works by sending a radio frequency pulse at a distance of up to 50 m. [21] Vehicle stoppers for military forces protection have been developed by the German company 'Diehl Defense' and already operate in more than a dozen countries. One of them - a system for stopping vehicles carrying improvised explosive devices HPEM Counter IED, based on an armored vehicle, was successfully tested in Afghanistan in 2011. [22] These devices are recently operating in several countries.

A high-power radio frequency (HPRF) vessel stopping device is under development within the US Non-Lethal Weapons Program. It is intended to provide increased range and the ability to aim at 360 degrees in the case of multiple targets. To increase the efficiency



against the respective outboard engines, various HPM sensitivity tests are performed to help determine various effective waveform parameters, such as pulse frequency and width, required power, or energy. Such a source can be integrated into a number of potential platforms. Concepts include the deployment on naval and coast guard ships, as well as unmanned aerial vehicles and aircraft. [23, 24]

The increasing use of UAVs to carry out attacks has led to the intensive development of counteraction systems. Jamming of radio communications between a drone and its remote pilot is often used

as an alternative to the drone physical destruction to prevent a hostile activity. [25, 26] For these purposes, systems based on RF HPM, which are much more powerful and operate in a wider frequency range than commercially available devices, are in development. The first documented successful use of high-power radio frequency microwave weapon against electronic equipment is marked in 2019 with the removal of an Iranian drone from the US Marine Corps using the LMADIS light integrated marine air defense system. The system consists of two off-road vehicles, one serving as a control unit and the other equipped with sensors and



jamming equipment. Typically, the system can be used to jam electronics, resulting in a return to base or landing elsewhere by default. However, it is powerful enough to destroy the electronics of a small drone at a short distance,

causing it to fall. According to [27], removing drones with the use of LMADIS is cheaper and easier than the use of artillery and requires less accuracy than using lasers. The disadvantages of the system are that it is relatively ineffective against fully autonomous drones, and can also cause 'confusion' in the communications of friendly aircraft. This system can find significant application in regions where small drone strikes are becoming more frequent, besides it can be seen as the initial phase of an ambitious project that has the potential to change the future of war.

Recently, the focus is on creating stopping systems with a more universal application. For example, the British 'Teledyne e2v' has developed a device called RF Safe-Stop, promoted on the company's website as the most modern existing contactless jamming system. According to it [28], the system is able to cause controlled stopping of moving targets on land, air and water, at a safe distance, without incidental damage. The technology has been successfully tested on drones, boats, motorcycles, cars and trucks. RF Safe-Stop is produced in full and light versions, offering stopping capabilities of up to 400 m for UAVs, up to 50 m for armored and civil vehicles and over 50 m for light boats.

Efforts in the United States are also yielding impressive results in this regard - according to a recent interview [12] with the director of the Non-Lethal Weapons Directorate, there is already a device which is powerful enough to stop everything which has electronics at a distance of hundreds of meters.

Chemical technologies

In the context of stopping vehicles, the potential of certain chemical technologies is also being considered. For example, in the US DoD' Non-Lethal Weapons Program for Fiscal 2015 [29], candidates for such applications include fast-acting low-volume combustion modifiers (for engine suffocation and combustion inhibitors), rapidly hardening synthetic concrete, solid epoxy foams, and other materials that will cause stopping the engines.

One of the concepts studied in the past is adhesive foam. It is a non-reactive liquid that is stored under high pressure. When released, the atmospheric pressure causes it to expand to several dozen times its storage capacity and its mechanical characteristics



allow it to adhere tightly to the object. In the 1990s, this concept was intended for anti-personnel use, but due to the risk of suffocation if foam covers the mouth and nose, interest has shifted to exploring its

ability to stop cars. Weapons are later being developed on this basis to stop vehicles - the foam must stop the engine and block the driver in the cab. A foam restraint system has been developed that consists of low-profile containers, each containing a sufficient amount of substances to generate extremely quickly several cubic meters of high-strength foam. Theoretically, the foam immediately deactivates the vehicle, blocking the fuel supply to the engine and the steering and absorbing the kinetic energy of the car. [30] The system can be activated automatically (via pressure sensors or light barriers) or by remote control.

Concepts of non-lethal weapons to prevent people and vehicles from accessing certain area also include substances that can create a slippery surface on which controlled movement is difficult or

impossible. Various types of chemicals have been studied, focusing primarily on water-active polymers that were harmless to the environment and health, easy to clean and provide satisfactory results. The disadvantage is that their effectiveness decreases in heavy rain, high temperatures and humidity. [31] The prototypes were many times more slippery than ice, inspiring hope that the system could be used to protect an area or building from crowds or equipment - for example, to prevent the enemy from using a strategic section of the railway line without destroying it permanently. However, slippery foam can be neutralized by simple countermeasures, such as throwing sand on the surface covered with it. These technologies seem not been particularly suitable for police activities, as they would hinder not only targets but also the police officers, however they have been studied for other applications. [32]

There is not official information in the global net concerning any current research programs on anti-materiel chemical substances of the type described. A possible reason could be that there is no consensus between the international law experts about the legal status of such means under the Chemical Weapons Convention.

Conclusions

Improving the existing and creating new means of stopping potentially dangerous vehicles and vessels is one of the highest priorities in the field of non-lethal weapons. As a result of the efforts, a wide range of equipment based on various technologies have been developed, ranging from relatively simple means to high-tech systems, in stand-alone configurations or integrated in various delivery platforms, including remotely controlled.

Data on available mechanical systems for stopping different types of vehicles show that they are very efficient, provided they are located on time and in the right place. The main problem to be solved in future systems of this type is increasing the passengers safety by finding ways to ensure controlled and smooth speed reduction. The development of mobile systems focuses on the accurate and fast placement of obstacles, including through remote control, with a view to the personnel safety.

From the available information, it can be concluded that attempts to exploit the potential of electrical and chemical technologies have not yet yielded satisfactory results.

As an alternative to mechanical means, the possibilities for using pulses of directed energy that affect the electronics controlling the engine are being intensively studied. Despite the promising advantages of these technologies, the developed systems still have significant technical problems, such as the safe stopping of fast-moving cars, controlling the range and area of effect, the equipment size, inapplicability to older generations of cars, and more. In addition, these technologies can cause some damage to people or infrastructure in their area of operation. Like the most non-lethal technologies that are new and unknown to society, those with directed energy will probably also provoke negative public reactions which could complicate their deployment.

As far as the alternative technologies are not yet sufficiently tested and accessible, they could find place in military operations in near future, however are unlikely to replace the more traditional mechanical devices used in the in law enforcement soon.

References

- [1] US DoD. A Research Guide for Civil Law Enforcement and Corrections. DoD Non-Lethal Weapons and Equipment Review. October 2004.
- [2] JNLWD. Non-lethal Weapons Program.
- [3] <https://magnumspike.com/spike-strip-devices/>
- [4] PSEMC. Nighthawk Police Stop Sticks.
- [5] Basich, M. PacSci EMC's NightHawk: Safer Pursuit Stopper. Police Magazine, 3 August 2017.
- [6] SCAMA. Vehicle Arresting Systems.
- [7] US DoD, Joint Non-Lethal Weapons Directorate. Non-Lethal Weapons Reference Book. 2012.
- [8] Rush, N., R. Miller. Developing and Fielding Non-Lethal Weapons. Defense Systems Information Analysis Journal, vol.3, No 3, 2017.

- [9] Dees, T. Safer tire-spike alternatives. PoliceOne, 31 January 2012.
- [10] Joint-Forces.com. BCB Non-Lethal Boat Stopping Systems, June 2019.
- [11] US DoD, JNLWD. Vehicle & Vessel Stopping: Non-Lethal Weapons Research and Technology Development. 22 June 2012.
- [12] Tadjdeh, Y. Directorate Wants to Change View of Nonlethal Weapons. National Defense, 31 July 2019.
- [13] Defense Update. StunStrike Weapon. 28 January 2005.
- [14] Electrolaser - Market Potential, Applications, Opportunities, Trends, Competitive & Investment Analysis. <https://www.mordorintelligence.com/industry-reports/electrolaser>
- [15] Valouch, J. Electromagnetic Devices for Stopping Vehicles. Sensors & Transducers, vol. 205, issue 10, October 2016, pp 33-37.
- [16] Abrams, M. Dawn of the E-Bomb. IEEE Spectrum, vol. 40, issue 11, November 2003, pp 24-30, DOI: 10.1109/MSPEC.2003.1242953.
- [17] Davison, N., N. Lewer, Nick. Bradford Non-Lethal Weapons Research Project (BNLWRP). Research Report No. 4, 2006.
- [18] Gunzinger, M., C. Dougherty. Changing the Game: The Promise of Directed-Energy Weapons. Center for Strategic and Budgetary Assessments (CSBA), 2012, pp. 27-28.
- [19] Feickert, A. U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress. Congressional Research Service, 12 February 2018.
- [20] Merryman, S. Multifrequency Radio-Frequency (RF) Vehicle Stopper. Report. Naval Surface Warfare Center, USA, 2012.
- [21] Johnston, C. New product shuts car engines off with a radio pulse. ARS Technica, 3 December 2013.
- [22] European Security and Defence. Eurosatory 2016: High-Power-Electro-Magnetics by Diehl Defence. 17 June 2016.
- [23] Walker, J. Nonlethal Small-Vessel Stopping With High-Power Microwave Technology. Leading Edge, 2012, pp 97-99.
- [24] JNLWD. Advanced Planning Brief to Industry, 21 September 2017.
- [25] Georgiev, N.L. Systems for detection and counteraction of short-range UAVs. 2018, ISBN 978-619-7466-00-3, 164 p.
- [26] Georgiev, N.L., O. Todorov. Possibilities for radio-electronic counter-action to the satellite navigation systems of short-range UAVs. Proc. Int. Conf. "Engineering Technology Education Safety", 3, 3, 2019, pp 262-265.
- [27] Barrett, B. The Marines' New Drone-Killer Aces its First Real World Test. Wired, 27 July 2019.
- [28] Teledyne e2v. RF Safe Stop - Target Deactivation across Land, Sea and Air.
- [29] JNLWD. Joint Non-Lethal Weapons Program Fiscal Year 2015 Non-Lethal Weapon Technologies.
- [30] Shachtman, N. Army Reloads on Sticky Foam Weaponry. Wired, 26 February 2009.
- [31] Donnelly, T. Less lethal technologies, initial prioritization and evaluation. PSDB, Home Office, London, 2001.
- [32] Downs, R. Less lethal weapons: a technologist's perspective. Policing: An International Journal of Police Strategies & Management, 30 (3), 2007, pp 358-384.

Evaluation of protective action of poisoned gas substances of new generated activated carbon for gas mask application

Liliya Manoilova¹, Kamelia Ruskova²
University of Chemical Technology and Metallurgy¹,
Technical University Sofia, Bulgaria²
lili_manoilova@abv.bg

Abstract: The object of the paper is the dynamic adsorption of new type generated gas mask carbons for respiratory protection, based on apricot shells and the impact of the protective properties of some poisonous gases or warfare poisonous substances. A study performed examined the impact on the breakthrough times of different quantities of K_2CO_3 (2 mass.% - 8 mass. %) and TEDA in the capacity of additives to the impregnation composition of the standard ASC Whetlerite type and newly obtained carbons.

Keywords: ACTIVATED CARBONS, PHYSICAL ADSORPTION, PROTECTIVE EFFECT DURATION

1. Introduction

Impregnated activated carbons represent a basic component of gas mask equipment, gas respirators, powered air purifying respirators and filter absorbers. In order to provide an effective protection against the warfare poisonous gaseous, some industrial toxic substances, and also because of the slight effect of aging processes during their storage and utilization as promising elements in the composition of the active phase of new type of gas carbons (carbon catalyst) are considered Cu, Zn, Mo, Ag, and are referred also potassium carbonate (K_2CO_3) and the organic compound like TEDA are considered [1-4]

Due to the high number of chemical warfare, potentially terroristic poisons and industrial toxic substances and various mechanisms of their detoxification from carbon catalysts, in order to test their protective properties, it is necessary to choose representative of the three mechanisms of toxic substances detoxification.

In the rescue services and armies of many countries for this aim Cl_3CNO_2 is chosen (for toxic substances which are neutralized by physical adsorption), HCN (for poisonous substances via chemisorptions) and carbon dichloride oxide- $COCl_2$ (for the toxic substances that are detoxification by catalytic sorption [5-7]).

The inclusion of alkaline carbonate - K_2CO_3 as supplements in the impregnation composition, leading to the development of meso- and micro-porosity can essentially affect the protection properties of the gas mask carbons [3,8] against the representative highly toxic compounds such as $COCl_2$ and HCN. Although $COCl_2$ has partially lost its significance as a combat poisonous substance, it is considered as an individual or mixed type potential terrorist-poison substance with a high probability of use, due to its high toxicity. In addition to its industrial production, small amounts from the toxic gas can be generated as a result of decomposition and combustion processes of organo-chlorine compounds.

The chlorinated solvents used for oil removal in aim to clean metals from different oil impurities, for example car breaks cleaners can be also converted to phosgene by the UV rays and arc welding processes.

The goal of the presented work is the examination of the impact on the protective properties (in particular the breakthrough times of different quantities of K_2CO_3 (2mass% - 8 mass %) and TEDA as additives of new synthesized type gas carbons to the vapor of $COCl_2$.

2. Experimental

A. Samples

The activated carbon used in the studies is a commercial product (signified as ACVM), obtained based on apricot shells through vapor gas activation (973 K), specific with its granulometric size 1.0 – 1.5 mm.

For the activated carbons (gas carbon catalyst) preparation was used different impregnation solutions: copper carbonate, zinc oxide, molybdenum oxide and silver nitrate. They were dissolved in aqueous solution of ammonium carbonate and ammonium

hydroxide (25%). Potassium carbonate was added and TEDA was added to the impregnation solutions.

Samples of gas mask carbons VSZC, VSZC-A2, VSZC-A4, VSZC-A6, VSZC -A8, VSZM and VSZMA2 were obtained using the standard impregnation procedure for obtaining carbon catalysts [8,9]

The selected gaseous (Cl_3CNO_2 , $COCl_2$, HCN) are representative for all toxic substances, which can be neutralized and detoxified by the following mechanisms:

□ Physical adsorption, by the volumetric filling of the micropores, particularly for the Cl_3CNO_2 . Although it is not considered a warfare substance, it is representative of the so-called well-absorbed toxic substances in testing of warfare toxic substances of gas mask carbons, including respiratory protective equipment [10].

□ Catalytic adsorption, combined with the chemisorptions of the semi-products of the impregnate components. Representative poisonous substance is $COCl_2$, referring to the acid gases, which hasn't lost its use as a chemical weapon, used especially in various poisonous formulations.

□ Chemisorption of toxic substances combined with catalytic sorption. Representative toxic substance selected is HCN, which apart from combat purposes has wide industrial application.

The samples obtained through standard impregnation procedure for carbon catalysts obtaining are presented in Table 1.

Table 1 carbon catalysts obtained [10].

Sample type signification	
ACVM	-
VC5W ASC Whetlerite type	Cu/Cr/Ag
VC5W-A2 ASC Whetlerite type	Cu/Cr/Ag + 2 % K_2CO_3
VC5W-T ASC Whetlerite type	Cu/Cr/Ag + TEDA
VSZ ASZ type	Cu/Zn/Ag
VSZ-A2 ASZ type	Cu/Zn/Ag + 2 % K_2CO_3
VSZC ASZC type	Cu/Zn/Cr/Ag
VSZC-A2 ASZC type	Cu/Zn/Cr/Ag + 2% K_2CO_3
VSZC-A4 ASZC type	Cu/Zn/Cr/Ag + 4% K_2CO_3
VSZC-A6 ASZC type	Cu/Zn/Cr/Ag + 6% K_2CO_3
VSZC-A8 ASZC type	Cu/Zn/Cr/Ag + 8% K_2CO_3
VSZC-T ASZC type	Cu/Zn/Cr/Ag + TEDA
VSZM ASZM type	Cu/Zn/Mo/Ag
VSZM-A2 ASZM type	Cu/Zn/Mo/Ag + 2% K_2CO_3
VSZM - T ASZM type	Cu/Zn/Mo/Ag + TEDA

The specific surface of the samples were determined using low temperature nitrogen adsorption of N_2 (77K) by the BET method. Data from the adsorption-textural parameters and distribution curves (micro- and mesopore size) are presented in [10,11]. The total volume of the pores (V_t) was determined based on the Gurvich rule [12] at the relative pressure p/p_0 of 0.95. The volume of the mesopores (V_{MES}) was estimated based on the Dubinin Radushkevich equation [13] (table 2).

III. Results and Discussion

A. Adsorption – textural characteristics

Based on the results for adsorption textural parameters (table 1) it can be seen that the impregnation procedure leads to increase of microporous heterogeneity, respectively specific surface of the impregnated samples compared to the initial activated carbon ACVM.

Table 2. Specific surfaces and basic texture parameters of cu/zn/cr/mo/ag gas mask carbons

Specimen	A_{BET} m^2/g	A_{MES} m^2/g	V_t cm^3/g	W_a cm^3/g	V_{MI} cm^3/g	V_{MA} cm^3/g	V_{MES} cm^3/g	$\bar{x}_p$ (nm)	τ_p Å
¹ ACVM	1060	165	0.930	0.396	0.377	0.019	0.534	0.68	17.5
² VCSW	892	280	0.861	0.352	0.202	0.150	0.509	0.93	19.3
³ VCSW-A2	881	363	0.851	0.313	0.185	0.128	0.538	0.78	19.3
⁴ VCSW-T	864	320	0.805	0.310	0.198	0.112	0.495	0.82	18.6
⁵ VSZ	882	354	0.830	0.327	0.264	0.063	0.503	0.87	18.8
⁶ VSZ-A2	852	365	0.829	0.324	0.226	0.098	0.505	0.99	19.5
⁷ VSZC	872	340	0.820	0.312	0.240	0.072	0.508	0.82	18.8
⁸ VSZC-A2	846	322	0.813	0.300	0.201	0.099	0.513	0.85	19.2
⁹ VSZC-A4	829	374	0.814	0.284	0.189	0.095	0.530	0.85	19.6
¹⁰ VSZC-A6	817	383	0.812	0.263	0.178	0.085	0.549	0.75	19.9
¹¹ VSZC-A8	776	417	0.808	0.250	0.142	0.108	0.558	0.86	20.8

The study of the protection properties (in particular the breakthrough times) was carried out with highly poisonous substances $COCl_2$ [14] synthesized by us.

B. Adsorption – dynamic studies

The pre-dried (378 K, 2 hours) carbon catalysts were loaded in glass dynamic sorption pipes and were exposed to the steam-air flow from toxic substances, passing through the samples, regarding the following set parameters:

Table 3. Test parameters set [8]

Layer thickness of the studied sample	3.0 cm
Internal diameter of the dynamic pipe	2.0 cm
Volumetric velocity of the vapor gas flow	1.57 l/min
Relative humidity of the flow	50%
Temperature	293 + 3 K
Inlet concentration of Cl_3CNO_2	5 ml/l
Concentration of registration of the Cl_3CNO_2 breakthrough	15 ml/ m^3
Inlet concentration of HCN	3 ± 0.3 mg/l
Concentration of registration of the HCN breakthrough	10 ml/ m^3
Concentration of registration of the $(CN)_2$ breakthrough	5 ml/ m^3

In the gas technique, the protective action of breakthrough time (t_B) is defined as the time for which the concentration of poisonous

substances in the steam-air flow after the sorbent layer reaches a preset value for the relevant experimental conditions.

The breakthrough time of the samples for the toxic substances Cl_3CNO_2 and HCN was investigated in our previous study [8].

A. The breakthrough time of the samples exposed to the vapor of $COCl_2$

The breakthrough time of the vapors of the chloropicrin under the conditions set, for the studied samples are given on figure 1.

According to the currently adopted mechanism [15] $COCl_2$ can be neutralized by physical adsorption combined with impregnation. $COCl_2$ is hydrolyzed from the pre-adsorbed water vapor from the air generating HCl and carbon dioxide $-CO_2$. Afterwards hydrogen chloride reacts with Cu and Zn (predominant basic carbonates) complexes to form Cu and Zn chlorides.

The last one has a negative effect on the possibilities of impregnates to further protection for example against HCN.

From table 1 it can be seen that the initial activated carbon-ACVM has an about two times shorter breakthrough time than the same parameter for all examined gas carbon samples. This strongly proves the role of the impregnated gas carbons in the process of disposing of the vapor of $COCl_2$.

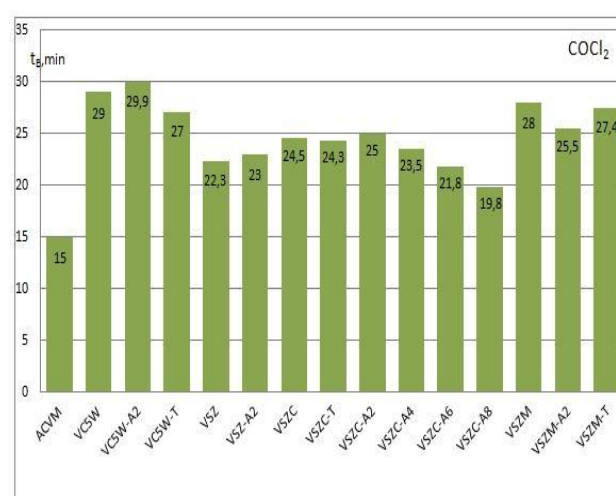


Fig1. Breakthrough time (t_B) of the initial activated carbon and the impregnated samples

Based on the obtained results and the comparison of the all gas type carbons, it can be concluded that the higher values of breakthrough time are shown by the samples of the ASC Whetlerite. Samples from the ASZC type (without samples with high content of K_2CO_3 i.e. > 4 mass%) have a breakthrough time a little lower than the samples from ASC Whetlerite and ASZM type, but higher t_B than the samples from ASZ-type.

Monitoring the impact of the modifier TEDA and K_2CO_3 on the breakthrough time of the investigated gas carbons was studied.

$COCl_2$ reacts with the primary amines, to which TEDA does not relate to. The results obtained Fig.1 show that for all type samples, also for the impregnates having TEDA to the composition leads to decrease of the service time (t_B), compared to the samples without TEDA. Therefore, despite its high alkalinity, TEDA does not promote the hydrolysis of $COCl_2$ in the pores of gas masks. The inclusion of K_2CO_3 (2 mass%) in all types of gas carbons except the sample VSZM-A2 (ASZM type carbons) leads to a slight increase of breakthrough time.

The inclusion of alkaline carbonates K_2CO_3 in the impregnation composition leads to:

- pH increasing, which leads to the improvement of the catalytic function of additives with respect to the hydrolysis of $COCl_2$. K^+ ions from the potassium carbonate improves the catalytic function of the carbon surface [17].
- K_2CO_3 reacts with the released HCl (hydrochloric acid) thus protecting the Cu and Zn- compounds (mainly basic

carbonates) of the impregnates. Thus the catalytic function remains for the longer period, respectively the breakthrough time is prolonged. Especially $\text{Zn}(\text{CO}_3)_2(\text{OH})_6$, protected with K_2CO_3 from HCl , also prolongs the reaction time with HCl , respectively the service time (t_B) of the gas carbons from the type ASZC (2 mass% K_2CO_3).

For the VSZM-A2 sample probably Mo cause an effect interfering with the function of K_2CO_3 .

The impact of the breakthrough time was studied with regard to the increasing content of K_2CO_3 (> 2 mass%). For the sample VSZC-A4 (4 mass% K_2CO_3) it can be seen a slightly decreasing breakthrough time - about 4.1% compared to VSZC. The tendency remains and is strongly expressed in samples VSZC-A6 and VSZC-A8, decreasing with 11% and 19.2% respectively. Therefore, an increase of the K_2CO_3 content with more than 2 to 4 mass%, leads to a decrease in breakthrough time of the sample type ASZC compared to VSZC, reaching about 20% for VSZC-A8.

The results obtained of the gas carbons catalyst, containing K_2CO_3 in the impregnant composition for COCl_2 detoxification, can be summarized in two groups, the first one is the samples, comprising $\text{K}_2\text{CO}_3 < 4$ mass%, and the other one for the samples with $\text{K}_2\text{CO}_3 > 4$ mass%.

For samples, comprising $\text{K}_2\text{CO}_3 < 4$ mass%, we can assume that the hydrolysis (including the components of the impregnates, as well as on the surface of the initial activated carbon, promoted with K^+ , do not proceed separately, but in a synergetic mechanism in COCl_2 hydrolysis. The weak physical adsorptions probably occurs not only at K_2CO_3 2 mass%, but also at 4 mass% (but probably much less significantly).

For the second modified gas carbons, comprising more than 4 mass% content K_2CO_3 , the catalytic process of hydrolysis weakens, based on the synergistic effect of the impregnates and the surface of the initial carbon weakens (due to the optimal values pH, corresponding to potassium carbonate mass content (2 до 4 mass% K_2CO_3). The physical adsorption of COCl_2 from the gas carbon is completely stopped.

IV. CONCLUSION

The protective properties of the obtained gas carbons (carbon catalyst) was studied, including the modified samples on the representative toxic substance (COCl_2) with catalytic detoxification combined with chemisorptions of the products of vapor conversion of the toxic substance was studied.

From the examined types of the carbon catalysts in terms of vapor of COCl_2 , the highest breakthrough time (t_B) was observed in the ASC Whetlerite type samples, and the lowest for the initial samples –ACVM.

The protective properties of the synthesized new type gas carbons (including the modified samples) of the newly obtained carbon catalysts were established, providing a sufficient level of protection against the studied toxic substances.

3. References

1. BSS EN 133:2003 Respiratory Protection Tools Classification (2003).
2. R. Nickolov, D. Mehandjiev, Comparative study on removal efficiency of impregnated carbons for hydrogen cyanide vapors in air depending on their phase composition and porous texture, *J. Colloid Interface Sci.*, 273, , 87-94, (2004).
3. A.P. Chatzis, L.Manoilova, G. Gentscheva, R.Nikolov, Purification of water contaminated with Tl, *Engineering.Technologies.Education.Security, Proceedings, Issue 1(7)*, pp.22-25, (2019).
4. K. Ruskova, L. Manoilova, Obtaining of Activated Carbon using Chemical Activation with KOH, *International Conference on High Technology for Sustainable Development*, 10-11 October, , Sofia, Bulgaria, (2019)
5. Manoilova, A. Chatzis, et all, Effect of additives in phase composition of carbon catalysts other than ASC Whetlerite type carbons on their removal efficiency against hydrogen cyanide vapors in the air, *Science. Business Society*, 5, 13-17, (2016)
6. L. Manoilova, A. Chatzis, Iv. Spassova, R. Nickolov, Concept for the development of a new type carbon catalyst designed for protection against vapours of highly toxic substances, *Machines, Technologies, Materials*, IX, issue 5, Veliko Tarnovo, pp.27-29, (2015)
7. L. Manoilova, A. Chatzis, D.Vladov, Iv. Spassova, R. Nikolov, Effect of additives in phase composition of carbon catalysts other than ASC Whetlerite type carbons on their removal efficiency against hydrogen cyanide vapors in the air, *Science. Business Society*, 5, 13-17, (2016)
8. L.Manoilova, R. Nicolov, Study on the impact on the protection properties of a new type of gas mask carbons in respect to Cl_3CNO_2 and $\text{HCN}(\text{CN})_2$ vapors, *Journal of Chemical Technology and Metallurgy*, 55,1, ,pp.98-102,(020)
9. R. Nickolov, D. Mehandjiev, Comparative study on removal efficiency of impregnated carbons for hydrogen cyanide vapors in air depending on their phase composition and porous texture, *J. Colloid Interface Sci.*, 273, 87-94, (2004)
10. L.Manoilova, R. Nicolov, Study on the impact of the modifier K_2CO_3 on the texture parameters of newly synthesized gas mask carbons, *Journal of Chemical Technology and Metallurgy*, 54,4,pp.838-844, (2019)
11. L.Manoilova, Impact of K_2CO_3 and TEDA on the texture parameters of new gas mask carbons, *Journal of Chemical Technology and Metallurgy Journal of Chemical Technology and Metallurgy*, 56,1,116-122, (2021)
12. Gurvich,L., *Journal for Physical Chemistry*, 47, 1915, 805.
13. Dubinin, M.M., T.I. Isotova, O. Kadlets, O.L. Krainova, *Not. AS Soviet Union, Ser. Chemistry*, , 1232, (in Russian), (1975)
14. Chatzis, A., L.Manoilova , R. Nickolov, The threat of chemical terrorism – review, *Scientific technical union of mechanical engineering, Technics. Technologies. Education. Safety, Proccedings*, Veliko Tarnovo, (2015)
15. Gorzkowska-Sobas, A. and K.M. Bjorgo, Adsorption performance of activated carbon towards toxic industrial chemicals, *Norwegian Defence Research Establishment (FFI)*, April (2015)