The FEDERATION OF THE SCIENTIFIC ENGINEERING UNIONS (FSEU)

in Bulgaria is a professional, scientific - educational, non-governmental, non-political non-profit association of legal entities - professional organizations registered under the Law on non-profit legal entities, whose members are engineers, economists and other specialists in the field of science, technology, economy and agriculture.

FSEU performed bilateral cooperation with similar organizations from many countries.

FSEU brings together 19 national associations - Scientific and Technical Unions / STU /, 34 territorial associations, which have more than 15 000 professionals across the country.

FSEU is a co-founder and member of the World Federation of Engineering Organizations (WFEO).

FSEU a member of the European Federation of National Engineering Associations (FEANI), and a member of the Standing Conference of engineering organizations from Southeast Europe / CO.PICEE /, Global Compact, European Young Engineers (EYE). The Federation has the exclusive right to give nominations for the European Engineer (EUR ING) title.

Contacts:
108 Rakovsky Str., Sofia 1000, Bulgaria
web: www.fnts.bg
e-mail: info@fnts.bg
INTERNATIONAL EDITORIAL BOARD

Prof. Dr. Eng. Alexander Tokarev,
Altai State Technical University, Russian Federation

Assoc. Prof. Dr. Aleksandar Kostikj
Ss. Cyril and Methodius University in Skopje, North Macedonia

Div. Gen. Dr. Hab. Boguslaw Pacek
Academy of National Defence, Warsaw, Poland

Prof. Dr. Vanya Banabakova
Vasil Levski National Military University, Bulgaria

Assoc. Prof. Dr. Igor Penkov
Tallinn University of Technology, Estonia

Prof. DSc. Igor Taratorkin
Ural Branch of the Russian Academy of Sciences, Russia

Assoc. Prof. Dr. Ivan Tsonev
University of Shumen, Bulgaria

Assoc. Prof. Dr. Jan Furch
University of Defence in Brno – Czech Republic

Col. Prof. Dr. Hab. Mariusz Wiatr
Land Forces Military Academy, Wroclaw, Poland

Assoc. Prof. Dr. Eng. Mitko Gospodinov
Scientific and Technical Union, Veliko Tarnovo, Bulgaria

Assoc. Prof. Dr. Eng. Mitko Nikolov
Rousse University – Angel Kanchev – Bulgaria

Assoc. Prof. Dr. Nebojsa Bojanic
University of Sarajevo, Bosnia and Herzegovina

Prof. Dr. M. Niyazi Eruslu
Yalova University, Turkey

Assoc. Prof. Dr. Oleg Stelya
National University named Taras Shevchenko, Kiev, Ukraine

Assoc. Prof. Dr. Eng. Penka Nedeltcheva
Technical University of Gabrovo, Bulgaria

Assoc. Prof. Dr. Eng. Petar Simonovski
Saints Cyril and Methodius University, Skopje, North Macedonia

Assoc. Prof. Dr. Rozalia Kuzmanova – Kartalova
University of Veliko Tarnovo, Bulgaria

Assoc. Prof. Dr. Svilen Rachew
Technical University of Gabrovo, Bulgaria

Colonel Assoc. Prof. Dr. Eng. Svilen Stefanov
Vasil Levski National Military University, Bulgaria

Assoc. Prof. Dr. Yordan Hristov
Vasil Levski National Military University, Bulgaria

Prof. DrSc. Eng. Vladimir Musiyko
National Transport University of Ukraine

Assoc. Prof. Dr. Volodymyr Zhavoronkov
National Aviation University of Ukraine

Prof. Dr. Zelimir Kesetovic
University of Belgrad, Serbia
# CONTENTS

**SECURITY.**

<table>
<thead>
<tr>
<th>Title</th>
<th>Author(s)</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARTIFICIAL INTELLIGENCE AND SECURITY. SECURITY 4.0</td>
<td>Prof. Radulov, N., PhD</td>
<td>214</td>
</tr>
<tr>
<td>COUNTER-DRONE ACTIVITY AS A SYSTEM</td>
<td>M.Sc. Csengeri J. PhD. candidate</td>
<td>217</td>
</tr>
<tr>
<td>CYBERSECURITY. ANTHROPOGENIC OR TECHNOGENIC THREAT?</td>
<td>Tihomir Stoychev</td>
<td>221</td>
</tr>
<tr>
<td>PSYCHOLOGICAL MODEL FOR THE INVESTIGATION OF ESCAPES FROM PLACES OF IMPRISONMENT.</td>
<td>PhD Madzharov E.</td>
<td>224</td>
</tr>
<tr>
<td>HARMONIZATION OF THE HUMAN FACTOR IN INTEGRATED AVIATION SECURITY SYSTEM</td>
<td>Filippov V.L., Ovchenkov N.I.</td>
<td>228</td>
</tr>
<tr>
<td>ISLAM: THE FRIGHTENING RELIGIOUS OTHERNESS</td>
<td>Assoc. Prof. Dr Veselin Bosakov</td>
<td>232</td>
</tr>
<tr>
<td>COMPETENCE CENTRES AND INTELLIGENT SECURITY SYSTEMS IN BULGARIA</td>
<td>Chief Assistant Dr. Eng. Panevski V.S.</td>
<td>236</td>
</tr>
<tr>
<td>STANDARDIZED APPROACHES FOR THE INTEGRATION OF MANAGEMENT SYSTEMS OF THE CRITICAL INFRASTRUCTURE OBJECTS</td>
<td>Associate professor Dimitrov D.L., Ph.D.</td>
<td>239</td>
</tr>
<tr>
<td>CONTENT SECURITY POLICY VALIDATION</td>
<td>L.Petkova, PhD</td>
<td>242</td>
</tr>
<tr>
<td>TRUST AS A PSYCHOLOGICAL FACTOR OF SAFE INTERACTION</td>
<td>T.A. Zhalagina, E.D. Korotkina</td>
<td>246</td>
</tr>
<tr>
<td>SECURITY SYSTEM CREATING IN CONDITIONS OF UNCERTAINTY AND RISK-OUTLINE OF THE PROBLEM</td>
<td>dr M.Szyłkowska</td>
<td>248</td>
</tr>
<tr>
<td>CHEMICAL MATERIALS (PRECURSORS) APPLIED IN IMPROVISED EXPLOSIVE DEVICES AND THEIR USE IN TERRORIST ATTACKS AGAINST CRITICAL INFRASTRUCTURE FACILITIES</td>
<td>MSc Vasileva, P. – PhD Student</td>
<td>251</td>
</tr>
<tr>
<td>THE THREATPOSED BY DRONES AND IMPROVISED EXPLOSIVE DEVICES USED AGAINST CRITICAL INFRASTRUCTURE</td>
<td>MSc Vasileva, P. – PhD Student</td>
<td>254</td>
</tr>
<tr>
<td>A CONCEPTUAL MODEL OF LAW ENFORCEMENT USE OF FORCE</td>
<td>Assist.-Prof. Dr. Eng. Tumbarska, A.</td>
<td>258</td>
</tr>
<tr>
<td>OPPORTUNITIES FOR RADIO-ELECTRONIC COUNTERACTION TO SATELLITE NAVIGATION OF UNMANNED AERIAL VEHICLES WITH A SMALL RADIUS OF ACTION</td>
<td>Prof. Dsc Georgiev, N.L. and Eng. Todorov, O.D.</td>
<td>262</td>
</tr>
<tr>
<td>SAFETY OF THE ENTITY’S FUNCTIONING IN THE CONTEXT OF THE IMPLEMENTED QUALITY MANAGEMENT SYSTEM IN ACCORDANCE WITH ISO 9001:2015 – A CASE STUDY ANALYSIS</td>
<td>M. Dąbrowska-Świder, Msc.</td>
<td>266</td>
</tr>
<tr>
<td>DEFENSE PREPARATIONS AS THE STATE SAFETY CONDITION – SELECTED LEGAL DOCUMENTS</td>
<td>Dr Wojnarowska-Szpucha S.</td>
<td>270</td>
</tr>
<tr>
<td>THE SECURITY ENVIRONMENT AND THE CHALLENGES TO THE EUROPEAN UNION AND NATO IN THE FIELD OF SECURITY</td>
<td>Colonel PhD. Eng. Ivaylo Angelov</td>
<td>274</td>
</tr>
</tbody>
</table>
ANALYSIS OF DATA TRANSMISSION METHODS USING VISIBLE LIGHT FOR INFORMATION SECURITY
Shvyrev B.A. PhD. (Phys.-Math.), PhD student Timonov D.A. .................................................................................................................................................................................................................................................. 279

STUDY OF THE EFFECTIVENESS OF CORUNDUM AND BORON CARBIDE CERAMICS IN HYBRID PROTECTION SYSTEMS
Prof. Lakov L., PhD Zheng Shunqi , Senior Assist. Prof. Asenov St., PhD ................................................................................................................................................................................................................. 281

PECULIARITIES IN CRISIS DECISION MAKING
Assos. Prof. Milen Ivanov PhD .......................................................................................................................................................................................................................................................... 284
ARTIFICIAL INTELLIGENCE AND SECURITY. SECURITY 4.0

Prof. Radulov, N., PhD
Department National and International Security, New Bulgarian University, Sofia, Bulgaria
nradulov@nbu.bg

Abstract: The Artificial Intelligence (AI) has giant possibilities to optimize the fight against crime and strengthen national security. In the conditions of unimaginable accumulation of information and the need for rapid decision-making, only the use of AI can lead to success. Intelligence, counterintelligence, forensic science, counteracting organized crime, rapid processing of available information, drafting of varied decisions, creating plans and multivariate scenarios, performing various analyzes is a time-consuming process. Only its use can significantly shorten this time and thus dramatically increase the possibilities for detection, prevention and curbing crimes.

Keywords: Artificial Intelligence; Intelligence; counterintelligence; security; forensic science; investigation; crime.

1. Introduction

Artificial Intelligence (AI) can turn into reality the scenarios of today's fantastic movies: intellectual operating systems and digital assistants. It may even be possible for robots to perform basic police functions. In practice today, if the police have high-quality computer systems with the scope of an AI, much of their routine office work can be done by them, resulting in new reservations being made to increase police presence in urban areas. One of the main resources today - the human - in police activity is increasingly burdened with administrative and cabinet activities, which leads to fewer police officers on the street. AI is now in a position to ensure the monitoring of video-data flows and data collected from a large number of sensors and can warn security services of suspicious activity. It is not far the complete integration of nowadays CCTV networks, their synthesis with modern image search programs, the parallel inspection of all available databases of people with contact with compromised persons, their ranking according to predefined indicators developed by experts. Today the police is already using robots to conduct search and rescue operations, to dispose explosive devices in terrorist activity and even to destroy armed criminals.

2. Integration of AI into our familiar world

Today, Orbital Insight is practicing machine self-training for low resolution photos from Landsat (US) and Sentinel (in the EU) satellites. It leads to easier identification of military sites, terrorist camps, solving problems of domestic and international security, counteracting organized crime, for example, monitoring and tracking channels for human trafficking and smuggling of goods.

Practice shows that the largest amount of funds are invested in programs in the national security sphere of the individual countries – since September 11, 2001, over $ 500 billion were given for NSA's electronic intelligence systems, and most high-tech products originated from military projects - for example, ARPA-Internet. This creates an additional and serious threat to predominantly militarization of AI by individual countries and individuals with the necessary assets. It is quite possible that some organized crime circles allocate funds and gain access to AI and specialized military and spy-oriented robots.

3. AI self-learning (Deep Learning)

We must proceed from the fact that adequate quality system can solve every task assigned to it, so it is necessary to formulate such a task that the solution found by the machine is unquestionable in the interest of man. The basic idea is that the purpose of the machine must be concluded in a maximum outreach of beneficial for people targets, but it does not have to know in advance what they are. In addition to being useful for the people, the solution must be guaranteed in its security and safety. New technologies, such as quantum computing, may change the AI's approach to getting information about different issues, and allow it to learn by receiving feedback, and perhaps even imitate human cognitive contact functions with the world. If this happens, AI will bring economic benefits, working without inherent human errors due to uniformity and cumulative fatigue. Giant information systems with security-related information stored in them can serve as a basis for comparing, improving and intensifying the deep learning process in a specific area such as national, international and civil security. There are many routine procedures in security processes that AI can handle with ease, but it is important to have a proactive and creative action with preemptive nature. Such action, based on a series of AI-proposed management solutions due to electronic forecasting, observed and corrected by talented managers and analysts, will lead to a major breakthrough in countering modern security threats in its broad and narrow sense. Early identification of threats, accurate forecasts in a different timeframe, provided sufficiently and timely, backed up with detailed multi-factor scenarios of management decisions, can dramatically optimize the fight against crime worldwide.

Security issues are also the issues of the safety and vulnerability of AI. Although the specialized AI offers vast opportunities to society, it can also be deceived, penetrated, or misled. Breaking the security systems is doubly devastating because it affects not only themselves but also the quality of their product – national, public and civil security. We need to be sure that the decisions taken by the machine are not the result of external interference and can not be changed by cyber attacks.

4. Features and capabilities of AI

In order to be aware of the security-related AI capabilities, we need to consider the following features.

The AI changes over time. Today, artificial intelligence is commonly referred to as machine learning opportunity - programming approaches using different algorithms and methods such as linear regression, decision trees, Bayesian networks, evolutionary algorithms, and artificial neural networks. Our understanding of what is AI varies with the passing of each milestone in this field. Adaptability, flexibility, predictability and

2 https://www.hsdl.org/?abstract&did=484061
3 https://www.uclalawreview.org/policing-police-robots/
4 Investments in the robot industry in 2019, according to experts, will exceed $ 135 billion, almost twice as high as in 2015 (n. a.)
5 It can now be estimated that transnational crime accounts for 15-20% of the world gross product as purely criminal turnover and not less than 25% as legal turnover controlled by criminal groups. Generally speaking, criminal groups control not less than a third, but rather about 50% of the global turnover of all kinds of goods and services, assets and finances. - Goodman, Marc: Future Crimes. Inside the Digital Underground and the Battle for Our Connected World, Penguin Random House, 2016.
6 Bayesian networks, also known as "belief networks" or "causal networks", are graphical models for representing multidimensional probability distributions. http://www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photof/g/web/glossary/bayesnet.html
proactivity in terms of minimum time resources, the speed of decision-making and scenarios realizing them should be the priorities of the AI used in the security sphere.

**AIs, robots and people work better when it comes together, there is a factual synergy.** In practice it has already shown that people who carry out complex actions or play games are more effective and win when interacting with high-tech applications than when analogous activity is done only by people or just by computers. Increased creativity of man helps to train the AI so that it strives to create original solutions using its capabilities quickly process huge data sets, classifying and arranging a giant number of operations, operative decisions and scenarios that allow special services to implement them successfully. In the field of security, it is clear that this, who apply high technology, uses more, better-processed and verified information, has a wider range of standard management to which he can rely. He receives more detailed scenarios for strategic and operational solutions, and his control capabilities are enhanced. This presupposes a natural basis for creative thinking and management therefore intelligence service gets a great resource for anticipating impact and success.

There are AI systems that help leverage data obtained from open sources, but their use for machine training needs to be arranged and protected accordingly. Data generated by specific forces and means, as well as by processing and monitoring of publicly available sources, are equally actively used in the security field. Allen Dulles claimed that intelligence works with over 90% acquired from open sources data. Therefore, the AI in the security can use all the possibilities for collecting, sorting and managing the data existing in the information space, which optimizes the performance of a quality, timely and effective activity in providing national and civil security.

Even the best intelligent systems can make mistakes and deviations. In the field of security, the data obtained should be further verified in order to eliminate the possibility of both incompetence and subsequent crisis and possible deliberate misinformation resulting from an enemy's operation.

**The security impact of AI will depend on the approach and how it is used.** The practical application for solving real problems will be decisive. Increasing the capabilities and influence of intelligent systems and robots will increase the importance of creative decisions taken by executives in the sector about location and time of use. This will require a radical change in the security manager's profile regarding his management culture – the set of knowledge, habits and skills, as well as a change in the subjects he will study and practice – cyber-management, cyber-planning, cyber-forecasting, cyber-scenarios, etc.

5. **Artificial Intelligence and Counteracting Crime**

**Collecting information**

Collecting data on crime situation is a way to derive the necessary knowledge from large data sets. In other words, this is an approach to discover hidden relationships between organizations and individuals committing crimes by using artificial intelligence methods. The wide range of data mining applications has become a significant area of research nowadays, as part of these applications are related to detection, prevention and curbing crimes. We must not forget the postulate that information and its analysis lie at the heart of the successful fight against crime, as well as the management of this counteraction.

**Criminology**

Criminology is one of the most important areas of application of intelligent data analysis. It is a process whose purpose is to identify the criminal characteristics. In fact, crime analysis involves investigating and detecting crimes and linking them to criminals. The large numbers of crime data and the complexity of links between them have turned criminology into a suitable area for the application of artificial intelligence analysis methods. Identifying the signs of crime is the first step for further investigation. Using this approach, crime information can be automatically collected and entered into law enforcement databases.\(^7\)

**AI, training, deep learning and fighting crime**

Machine Learning - computer algorithms that allow AI to learn to work with a large amount of data are widely used by technology giants such as Google, Apple and Netflix. The same technology that allows programs to recommend films or to set the order in the Google search results list is now successfully used to combat crimes of varying severity.

**Detecting crimes**

Because AI is able to analyze a huge amount of data, it can be used to both investigate and prevent crime. An example of this is the advertising of sex services on the Internet. Sex workers are thought to be relatively anonymous and advertise their services almost under the nose of law enforcement authority. But every message on the web leaves a digital trace. Cyber experts can use algorithms for digital tracking data on the internet to train AI to see if women volunteer or coerced advertise their services, focusing on seemingly insignificant details. By processing the input data, algorithms are programmed to analyze such details as a boom of small theft arrests in the area where sex services are advertised. AI may detect an increase in thefts of the least important things, such as toothpaste or soap. The idea of this methodology is that if someone is a victim of human trafficking and is brought from another region, he may be deprived of access to basic subjects for a normal life. Furthermore, AI training is applicable to data related to hotel rooms paid in cash areas where sexual services are provided and advertised during major events such as concerts or sporting events. This algorithm applies to other details related to trafficking in human beings. For example, analyzing the above-mentioned messages, law enforcement officers use the training opportunities of AI to establish links between ads and their authors, paying attention to such nuances as similar styles of writing and settings used in more than one ad, , on websites in missing persons' databases. A learning algorithm is also used to track payment transactions to provide intimate services to identify the links of those paying for advertising with larger organizations involved in trafficking. Machine learning technology for AI can be applied not only to the detection of crimes related to human trafficking and forced prostitution but also for practically any other types of crime.

**Forced labor**

By training and self-learning AI, law enforcement can determine whether some business works together with companies using forced labor. In the area of supply chain logistics, the use of forced labor is not unusual. AI can help investigate allegations of labor violations or complaints against companies using forced labor. Analysis of data through AI may reveal links that would otherwise be difficult to identify.

**Cybercrime**

AI can help companies prevent cyber-crime that can cause financial damage and harm their reputation. It can be trained to recognize keywords or topics related to harmful content, thus stopping the potential cyber attack.

**Burglary**

Law enforcement can use training to detect crimes such as burglary. For example, data on a large volume of theft (date and time when offenses were committed, crime objects and methods, tools to commit) may show similarities with other comparable crimes that have not been resolved. After gathering information\(^8\)

\(^{7}\) The Craft of Intelligence, 1963, Lyons Press; Reprint edition, May 1, 2016

about the crime (investigation of the crime scene, interviewing witnesses, investigating crime objects, etc.), they can be used to train AIs to analyze this data, find links with others crimes. AI can easily detect it when formalizing a large enough volume of crime data, or identify suspects and identify gaps in the investigation, and at the same time relieve police officers of unnecessary work to be able to focus on other important aspects of the investigation.

**DNA analysis**

Modern forensic expertise of DNA is critical to the investigation of crimes, but the interpretation of the DNA code can be quite complicated. Specialized AI training techniques can be used to simplify the interpretation of DNA, especially when it comes to DNA samples of several individuals. There is a huge amount of data that is not currently read solely because our limited capabilities, but the computer algorithms of AI can easily do this.  

**Face recognition**

A common method of combating crime using AI is the Face Detection Technology. It is often used at airports to include mapping of human images into law enforcement database files, which allows to identify the perpetrator.

**Prevention of crimes of a terrorist nature**

Scanning social networks to find people who can be radicalized is another activity that AI can effectively perform after appropriate training. Nowadays, some law enforcement agencies are already using social networking monitoring and analysis to prevent attempts to recruit new members of terrorist organizations such as ISIS and others like them. One such monitoring tool is called iAWACS or the AWACS internet system. This name is similar to the abbreviation used by the US military to describe its intelligence stations. The purpose of iAWACS is to prevent negative events by monitoring the activity on the Internet, identifying and locating potential criminal scenarios.

6. Conclusion

The abovementioned abilities of artificial intelligence in the security sphere impress with the breadth of application and the possible positive effect. Without expanding the scope of the solutions discussed, which can be implemented with the help of the AI, we can certainly argue that it and Security 4.0 will completely change the possibilities for enhancing the quality and intensity of the product “civil and national security” and this change is close and forthcoming.

**Bibliography**


3. www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photoz/g/web/glossary/bayesnet.html


5. www.hsdl.org/?abstract&did=484061


COUNTER-DRONE ACTIVITY AS A SYSTEM

M.Sc. Csengeri J. PhD. candidate
Faculty of Military Science and Officer Training – National University of Public Service, Hungary

csengeri.janos@uni-nke.hu

Abstract: However, several counter-drone solutions exist, these are individual, isolated means of countering drones. The aim of the paper is to sum up the counter-commercial-drone solutions and to highlight the possible synergic effects of employing these assets as a system. The author reckons that during the formulation of counter-drone systems, the basic tenets of defensive counter-air and airspace control also can be applied. In the paper, the expression of drone means a remotely piloted aircraft system which can be purchased from commercial stores or from internet based stores.

Keywords: DRONE, COUNTERING DRONES, DRONE THREAT, SYSTEM, TRAFFIC MANAGEMENT, DEFENSIVE COUNTER-AIR

1. Introduction

By the rapidly increasing number of commercial drones, also known as Small Unmanned Aircraft System (S-UAV), the threat generated by these assets and the burden on air traffic management systems is also raising. According to the latest Eurocontrol estimates, the number of drones sold in Europe is about 1-1.5 million pieces and still growing. [1, p.17.] Being the threat intentional or unintentional, a highly capable countering system shall be formulated in order to protect industrial facilities, governmental buildings, military facilities, sports stadiums and any other important interests identified by the government and by proper agencies or professional organisations.

The management of harmless hobby, business, or governmental drone traffic and the protection against intentional drone threat require a highly capable and extremely complex solution. On the one hand, the former category (harmless drone traffic) should be managed by a mostly procedural unmanned traffic management system and judicial means. On the other hand, for the protection against the latter one (intentional drone threat) another complex solution shall be formed. However creating such a system looks a bit far away and needs plenty of work and tests, the theoretical basis is already exists and in effect for decades. NATO AJP 3.3.1 B, which document is the Allied Joint Doctrine for Counter-Air, describes complete, really thorough and proven active air defence functions.

2. The Light and Dark Sides of Drone Employment

Even if the majority of drone traffic is not hurtful or obviously beneficial, it has to be managed. For first, the author gives an overview on the positive side of drone application. The most common area is the hobby use of drones. It is for the joy of people, for instance a parent plays with his/her child, creating aerial pictures or motion picture, and so on. The employers of drones from the business sector might be the agriculture-, film-, energy-, security-, traffic and transportation-, mining- or construction industry and even the commerce area. [1, p.23-28.] The third great area of drone application is realised by the governmental sector. Drones might be utilized by the low enforcement [2], disaster relief [3] and of course governmental buildings, military facilities, sports stadiums and any other important interests identified by the government and by proper agencies or professional organisations.

Besides from the beneficial areas we must be aware of the risks and threats posed by drones. Even the most threat meant by drones is not intentional. In most cases the reason is lack of skill, poor navigation, unknown regulations, lost contact signal, technical failure and so on. In the recent history several incidents or accidents has been registered: drone fallen in the garden of the White House (USA); danger close to German Chancellor Angela Merkel; drone harmed sportsmen, reporter, and spectators; drone endangered airplane and helicopter; drone crashed into buildings and flew into stadiums dangerously; etc. [5] In London, UK Gatwick Airport was closed for more than 36 hour due to unknown drone presence [6] and also in London, just one hour closure at Heathrow Airport effected more than 1 000 airlines, due to drones as well. [7] All the former incidents could be committed unintentional due to the above mentioned reasons or even intentional. Unless the perpetrator is arrested, the origin of intention is really difficult to find out.

The other great source of risks is the kamikaze like use of drones as a weapon and also the armed use of drones by aggressive non-governmental organisations or terrorist organisations. Given sources date the first armed use of drones for the 1990s [8, p.360], others originate it for the early 2000s by Hezbollah. [9] The most experienced employer with the most extensive roles of drones is the Islamic State of Iraq and Syria (ISIS). This organization possesses facilities for modifying drones for their “special” purposes and for training of drone pilots for the roles of reconnaissance, attack and inducing panic amongst the opposing armed forces and public. [10, p.2-14.] [11] Besides the former activities, several other injurious acts can be mentioned: information smuggling, [12] or item smuggling into prisons, [13] or even transportation of radioactive material. [14] As a summary of directions of risks and threats posed by drones, see the figure below (Fig. 2.).
In order to the aggressive drone traffic be manageable and the perpetrators also could be located, much more active measures shall be implemented than it was presented in the former section. In this section the intention of the author is not to create another brochure like collection – others have already done that – but to present an overview on the categories of active means of countering drones, which will be also important elements of a counter-drone system. These means can be divided into three main classes.

The first group of active counter measure elements consists of different types of airspace surveillance assets. These sensors provide the majority of information on threats from the air and fundamentally determine the situational awareness, therefore the success of the counter-drone activity. The most common resource of airspace control is a radar based sensor system. In case of counter-drone activity, the acoustic surveillance is also a quite effective solution, furthermore electro-magnetic wave detection or electro-optical sensing augmented with infrared sensors are applied as well. [21]

Another group of counter-drone means is the different types of jammers. In this case also different types of solutions exist. The communication between the controller and aircraft can be disturbed, the aircraft itself [21] [22] and even the global positioning can be jammed as well. [23] In this scenario we can talk about a real counter-measure where the controller and the aircraft will be separated. At certain areas this is a more preferable way of denying drones than shooting them from the sky, though this might be a slower and less certain solution.

The third, final and most violent group contains the kinetic countering methods, mostly weapons. One way can be an interceptor drone which drops a net on the attacking drone. [21] Furthermore kinetic means can be missiles, cannons, guns, personal weapons, laser- or microwave weapons, etc. [25, p.90-91.] [26] [27] Causing collateral damage is a very high risk factor during applying any of the former measures, the falling parts and debris and flying projectiles necessitate precise and careful employment.

5. Counter-drone activity as a system

Echoing the author’s observations from above: during the study of this topic, there was no book, study or paper which has given a comprehensive approach on countering drones. In this last section, for first the scientific classification will be discussed of counter-drone activity, than a build-up of comprehensive synergetic drone managing system will be recommended.

In Military Sciences, the counter-drone activity can be classified into Air Power Theory, from the five core Air Power Roles (Counter-Air, Attack, Information Collection, Air Mobility and Personnel Recovery) [28, p.1-8–1–17.] it can be classified into the role of Counter-Air. Finally in Counter-Air role, countering drones shall be recognised as a Defensive Counter-Air activity with both the sub-categories of Active- and Passive Air Defence (Fig. 3.).

It is quite obvious and easy to understand that the former traffic management system is for a cooperating user who is able and willing to observe the regarding rules of the air. For the aggressive and harmful use of drones a different, aggressive and harmful active system of counter measures is needed.

4. The Active Counter Measures against Drones

In order to the aggressive drone traffic be manageable and the perpetrators also could be located, much more active measures shall be implemented than it was presented in the former section. In this section the intention of the author is not to create another brochure like collection – others have already done that – but to present an overview on the categories of active means of countering drones, which will be also important elements of a counter-drone system. These means can be divided into three main classes.

The first group of active counter measure elements consists of different types of airspace surveillance assets. These sensors provide the majority of information on threats from the air and fundamentally determine the situational awareness, therefore the success of the counter-drone activity. The most common resource of airspace control is a radar based sensor system. In case of counter-drone activity, the acoustic surveillance is also a quite effective solution, furthermore electro-magnetic wave detection or electro-optical sensing augmented with infrared sensors are applied as well. [21]

Another group of counter-drone means is the different types of jammers. In this case also different types of solutions exist. The communication between the controller and aircraft can be disturbed, the aircraft itself [21] [22] and even the global positioning can be jammed as well. [23] In this scenario we can talk about a real counter-measure where the controller and the aircraft will be separated. At certain areas this is a more preferable way of denying drones than shooting them from the sky, though this might be a slower and less certain solution.

The third, final and most violent group contains the kinetic countering methods, mostly weapons. One way can be an interceptor drone which drops a net on the attacking drone. [21] Furthermore kinetic means can be missiles, cannons, guns, personal weapons, laser- or microwave weapons, etc. [25, p.90-91.] [26] [27] Causing collateral damage is a very high risk factor during applying any of the former measures, the falling parts and debris and flying projectiles necessitate precise and careful employment.

5. Counter-drone activity as a system

Echoing the author’s observations from above: during the study of this topic, there was no book, study or paper which has given a comprehensive approach on countering drones. In this last section, for first the scientific classification will be discussed of counter-drone activity, than a build-up of comprehensive synergetic drone managing system will be recommended.

In Military Sciences, the counter-drone activity can be classified into Air Power Theory, from the five core Air Power Roles (Counter-Air, Attack, Information Collection, Air Mobility and Personnel Recovery) [28, p.1-8–1–17.] it can be classified into the role of Counter-Air. Finally in Counter-Air role, countering drones shall be recognised as a Defensive Counter-Air activity with both the sub-categories of Active- and Passive Air Defence (Fig. 3.).

It is quite obvious and easy to understand that the former traffic management system is for a cooperating user who is able and willing to observe the regarding rules of the air. For the aggressive and harmful use of drones a different, aggressive and harmful active system of counter measures is needed.

3 Edited by the author based on references [5]-[14].
conducted as far from the friendly operations area as feasible. They aim to detect, identify, intercept, negate or preferably destroy enemy air and missile forces attempting to attack or penetrate the friendly air environment. Effective employment of limited assets across a broad front can only be achieved by prioritizing tasks and managing risks. Consequently, the ability to react effectively must be premised on a comprehensive infrastructure facilitated by detailed planning.” [29, p.5-1.] When the reader changes the words of air and missile attack for drone attacks – which are also threats from the air against a nation’s (vital) interests – the definition will still be valid and credible.

The one of the two sub-categories of Defensive Counter-Air is Active Air Defence and the other one is Passive Air Defence. “Active AD is direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. It includes the use of aircraft, air defence weapons, EW, and other available weapons. Integration of these weapon systems will allow for a defence in depth, using multiple engagements.” [29, p.5-1.] “Passive AD consists of all measures, other than active air defence, taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets. These measures include camouflage, deception, dispersion, and the use of protective construction. …” [29, p.5-1.]

For a complex and active counter-drone system NATO AJP 3.3.1 B also provides the framework, the doctrine defines Active Air Defence Functions as follows:

- Detection;
- Routing;
- Identification;
- Transmission of information;
- Assignment of weapons;
- Control of weapons;
- Engagement;
- Combat assessment;
- Recovery of aircraft.

A comprehensive synergic drone traffic managing system should be consisting of Active- and Passive Air Defence segments. The classic Passive Air Defence measures are less applicable in this case, but the above discussed administrative means for drone traffic management can be interpreted as the passive subdivision. The active part mostly consists of the means of the former sections, which are incorporated into the Active Air Defence Functions along with some other measures and procedures. In order to create such a visioned system every element is on the shelves, our task is to work with, integrate and test them.

Analogously with the classic Active Air Defence Functions the functions of an active counter-drone subsystem should be the following:

- If the drone poses threat towards the given facility, after a quick threat analysis, the proper type of counter-measure and procedure is selected;
- After that selection, the application of proper active counter-measure or procedure occurs. This might be jamming, forcing the drone to land, application of impulse weapon, or employment of any kinetic mean;
- Finally, an assessment should be performed whether the countering activity was successful and whether the system was able to cope with the threat. After the assessment the countering system returns to its base state and the surveillance of the airspace continues.

6. Summary

The counter-drone activity cannot be and will not be effective by utilizing individual counter measures and drone traffic managing means parallel. From the available resources, know-how and best practices an integrated and synergic counter-drone system should be formulated which contains active and passive means as well. During the resources no company was found which would be perform such an integration, the author reckons that such an effort would be feasible by a state, or rather an alliance of states, like NATO.

In the NATO thinking about countering drones must be a really highlighted topic, because these small remotely piloted aircraft systems redefine the airspace sovereignty. For mall states or non-governmental (even terror) organisations with restricted finance opportunities, drones provide access to such Air Power capabilities which would be unreachable in case of the mere accessibility of conventional air assets.

References


Abstract: Cyber security and threats are increasingly associated in everyday life. They are capable of generating a sense of threat to everyone. But is it really real threats and how do we recognize them?

KEYWORDS: CIBERSECURITY, THREAT
вина за тези състояния носят националните елити. Гарантирана предпоставка киберсигурността на национално ниво да е разбирането, че рисковете и заплахите за сигурността, които водят към връщане на война, аналогични за насочените за досегашните състояния, твърдения, че имаме уредена организация със засегнато максимално количество обекти и сфери на общественото, далена държава или коалиция[26]. Европа: Глобални заплахи и интегрирана сигурност. Интернет мрежата допълва каналите за проникване, въздействие, манипулиране на информацията, провеждане на машини за пропагандни мероприятия. Това обяснява, че кибератаката е съществен предмет за противодействие като една от видовете проявления на киберпрестъпността следва да се търси непрекъснато обособяване и затваряне, от което се изгражда на възможности за нейната уязвимост. Киберпрестижността оценява качеството, а не адекватността ни... Необходимо е обогатяване и осъвременяване разбираемите за сигурността, като се отчитатъ съвременни и перспективи възможности за нейната уязвимост.
PSYCHOLOGICAL MODEL FOR THE INVESTIGATION OF ESCAPES FROM PLACES OF IMPRISONMENT.

Abstract: Various approaches and studies are being analysed regarding the interpretation of escapes from places of imprisonment. A comprehensive, complex and integrated model for psychological analysis of escape from penitentiary institutions has been developed, based on the dynamic interaction of the fugitive personality and the situation.

KEY WORDS: PERSONAL VALUES, SELF-ESTEEM, CHARACTERISTIC FEATURES, MOTIVES, MENTAL STATES, PREPARATION, ESCAPE REALISATION, HIDING SCENARIO. KEYWORDS:

1. Увод

Актуалната необходимост от прецизното психологическо изследване на бягствата на лишениите от свобода се обуславя не така от техния брой, а от опасностите, които те пораждат. Лишените от свобода-беглец добре осъзнават, че може да бъде физически ликвидиран, заловен или отново да се завърне в затвора с увеличена присъда. По тези причини той се намира в превъзбудено и фрустрирано състояние, поради което с лекота може да реагира неадекватно, насилствено по отношение на обкръжаващите го.[12]

Успешно извършени бягства от затворите в нашата страна за периода 1995-2013 година са съпроводени в 70% от случаите с реализирането на користни или насилствени прояви. Същевременно лишениите от свобода след всяко напрегнато, тревожно, възбудимо преживяване, неустойчивост, конформизъм, упоритост, високо самомнение, което се съчетава с трайна асоциална насоченост и ригидност, значително потисна вътрешните имунизации и резерви в контактите с обществеността и медиите много остро реагират на успешното изпълнение на плана за бягство или отново да избегне преследване заради проблемни отношения, опасения от престъпни дейности, които се възникват и функционират в актуалната ситуация. Подобна роля изпълнява желанието за контакт с жена или бързото получаване на удоволствие от доза доминация и защита на личното пространство.[10, 14, 12, 8]

2. ПРЕДПОСТАВКИ И НАЧИНИ ЗА РЗРЕШАВАНЕ НА ПРОБЛЕМА.

При психологическата интерпретация на бягствата от затворите се създават условия за правилно и диференцирано преценно отношение към посочените мотиви за бягство, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещи устойчиви мотиви за бягства, презентиращи водещите устойчиви мотиви.
борбата специално внимание се обръща на преживяването от тях на наличната ситуация като персонално значима, психотравмираща и фрустрираща.[15] В отделни публикации се поставя акцент върху недостига на персонал, неговата демотивация и емоционално прегаряне, допуснатите грешки при оценката на рисковите в поведението на лицата от свобода и дефицита от технически средства за реализация на охраната.[10] Всички тези външни предпоставки заедно и поотделно се перцептират от осъдените като шанс за осъществяване на бягство.

Сценарните за извършване на бягство са описани в следната последователност:
а) интелектуално-манипулативен - чрез представяне на безлъч за друг осъден, на който предстои освобождаване;
б) авантюрично-моторен - с преходяване на височини, заграждения, решетки, врати;
в) авантюрично-насилиствен вариант с използване на оръжие, заложници, транспорт, извършване на групово бягство.[6]

Бягствата от местата за лишаване от свобода се анализират като динамичен процес, който включва подготовка, неординарно извършване и укриване след бягството. [8, 11, 1] Авторите, които са склонни към процесуална интерпретация на бягствата, проследяват спецификата на тяхната ситуация и психическите състояния на осъдените при реализацията на всеки един етап. Особен интерес представляват сценарните за действие след извършване на бягството.[2] Първият от тях предполага укриване в голяма манисополис, при което извършителите могат да съхранят анонимноста си за дълъг период от време и да развива със съвместна работа. Бегълците, предпочитат този тип сценарий, защото могат да се интерпретират като групово бягство, с преобладаване на вътрешни мотиви. Вторият сценарий е свързан с използване на право на пълноценно извършване на бягство и през извършването на бягство. В този смисъл той е съдържателно-процесулен и отчита динамиката на интеракциите на основните структурни компоненти. Това позволява изграждането на по-ефективен и рационален подход за анализ на изживяването от бягството, въпреки че дълго време не са бягство се стават на вътрешно неадекватно явление. От същия идея можем да достигнем до резултат, че бягствата от местата за лишаване от свобода са една от основните причини за преживяването от бягството.
Личностните предразположености са само предпоставка, която влиз в действие при наличието на конкретни ситуации. От своя страна те могат да детерминират съзнателното търсене, целенасоченото, последователно създаване и провокиране на ситуации за бягство.

При подходяща ситуация и предизвикана от нея интензивна мотивация и стресов психически състояния, дори при отсъствие на подходящи личностни свойства от типа на импулсивност, ниска стресоустойчивост, слаб самоконтрол и повишена агресивност, може да се реализира бягство. Това се потвърждава от множество примери от собствената ни психологодиагностична, консултативна и управлена практика в местата за лишаване от свобода.

Мотивиращата роля при бягствата играят и психическите състояния и в частност фрустрацията, но тя все пак се предизвиква от определена ситуация. Трябва да се изготвя и важното обстоятелство, че взаимодействието на бъдеще. отреагиране, за да се преживее в момента така желаното на наличните ценности, самооценка и характер, които се много важна роля, но това става възможно благодарение на разглеждането на дадения практически казус ситуацията има осъдени, младежи в пенитенциарна система. Техните извършители са непълнолетни опит за бягство.

Непълнолетен правонарушител изтърпява присъда с лишаване в последния момент. Това се случва, когато съответния бягство на непълнолетните осъдени от затворническа хистеричния тип. Допълнително тя може да се драматизира модифицират в следствие на конкретна ситуация. на лишените от свобода, но те се пораждат, усилват и бягствата.

По-късно проведеното в рамките на предизвикана от инцидента проверка психиедиагностично изследване на осъдения-беглец показа, че става дума за личност с егзистенциално-самоосъзнателна ориентация и малоценностен тип самооценка, затворен, регулярен, упорит, който продължително се фокусира върху своите негативни преживявания. Ситуацията на понесената обида поражда в него устойчив мотив за постигане на възмездие. Неговата практическа реализация е свързана с находчиво, решително и смело осъществяване на авантюрно-мотиран сценарий на бягство, предполагащ справяне с врати, решетки и охранителни заграждения.

Впоследствие осъденният пристъпва към увреждане в пуста, безпомощна страда. След като в течение на десет дни не е открит след интензивни изграждали мероприятия, той сам се предава на полицията, тъй като смята, че е постигнал желаното възмездие и справедливостта е възстановена.

Разглеждането на този конкретен случай от нашия пенитенциарна практика отново потвърждава възможността на изградения структурно-процесуален модел за психологическа интерпретация на конкретно бягство, базиран на съществено-динамичните интеракции на личността и ситуацията.

6. Заключение.

6.1. Научно-изследователските проекти, посветени на бягствата от местата за лишаване от свобода, както и дейностите по практических психологорганизм, превантивно-консултативните мерки и извършителите мероприятия за заявяване на беглеми, потвърдяват актуалната необходимост от създаването на цялостен, интегриран и комплексен модел. Той трябва да съдейства за повишаване качеството на извършване психологически анализ, прогнозиране и интерпретиране на разнообразните случаи на бягство от пенитенциарните институции.

6.2. Новият концептуален модел се основава на динамичното взаимодействие между личността на беглем и ситуацията. Той включва както интегралните, базови личностни образования като ценностни ориентации, самооценка и характерологични черти, така и психо-динамични компоненти като мотиви и психически състояния.

6.3. Базовите и психо-динамичните личностни структури взаимодействат по различен начин в ситуацията, която по определен начин ги активира, потиска или модифицира тяхното влияние върху избираемия тип поведение.
Integrative and dynamic structures in the personality of the refugee can significantly determine the orientation towards corresponding situations, their perception, and use as favorable for committing escapes from different categories of penitentiary institutions.

6.4. The new model possesses structural and procedural components. The latter present the stages of each escape from the place of deprivation. They are preparation, implementation, and evasion. The actual implementation of the escape means utilization of one of the three variants: intellectual-manipulative; adventurous-motoric; adventurous-violent. Besides, the model also contains scenarios for evasion, which are generally referred to as camouflage in the big metropolis or evasion in a deserted, deserted place or an unoccupied building.

6.5. The application of the newly formed conceptual model to even the most specific and unique cases of escapes confirms its heuristic, analytically-interpretative possibilities.

6.6. The new model was used for psychological analysis and interpretation of the actions of preparing for escaping from the place of deprivation by persons of high risk for committing escape. The action was identified as a potential risk for escaping from the place of deprivation.

The proposed conceptual model can successfully interact with the specific features and uniqueness of the case. The action was identified as a potential risk for escaping from the place of deprivation.

The specified conceptual model can successfully interact with the specific features and uniqueness of the case. The action was identified as a potential risk for escaping from the place of deprivation.

7. Literature


2. Маджаров, Е. Пенитенциарная психология. С. „Албатрос“, 2016, стр.189-200.


5. Андреева, Г. Социальная психология. М. „МГУ“, 1980, стр.121.


7. Демольский, М. Методические рекомендации по проведению психodiagnosticеского обследования осужденных. М. ФСИН России, 2008, стр. 32 (Демольский М., Васильев А., Ильин А., Матеев, И. Рассказчикова Е.)

8. Дмитриев, Ю. Пенитенциарная психология. Ростов н/Д „Феникс“, 2007, стр.447-448 (Дмитриев, Ю., Казак, Б)
HARMONIZATION OF THE HUMAN FACTOR IN INTEGRATED AVIATION SECURITY SYSTEM

Filippov V.L., Ovchenkov N.I.

1 State research Institute of civil aviation, Moscow, Russian Federation
2 P.G.Demidov Yaroslavl State University, Yaroslavl, Russian Federation

Abstract: Aviation security in the Russian Federation as a scientific direction deals with the problems of protection of civil aviation from unlawful interference in its activities, including the use of integrated aviation security systems. One of the most important problems in this area is the problem of the human factor. The paper discusses the harmonization of the human factor in security systems.

Keywords: Civil aviation, aviation security, human factor, integrated systems, harmonization of the human factor.

1. Введение

Обеспечение авиационной безопасности рассматривается с двух сторон. Это может быть некоторая деятельность, направленная на предотвращение незаконного вмешательства в деятельность гражданской авиации. Применительно к аэропорту эта деятельность направлена на предотвращение возможного нарушения его нормальной функционирования в результате воздействия криминальных или других угроз. Реализуют указанную деятельность должностные лица аэропорта, его персонал, служба авиационной безопасности, государственные правоохранительные органы и иные структуры. Обеспечение АБ можно рассматривать также как результат указанной деятельности, при этом этот результат невозможен, можно только стремиться к достижению некоторого приемлемого состояния. В таком случае возникает понятие уровень авиационной безопасности, т.е. количество отражение состояния защищенности объекта. Эта величина динамически изменяется под воздействием угроз (внешних и внутренних) и принимаемых мер защиты объекта.

Основными задачами обеспечения авиационной безопасности являются: прогнозирование, выявление и устранение угроз авиационной безопасности, оперативное реагирование на них, эффективное применение соответствующих методов и средств обеспечения авиационной безопасности.

Традиционные подходы к построению систем безопасности не выдерживают объективных требований времени. Основным концептуальным требованием к современной системе безопасности является соблюдение баланса между безопасностью и комфортом пассажиров. Существуют два подхода к построению систем безопасности. Первый подход делает ставку на человека, который считается предпочтительным и надежным элементом системы, второй основан на минимизации человеческого фактора.

Проблемы совершенствования системы обеспечения авиационной безопасности аэропортов нельзя рассматривать в отрыве от внешних и внутренних условий, в которых аэропорт осуществляет свою производственную деятельность.

Условия определяются мировыми тенденциями развития цивилизации: отсутствие общеприятных идей социального взаимодействия, обеспечивающих развитие права в межгосударственном обмене; противоречия между государственными, межнациональным и межэтническим характера сглаживаются, но темп этих изменений не могут удовлетворить мировое сообщество; в условиях истощения природных ресурсов в мире усиливается борьба за неё; противоречивые тенденции в современных условиях развиваются ускоренными темпами. С учётом этих факторов меняется характер террористической деятельности, т.е. внешние условия: она усиливается и расширяется, появляются новые формы, она становится более изощрённой, усиливается тенденции сепаратизма, стремление дестабилизировать политическую обстановку, укрепляются финансовые возможности террористических организаций.

На этом фоне существенно меняется характер аэропортовой деятельности: изменяется и усиливается нормативная база, регламентирующая производственную деятельность аэропорта; изменяется и усиливается технология организации воздушных перевозок и обслуживания пассажиров и воздушных судов.

Все вышеперечисленное выдвигает новые требования к системам обеспечения авиационной безопасности аэропорта. В этих целях изменяется нормативная база, решаются финансовые проблемы, увеличивается номенклатура и сложность технических средств обеспечения авиационной безопасности.

Принципиальные проблемы управления авиационной безопасностью состоят в следующем.

Авиационная безопасность - состояние. Аэропорт - объект транспортной инфраструктуры, включая все его элементы, персонал и пассажиров. Если говорить о состоянии этого объекта, то его следует рассматривать как единую систему, в противном случае оценить состояние невозможно.

Вторая проблема состоит в управлении авиационной безопасностью, т.е. этим состоянием. Чтобы управлять чем-то, необходимо уметь это что-то измерять, оценивать и сопоставлять с нормативным значением. В случае несоответствия – принимать меры. Применительно к авиационной безопасности, необходимо уметь измерять уровень безопасности, решить проблему единиц измерения и шкалы, тогда можно говорить о реальном управлении.

2. Человеческий фактор в авиационной безопасности

Человеческий фактор - совокупность врожденных и приобретенных качеств личности авиационного персонала, которые являются основой или сопутствующей причиной тех или иных нестандартных ситуаций в условиях полета или вне его [1,2].

Как показывает практика, система авиационной безопасности, ориентированная на человека, в значительной степени зависит от лояльности конкретного специалиста, поскольку рабочего человека системой безопасности находятся в его руках, что определяет негативные проявления, например:
несанкционированный пропуск на объект/с объекта; не постановка объектов и периметра под охрану; несанкционированное снятие объекта с охраны; не доведение информации о тревожных событиях до руководства; сокрытие информации о неработоспособности систем обнаружения; выявление системы безопасности или ее элементов из строя; инсценировка поломок; временное отключение электропитания и освещения с целью парализовать систему видеонаблюдения и другие.

К этому перечню добавляется личностная составляющая человеческого фактора: физиологические и психологические ограничения, невозможность обрабатывать большой поток информации, сообщения о множественных тревогах и т. д. [3,4].

Негативные последствия человеческого фактора приводят к тому, что ситуация становится слабоуправляемой, что снижает эффективность системы, откуда появляется задача привести влияние человеческого фактора к минимуму.

Человеческий фактор продолжает оставаться "ахиллесовой пятой" любой системы безопасности. Людям свойственно ошибаться. Следует признать, что ни одна система безопасности не застрахована от влияния человеческого фактора полностью. Но современная система должна сводить это влияние к минимуму: чем меньше возможность человека влиять на систему, тем ниже риск ошибок [5].

Проблема традиционных систем безопасности в том, что они бессильна обнаруживать симптомы подготовки противоправных действий. Они добросовестно зафиксируют сам факт совершения действия и предупредят меры по его ликвидации. Но в современной ситуации важна именно превентивная функция. Предупреждение угроз безопасности намного эффективнее, чем их отражение и ликвидация дефектов, когда ценное время уже упущено и ущерб нанесен.

Общий уровень безопасности объекта зависит не только от использования высокотехнологичных систем, но и от способности этих систем обмениваться информацией в единой базе данных, обеспечивающей принципиально более высокий уровень защиты.

3. Интегрированные системы авиационной безопасности

Основным направлением развития систем обеспечения авиационной безопасности является создание интегрированных систем. Интеграция всех имеющихся систем и технических средств на общей платформе вместе с созданием программы анализа и предоставления информации позволяет поднять безопасность объекта на качественно новый уровень. Интегрированные на единой платформе технические средства позволяют обеспечить автоматизированную и систематическую проверку настроек оборудования, осуществлять дистанционное контроль работы сотрудников службы безопасности, устранять инциденты и давать консультации по работе с оборудованием из единого диспетчерского центра.

Само по себе оборудование для защиты объекта является не более чем инструментом, с помощью которого формируется поток информации, необходимый для принятия человеком решения о мерах по защите объекта. Когда же вся техника объединена в единую информационную систему, контроль может задаваться автоматически и регулироваться одновременно на всем оборудовании в зависимости от уровня угрозы.

Интеграция не должна сводиться к простому созданию единых хранилищ данных и выводу всей информации на средства отображения информации коллективного пользования. Интеграция должна позволять проводить анализ разнородной информации на предмет выявления критических событий с высокой степенью точности. Принцип минимизации человеческого фактора должен закладываться в систему на этапе разработки концепции: все, что может обработать компьютерная техника - она должна обрабатывать и предоставлять информацию в наиболее простом и доступном виде [6-7].

Основная функция системы - аналитические отчеты по накопленной информации. При формировании отчета используются алгоритмы принятия решений. При этом субъективное мнение оператора минимально. В систему безопасности должны быть заложены механизмы самоконтrolля работоспособности ее элементов.

Отсюда возникает проблема интегрированных систем, а именно: соблюдение в динамике оптимального в смысле некоторых критериев баланса между комплексом технических средств обеспечения авиационной безопасности и человеческим фактором. При этом отдельной проблемой становится вопрос о критериях оптимизации. Это означает, что вопрос об управлении интегрированным комплексом технических средств должен рассматриваться не только в плоскости функционального управления, но и в области управления системными параметрами интеграции, т.е. система авиационной безопасности должна быть адаптивной, а управление ситуационным.

Основная задача эффективной системы безопасности: как можно раньше обнаружить и идентифицировать угрозу, оперативно оповестить ответственных лиц и обеспечить выполнение всех необходимых действий по реагированию. Временной период с момента обнаружения угрозы до ее ликвидации должен быть меньше, чем время, необходимое противнику для преодоления технических рубежей защиты и нанесения ущерба [2]. При создании интегрированных систем безопасности возникает ряд проблем:

1. Широкий спектр средств обеспечения авиационной безопасности ставит проблему актуализации их номенклатуры и оптимизации связей между ними, т.е. проблему оптимизации организационной структуры системы.

2. С учётом динамического характера угроз, против которых выстраивается такая система, возникает проблема динамического управления структурой системы обеспечения авиационной безопасности аэропорта.

3. Система авиационной безопасности, тем более интегрированная система, относится к категории сложных систем эргатического типа, в которых баланс между человеческой и технической компонентами должен быть оптимальным для данных условий эксплуатации системы. С учётом динамики угроз соотношение указанных компонентов должно регулироваться, т.е. система должна быть адаптивной.

Для их решения необходимо реализовать следующие функции [9,11]:

− минимизировать затраты на оснащение объекта за счет интеграции систем и использования существующей инфраструктуры;

− объединить все системы безопасности объекта в единую информационную среду, с единой базой данных и единым подходом к анализу событий и принятию решений;

− задавать разнообразные алгоритмы взаимодействия систем по сигналам друг друга;

− автоматизировать принятие решений для типовых ситуаций;

− вести комплексный автоматизированный анализ данных по событиям всего комплекса, включая сопоставительный анализ показаний разных систем по выбранным событиям и т.д.
обеспечить оперативное предоставление руководству достоверных данных; 
оперативно оповещать персонал службы безопасности и координировать их действия; 
снизить количество информации, поступающей к оператору, и сделать ее более наглядной; 
убыть вероятность ошибочных действий оператора; 
минимизировать зависимость системы от конкретного исполнителя и снизить негативное влияние человеческого фактора.

Каждая интегрированная система авиационной безопасности уникальна, т.е. не имеет полных аналогов поведения, что определяется существенным различием в исходных моделях (модель объекта, модель защиты, модель угроз и т.д.).

Исследуемые системы в достаточной степени плохо идентифицируемы, поскольку знание алгоритмов поведения отдельных элементов системы не позволяет сформировать на этой основе функционал ее деятельности, который зависит, прежде всего, от ситуации, поэтому в таких системах точный прогноз их поведения на основе предыдущих событий практически невозможен.

Интегрированные системы сугубо стационарны, т.е. их главная задача состоит в том, чтобы сохранить заданное состояние или процесс, что определяется способностью устранять последствия внешних и внутренних воздействий.

4. Гармонизация человеческого фактора в авиационной безопасности

Прежде всего, о понятии. В общепринятом смысле гармонизация понимается как взаимное согласование, сведение в систему, унификация, упорядочение и т.п. В этом смысле гармонизация человеческого фактора в авиационной безопасности представляет более сложной. Выше было показано, что человеческий фактор в системах безопасности должен быть минимизирован.

Проблема состоит в том, что абсолютная минимизация в данной предметной области с учетом выполняемых специалистом-оператором функций практически невозможна. С другой стороны, критерии минимизации в современных системах безопасности тоже не определены. Поэтому вопрос о минимизации, очевидно, следует ставить как вопрос о гармонизации, т.е. как некоторое упорядочение, согласование человеческой компоненты и технических средств. Тем не менее, вопрос о критерии остается открытым.

Производственная деятельность специалиста-оператора в системе авиационной безопасности состоит из двух частей: деятельность в соответствии с заданной программой, когда результат только положительный, и деятельность с нарушениями заданного алгоритма, превышающая специалиста в антагониста системы, а результаты его деятельности в негативные проявления. Вопрос о причинах такой деятельности требует отдельного исследования, здесь достаточно отметить, что именно такая деятельность должна быть минимизирована. Отсюда, появляется критерий минимизации человеческого фактора, а именно: время обнаружения негативного проявления. Ним же называется, единый функционал системы управления авиационной безопасностью должен быть дополнен функцией мониторинга и анализа производственной деятельности специалиста в области авиационной безопасности и принятия соответствующих решений по отстранению специалиста от выполнения своих функций в момент времени, когда его деятельность становится негативной.

В современных интегрированных системах управления авиационной безопасностью реализация указанной функции принципиально возможна и достаточно хорошо координируется с выполнением системой основного функционала. На рис. 1 обобщенно представлены этапы алгоритма реализации основного функционала системы по отработке некоторого негативного события, названного инцидентом. На этот алгоритм накладывается алгоритм мониторинга и анализа производственной деятельности специалиста.

Рис. 1 Структура анализа инцидентов

В рамках анализа инцидентов выполняются следующие процедуры по отработке результатов мониторинга производственной деятельности специалиста [12,13].

1. Момент регистрации негативного события, т.е. фиксируется событие, когда производственная деятельность специалиста стала сугубо негативной.
2. Фиксируются результаты мониторинга, которые раскрывают суть негативного проявления.
3. Событие сравнивается с шаблонами аналогичных событий в базе данных, определяется его статус и уровень опасности. Запускаются процедуры реагирования.
4. Принимается решение о мерах безопасности и запускаются процедуры перестройки системы, которые включают изменения структуры технических средств, человеческих ресурсов, подключаются резервное программное обеспечение.
5. Инцидент ликвидируется, когда негативное воздействие приводится к приемлемому уровню. Запускаются программы фиксации и архивирования.

5. Заключение

Подсистема перестройки структуры учитывает человеческий фактор с точки зрения его возможной минимизации. В этой подсистеме формируются параметры управления системой обеспечения авиационной безопасности в части, касающейся режимов работы технических средств и параметров их структуры, включая управление персоналом. В ситуации центре интеграции сосредоточены средства сбора, обработки, анализа и исследования совокупной информации о ситуации в системе обеспечения авиационной безопасности аэропорта и выработки соответствующих решений по управлению, в том числе персоналом. Для решения этих задач требуется достаточно высокий уровень автоматизации, хотя при этом определенная часть управления остается в сфере эвристических решений, т.е. осуществляется лицом, принимающим решения.
6. ЛИТЕРАТУРА

2. Елисов Л.Н., Овченков Н.И., Фадеев Р.С. Введение в теорию авиационной безопасности (под ред. Л.Н. Елисова), Ярославль: Филигрань, 2016. 320 с.
5. Елисов Л.Н., Овченков Н.И. Авиационная безопасность как объект математического моделирования // Научный вестник МГТУГА. 2017. Том 20, № 3. С.13-20
7. Елисов Л.Н., Овченков Н.И. К вопросу структурного моделирования субъектов транспортной безопасности. Научный вестник Московского государственного технического университета гражданской авиации. 2013. №197. С. 58-61
8. Елисов Л.Н., Овченков Н.И. Интегральная безопасность воздушного транспорта. Научный вестник МГТУГА, том 20-М.: МГТУГА, 2017, № 6-с.36-44
10. Овченков Н.И., Елисов Л.Н. Оценка уязвимости объектов транспортной инфраструктуры и транспортных средств в гражданской авиации // Научный вестник МГТУГА. 2014. № 204. С.65-68.

REFERENCES


ABOUT THE AUTHORS

Filippov Vadim L., State Adviser of the Russian Federation, 1-st class, Acting Director General, The State Scientific Research Institute of Civil Aviation, Ministry of Transport of the Russian Federation, 67, Mikhalkovskaya Street, building 1, 125438 Moscow, Russian Federation; gosniiga@gosniiga.ru
Ovchenkov Nikolay I., Candidate of Technical Sciences, Associate Professor of the Department of Theoretical Informatics, Yaroslavl State University named after P. G. Demidova, Ministry of Education and Science of the Russian Federation, tsvetkovskaya Street, 14, 150003 Yaroslavl, Russian Federation; e-mail: ovchenkov@electronika.ru
ISLAM: THE FRIGHTENING RELIGIOUS OTHERNESS

Assoc. Prof. Dr Veselin Bosakov,
Institute for the Study of Societies and Knowledge – BAS, Sofia,
vesobos@abv.bg

Abstract: Against the backdrop of the changing role of religion in geopolitical relations, and in connections with the identified global threats to humankind (such as terrorism, organized crime, human trafficking, etc.), a considerable number of theorists and ideologues focused on the problem of security are relating these threats to the growing activism of religious minorities in various parts of the world, and specifically of supporters of the extreme, fundamentalist version of Islam. Speaking of security, we must inevitably think of fears. The latter are about personal and public safety or the anxiety that society may stop functioning. Widespread fears have a corrosive, long-term effect on social cohesion and stability. The social exclusion of ever-greater groups of people spreads to more and more spheres, such as those of the economy, the market, politics, education, healthcare, etc. The increasing marginalization of groups of people, and the inability of institutions to resolve the problem, result in the search for a scapegoat – the role of such may fall upon the political elites, ethnic minorities, migrants. Identifying an enemy is a precondition of social conflict. We are increasingly afraid of one another as we have become accustomed to believing that our worlds are so different that there meeting would bring about the end of at least one of them. Labeling, supported by passionate qualifications, has proved to be a universal way of dealing with the unfamiliar. Woe to him who cannot define himself and continues naively to believe we can live together without the aid of stereotypes. The oldest and strongest human emotion is fear, and the oldest and strongest fear is that of the unknown. Some of the images related to contemporary Islam are formed not within the House of Islam, but where the religious community is obliged to coexist with others. The change of representations of the so-called European Islam can be identified in Bulgarian reality as well. The willingness to adopt and follow certain principles of conduct typical for the arguments of fundamentalism grows in direct proportion with the growing variety of the immediate social environments of Muslims. In fact, the spaces of fundamentalist interpretation of the religious canon are formed not within the traditional Muslim communities but at the points of their active contacts with other cultural and religious models.

KEYWORDS: ISLAM, SECURITY, FEAR, ENEMY, FUNDAMENTALISM, COMMUNITY, NEIGHBORHOOD, TENSION, CONFLICT, OTHERNESS

The first level at which we may construct arguments for the formulation of new research questions is connected to the specific dimensions of the desecularization process, as discussed by Peter Berger. In this sense, is it possible to assume that religious faith is able once again to reintegrate the everyday representations of people regarding the significance of their difference with regard to the others? Is it possible that the post-modern situation will form a new need for belonging in terms of the total identification framework of religion? And if so, how is the representation of religious difference constructed? What levels of commensurability or opposition are being articulated with respect to the religiousness of the Other? Beyond the abstract dimensions of interaction between different religious systems, new challenges arise for researchers of the field of religiously reconstructed social reality of neighborhood. Assuming that the level of shared, immediate social experience is correlated with higher tolerance towards religious difference, how true is it that the absence of tolerance will always provoke higher levels of conflict and non-recognition of the right of the Other to be different? In other words, if the spatial and social differences are in direct proportion to each other, can we assume that it is possible to achieve a shared perspective on the right of equality of what pertains to the Other even when it is not part of the everyday life of people? Hence, can the declared tolerance continue to be a substitute basis for building a set of shared cultural values? In the context of present-day Bulgarian reality, do we have reason to claim that specifically religious distances and tensions are arising, or are we witnessing a fervid loyalty to religious dogma as a means for compensating for the long period of declared and militant atheism? Even more concretely, would Islam be such a problem for Bulgarian society if it were not negatively linked to a dramatic part of Bulgarian history? May we expect that rejection and disregard for the right of existence of a different religious doctrine would exist in the same degree towards other world religions, such as Buddhism (for instance)? Is this a matter of attitude toward a different religion or a complex set of ascribed characteristics, a kind of attributive identity of every cultural difference, perceived as favored or legitimized through unequal access to power or other deficit resources?

The traditional scale of sociological analysis treating of the relations between secular and religious, between the sacred and the profane, is no longer sufficient for interpreting the similarities in meaning or the essential differences between the democratic norms on one hand and the revived religious practices in the Muslim environment on the other. In interpretations of the on-going processes in the Islamic life-world, there prevails a schematic understanding of Islam, which views this religion as opposed to the very notion of democracy, civil rights, and personal liberties. The leading schema of interpretation in this case has acquired the form of the following syllogism: Every form of Islam is a fundamentalism; Every fundamentalism is terrorism; Therefore, every form of Islam is terrorism.

But reality actually offers many reasons for rethinking such a schema of interpretation. Religious values, as general representations and as a picture of the world, influence not only the individual attitudes and behavior but also the degree of tolerance and social solidarity between different ethnic-religious communities. Against the backdrop of the new fundamentalisms and the accelerated social transformations brought about by the so-called second modernity that characterizes the risk society, the problem of values becomes increasingly topical in a sociological and philosophical aspect. The integrative and disintegrative functions of values and their instrumentalization may lead either to the consolidation or to the breakdown of social ties; so knowledge of these functions is crucial as a possible remedy for the kind of active ignorance that involves suppression of, or disregard for, the real problems that exist.

Some basic questions need to be answered:

- How do the representations of Muslims encompass simultaneously the image of the citizen on one hand and, on the other, the Islamic religious identity formed under the conditions of a new horizon (the global media and the intensified religious consciousness leading the faithful to believe? Is this layers of their religiosity) that draws the local community into a unified Ummah?
- Is it possible to correlate religious freedom and freedom in a democratic society; in other words, to juxtapose freedom as a personal, political, and economic choice and freedom in the religious sense?
Is there an area of shared interpretations and moral norms that mediates between the democratic vs. the religious principles in the Muslim environment?

Is an Islamic modernity possible, and if so, how would it be related to the democratic values of an essentially secular political system?

In a methodological aspect, the analysis of Islam under conditions of modernity may be situated in the context of the dichotomy “traditional vs. modern”. The two sides of this dichotomy should be taken as ideal types in the Weberian sense. Ideal types are instruments for achieving the tasks of the social sciences. Attempts had been made to use ideal types even before Max Weber, but without methodological awareness, so that confusion occurs between ideal types and the laws of historical generalization. Weber’s ideal types are not colored by value-judgments and are not related to “perfection”, except in terms of logical perfection. They are not generic concepts, i.e., they are not a set of traits that pertain to all the objects belonging to a certain class. Nor are they statistical averages. They are not the constant essence of things, which is gradually discovered in the course of investigation. The ideal type is an instrument constructed by the researcher in order to structure the in-itself amorphous reality and to thereby make possible the understanding of that reality. In its conceptual purity, the ideal type is not to be found in empirical reality. The elements of the ideal type are empirical in origin, but they are stylized, and their assembly into a unified mental picture represents a completely artificial construction. The closer the investigated reality comes to the ideal type, the more it lends itself to comprehension according to the chosen viewpoint. If a given ideal type proves to be of no heuristic value and does not enable an interpretative understanding of empirical reality, for the purpose of which it was mentally constructed, it should be discarded and another ideal type should be constructed in its place, which should be tested in turn by means of empirical study. Ideal types are neither “true” nor “false”. They are only an intellectual game, the purpose of which is to attain knowledge of concrete cultural phenomena and their structure, their determining conditions (Weber 1968).

The ideologists of the Islamic revival have developed the doctrine that the modernization of the Muslim community is to be achieved only through the prism of religion; they have argued the need for a contemporary interpretation of Islam that matches the challenges of modern times. The revival and transformation of Islam provoked by its dynamic encounter with a constellation of rationalities that modernity represents reveals the specific connection of Islamic activism to the process of modernization. This process is understood in a specific way, whereby modernity is not perceived as a transition from theonomy to autonomy and as a shift of the emphasis of meaning from the past to the future. In taking advantage of the modern achievements of science and technology, Islamic activism restricts the use of the technological innovations of Western science only to the dissemination of Islam.

The process of religious revival of Muslims in Bulgaria cannot be simply interpreted as re-Islamization, as some researchers are inclined to see it. It is rather a rediscovery and re-affirming of the values of Islam as a philosophy of life and a moral practice under the conditions of growing diversity of cultural models of social integration. In itself, this process cannot be defined either as encouraging social integration or as a kind of incitement to closure to and distancing from, the rest of society. It is rather a sort of community response to the disintegration processes and growing social inequalities in Bulgarian society today. The traditional Muslim community used to maintain its own cultural measure without trying to spread its values via active dialogue with the other religious groups, especially not in open debate with the official atheism of state policy. Today’s forms of religious mobilization in the Muslim community are significantly different, especially in respect to its willingness not only to strictly follow the requirements of the religious canon but also to preach the values of Islam. The so-called folk Islam has been deeply rethought in the context of modern democratic development and under the impact of contradictory trends that have been defined as a new Islamic culture and that indicate the effort being made to build a new, specifically Islamic, modernity (Bosakov 2015).

The analysis of the Islamic community (the Ummah) as a space of total identity can be meaningfully conducted in two basic aspects: the existing notion of community that Muslims have, and the specific nature of the mutual personal and community ties that the faithful maintain when coexisting with the Others. The unwavering idealization of the Ummah in both the historical and theological aspect is a trend that shapes individual and collective consciousness. People are seen as either believers in Allah or non-believers, as either “House of Islam” or “the House of War”. Armed conflicts are either a “holy war” for the true faith or “internece conflict” (Fitnah). Taxation is either sanctioned by Sharia law or is non-legitimate, etc. In this concrete but comprehensive sense, religious affiliation, the belonging to the Ummah, is established, maintained and transmitted as the fundament of a person’s life; it turns into a total identity. Given the dissolved boundaries between the religious and the secular sphere, the religious norms become a factor that regulates and largely predetermines the social and political reality in the Ummah. In Islamic cannon, all possible human activities are encompassed by two categories: permissible (halal) and prohibited (Haram). The religious identity of the true believer would be impossible without this all-encompassing regulation. In other words, all values in Islam are refracted through the lens of “religion”, which is not one value among others but is the integral environment that determines, encourages or penalizes human conduct. How is the integration of the faithful within modern society and the nation state made possible? To what degree are the inner dynamics and cohesion of the Islamic community influenced by the transformations occurring in society? (Given that these are transformation whose historical memory is linked to a different religious dimension and whose political development in history includes periods of passionate rejection of all religious traditions.) Closely connected with these two questions are two essential aspects of the norm in the Islamic community: 1. The prescribed rules of relations and conduct in the family, and 2. Canonical principles of the relation between parents and children and, in a broader aspect, between adults and young people.

Regardless of the canonic differences between various religions, each of them expresses an image of an enduring, meaningfully ordered world. This image attains its ultimate justification by turning into a certain way of life. In this sense, religious values, as a driving force of individual and collective actions, serve as an explanatory reference point that gives us access to the social dimensions of religion. The analysis of the influence of religious convictions upon people’s everyday life illuminates an important dimension of their religiousness. The latter inevitably includes actions undertaken out of religious motives that carry religious meaning. In other words, by shedding light on the mutual connection between religious attitudes on one hand and values such as justice, family and work on the other, it is possible to answer the question to what extent these values are a resource for constructing the meaning of the community ties and for strengthening them. In the perspective of dialogical sociology and the tools of the European Values Study (data for Bulgaria, Fourth Wave 2008/2009) we find that the processes of growingly dynamic influence of religious identity are typical not so much for a homogenous religious environment as for the Muslim communities that co-exist with other ethic-religious group (Bosakov 2009).

How is the full integration of a religious community like the Islamic one into modern Bulgarian society possible? Significant changes have taken place in traditional Bulgarian Islam. Some of the basic actors of these changes at present are the young Muslims who are now still in high school or university.
They are the future spiritual elite of the Muslim community in Bulgaria and will contribute to the formation and consolidation of new dimensions and dynamics in the process of integration. The attitudes and standpoints of these young people, the values they uphold, will to a great degree define the direction that the process of integration of religious communities takes in the secular democratic political model. That is why part of the research efforts for understanding the integration problem of the Islamic community in modern Bulgarian society should be increasingly focused on analyzing the representations, reasons and arguments of the spiritual and intellectual elite of the Muslim community in Bulgaria. Together with this, we share the view that the Muslim community in our country is singular only in the perceptions of non-Muslims. The internal differentiation and fragmentation in the life world of present-day Islam is a fact of fundamental importance that must not be underestimated. That is precisely why the focus of research is, among other things, the internal heterogeneity in what is perceived to be the unified impact of religious education in the Muslim milieu.

The analysis indicates that the scope of declared tolerance is much greater than it seemed to be in the past, or, at least, that our striving to distinguish stable processes of social integration with respect to cultural development have diminished the critical attitude towards some of the obtained results. There is no reason to presume there has been a qualitative change in the level of knowledge about the religious foundations of the Other. Over a comparatively long period of time (during the past twenty years at least) the importance of spatial proximity in the everyday reality of cultural variety has remained the same. The boundaries of real dialogue and tolerance remain strongly dependent on the direct shared experience in life and society of individuals from different ethnic-religious groups. Hence the attitude towards Islam in Bulgaria confronts us with a far more important issue – that of the limits to which the fear of what is different can be surmounted. Are there reasons to believe there is a more important issue than the fear of what is different? The question is: who is actually speaking on behalf of Islam – in Europe, throughout the world, and in our country? How valid is the exchange of thoughts and the mutual understanding in the face of public debate? Is there a double perspective, a specific communication strategy of the Muslim community, which may be sending out certain messages outside and different messages inwardly, to the brothers and sisters in the community? Could this double meaning be part of the reason for the lack of mutual understanding, or does the reason lie mostly in the various dimensions of the phenomenon that we traditionally define as a crisis of identity?

The transformation of the representations regarding the so-called European Islam can be identified in Bulgarian reality. The willingness to accept and obey certain rules of behavior typical for fundamentalism grows according to the variety of the immediate social environment. In fact, the spaces of fundamental interpretation of the religious canon are formed not where the traditional Muslim community exists and develops, but at the borderline of its active contacts with other cultural and religious models.

With time research is clearly confirming the hypothesis that the attitude towards ethnic and, even more so, religious difference is mediated and defined to a great degree by the problem of power. Concrete cases taken from the Bulgarian political environment prove the high degree of connection and mutual dependence between the forms and intensity of religious separation on one hand and access to power resources on the other. That is why every attempt at taking a partisan approach to the problem or using it for short-term political aims, essentially enhances the feeling of otherness in the Muslims, perceived by them as a situation of inequality, and hence strengthens the internal ties within the community and the search for new grounds of difference from the society at large. The processes of religious revival among Muslims in Bulgaria cannot be interpreted one-sidedly as a threat against the secular nature of the state or social peace. Above all, they indicate the need for dialogue. Passing from negative to positive polarization is possible only by increasing dialogue, by active interaction which preserves differences as an incentive for integration. In the perspective of “dialogical sociology”, but also in a wider cultural sense, integration into the world of modern-day Islam is a fact of fundamental importance that must not be underestimated. That is precisely why the focus of research is, among other things, the internal heterogeneity in what is perceived to be the unified impact of religious education in the Muslim milieu.

One of the major problems related to research on Islam continues to be the degree of legitimacy of its representatives and the measure of shared meanings and symbols interpreted in a communication context. The question is: who is actually speaking on behalf of Islam – in Europe, throughout the world, and in our country? How valid is the exchange of thoughts and the mutual understanding in the face of public debate? Is there a double perspective, a specific communication strategy of the Muslim community, which may be sending out certain messages outside and different messages inwardly, to the brothers and sisters in the community? Could this double meaning be part of the reason for the lack of mutual understanding, or does the reason lie mostly in the various dimensions of the phenomenon that we traditionally define as a crisis of identity?

The transformation of the representations regarding the so-called European Islam can be identified in Bulgarian reality. The willingness to accept and obey certain rules of behavior typical for fundamentalism grows according to the variety of the immediate social environment. In fact, the spaces of fundamental interpretation of the religious canon are formed not where the traditional Muslim community exists and develops, but at the borderline of its active contacts with other cultural and religious models.

With time research is clearly confirming the hypothesis that the attitude towards ethnic and, even more so, religious difference is mediated and defined to a great degree by the problem of power. Concrete cases taken from the Bulgarian political environment prove the high degree of connection and mutual
postmodern age that are forcefully entering into the life of society will be integrated without contradiction in the body of ethical views and values typical for the orthodoxy and orthopraxis of Islam;

- The admissibility of religiousness is not yet closely matched by respect for the right of others to be different and to follow religious norms different from one’s own;
- The negative trends of development in the relations between tolerance vs. toleration of a different religious identity is a sign of an unfocused mass consciousness (toleration is primarily determined by the restricted option to be other than tolerant, rather than by an authentic culture of tolerance and respect for the different others).

The arguments in support of democratic values, which are usually centered around human rights (that seem particularly problematic in the practice of Sharia) are still not convincing enough for the youngest generations of Muslim living in multicultural societies. The very principle of multiculturalism, based on recognition of the right of difference of others, does not seem adequately protected in the everyday practice of present-day public life. The right to difference and acceptance of difference does not exhaust the problem of coexistence, where the building of a community seems to depend on the expanding influence of the fundamental values of that community. The norm of multiculturalism is only the first step, the mandatory precondition for engaging in dialogue with difference. At least for the time being, it seems that Western civilization and Bulgarian society are not prepared to take the next step and maintain their values while engaging in dialogue on terms of equality in the course of building new, supra-religious communities. The notion that integration amounts to unification or assimilation based on acculturation, on partial elimination of the cultural grounds of difference is leading, more than ever, to the reverse result. Decreasingly effective is the prospect of some kind of social integration that should compensate for the lack of shared values as a basis of coexistence. Representation can no longer make up for the lack of equality. Encouraging participation, even in the completely ineffective form of quota representation, has long since ceased to be the answer to the problem of quality integration into Bulgarian society. Formal recognition of the right to hold a different opinion does not signify willingness to accept this opinion as being of an equal standing or equally significant and valuable in building a shared notion of reality. Respect for difference must grow into willingness to have a personal position in an expanding space of mutually accepted dialogue that is perceived as a necessary part of life in society. Only then will the existence of different ethnic, cultural, and religious communities become a guarantee of the viability and integrity of the national community itself. The construction of an integration model based on authentic dialogue is yet to come. Without knowledge of difference and otherness, there can be no field for dialogue, which is the proper place for the encounter between “us” and “them”. Such knowledge is also a powerful means for reducing the ethnoreligious distances that make difference and otherness grow into alienness. The changing reality in society is continuously putting in question the framework of the stereotypical knowledge of others that restricts people’s expectations and their willingness for joint efforts.

In Europe, the Other is primarily the Muslim. The latter is most often an immigrant, whose social position is defined almost entirely by his/her limited access to resources. The Muslim is usually centered around human rights (that seem particularly problematic in the practice of Sharia) are still not convincing enough for the youngest generations of Muslim living in multicultural societies. The very principle of multiculturalism, based on recognition of the right of difference of others, does not seem adequately protected in the everyday practice of present-day public life. The right to difference and acceptance of difference does not exhaust the problem of coexistence, where the building of a community seems to depend on the expanding influence of the fundamental values of that community. The norm of multiculturalism is only the first step, the mandatory precondition for engaging in dialogue with difference. At least for the time being, it seems that Western civilization and Bulgarian society are not prepared to take the next step and maintain their values while engaging in dialogue on terms of equality in the course of building new, supra-religious communities. The notion that integration amounts to unification or assimilation based on acculturation, on partial elimination of the cultural grounds of difference is leading, more than ever, to the reverse result. Decreasingly effective is the prospect of some kind of social integration that should compensate for the lack of shared values as a basis of coexistence. Representation can no longer make up for the lack of equality. Encouraging participation, even in the completely ineffective form of quota representation, has long since ceased to be the answer to the problem of quality integration into Bulgarian society. Formal recognition of the right to hold a different opinion does not signify willingness to accept this opinion as being of an equal standing or equally significant and valuable in building a shared notion of reality. Respect for difference must grow into willingness to have a personal position in an expanding space of mutually accepted dialogue that is perceived as a necessary part of life in society. Only then will the existence of different ethnic, cultural, and religious communities become a guarantee of the viability and integrity of the national community itself. The construction of an integration model based on authentic dialogue is yet to come. Without knowledge of difference and otherness, there can be no field for dialogue, which is the proper place for the encounter between “us” and “them”. Such knowledge is also a powerful means for reducing the ethnoreligious distances that make difference and otherness grow into alienness. The changing reality in society is continuously putting in question the framework of the stereotypical knowledge of others that restricts people’s expectations and their willingness for joint efforts.

REFERENCES


Bosakov, V. 2006. Identity and Diversity of Islam in Bulgaria (in Bulgarian) [Identichnost i mnogoobrazie na islyama v Balgariya. Sofiya: Virtualen tsentar za muzika, kultura i nauchni izsledvania]

Bosakov, V. 2000. The Bulgarian Turks between the Culture of Neighbourhood and Religious Identity. Sofia: LiK Pbls (in Bulgarian) [Balgarskite tursi mezhdu kulturata na sasedstvo i religioznata identichnost. Sofiya: LiK]


COMPETENCE CENTRES AND INTELLIGENT SECURITY SYSTEMS IN BULGARIA

Chief Assistant Dr. Eng. Panevski V.S.
Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski”, Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: Joint Research Center, as a European Commission’s structure for science and knowledge, provides independent research to support the overall European Union policy. Innovative tool for dealing with expected and/or emerging challenges that need to be addressed at EU and Member States levels, and understood by the political environment is the building of competence centers. Centers focus their work on the development of analytical tools that can be applied to each policy area. A concrete example of rational national approach for implementation of this policy is establishment of the Center of Competence “Quantum Communication, Intelligent Security Systems and Risk Management” (Quasar). Thereby it is anticipated that innovative collaborative approaches and practices will be developed between different organizations with responsibility in the field of higher education and science, aiming at the modeling and development of interoperable, at national and European level, intelligent security systems.

Keywords: COMPETENCE CENTER; INTELLIGENT SECURITY SYSTEMS

1. Introduction

In the modern scientific world where the flow of knowledge increases, there is a greater need of review and analysis of that information. The Joint Research Center (JRC), as the European Commission’s (EC) Science and Knowledge Structure, provides independent research to support the overall European Union (EU) policy. An innovative tool for addressing anticipated and/or emerging challenges that need to be addressed at EU and Member State level and understood by the political environment is the building of competence centers (CC). The EC’s CCs focusing its activities on the development of analytical tools that can be applied to each policy area. At the same time, the Commission is developing the Knowledge4Policy (K4P) Platform from 2018, which supports the development of evidence-based policies, thus linking the world of policy makers (ideally developing a public policy based on reliable scientific evidences) and the scientists who develop this evidences. A key element of this policy is CCs, with 5 CCs being set up and functioning at the moment and in the process of being created is European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [1].

Thus established CCs are focusing on the development of analytical tools that can be applied to any area of policy, bringing together in one place a wealth of experience in this field. Through their members’ rich experience, they contribute to policy making, consult with their choice, and work directly with the EC Directorates-General to implement the tools to solve political issues. Their work has a direct impact on citizens’ lives, contributing to the results of research into a healthy and safe environment, secure energy supply, sustainable mobility and health and safety of consumers.

In our country, under the Science and Education for Smart Growth Operational Programme, in the process of development are centers of competence in research and innovation in the areas, identified in the Strategy for Research and Innovation for Smart Specialization. By creating such research infrastructures of regional and national importance, the specialization of Bulgarian researchers and their participation in the European Research Area will be supported. A specific example in this direction is the Center of Competence “Quantum Communication, Intelligent Security Systems and Risk Management” (Quasar) [2]. It is expected that innovative collaborative approaches and practices to be developed in synergy by different organizations with responsibility in higher education and science. The modeling and development of compatible at national and European aspects, intelligent security system will be done under the leadership of the Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. Angel Balevski” at the Bulgarian Academy of Sciences (IMSETHC-BAS), which will be discussed in the following text.

2. Center of Competence “Quantum Communication, Intelligent Security Systems and Risk Management” (Quasar)

The concept of the construction of the CC Quasar is aimed at creating a network of resources forming a modern large-scale research infrastructure in the field of information and communication technologies that will help to achieve Bulgaria’s and EU’s research and technological development goals. Within the project will be implemented four work packages of the 8 partners, one of which is the Work Package 2 ‘Intelligent Security Systems’ (WP2). This working package is headed by the IMSETHC-BAS. The activities included in WP2 concern the area of intelligent security systems and business continuity management, which will contribute to the development of an innovative, multifunctional, basic, sensory system providing critical infrastructure security and sites with national, regional and local importance, as well as capacity building to significantly modernize existing specialized research capabilities.

As a result of the implementation of WP2 it is expected to be provided:

- Improving social security in our country by developing an innovative, multi-functional, basic, multisensor security system having the ability to: intelligent motion detection (detection and identification); constant video surveillance under different climatic conditions and periods of the day; registration, storage, archiving and visualization of information; operation, mobility and autonomy;
- Significant modernization of existing specialized research infrastructures to meet the needs of researchers and innovators;
- Structuring of the processes and business models for R & D management in the interest of organizations / enterprises to enhance their competitiveness;
- Building comprehensive research and innovation capacities, integrating planned research with the development of new and emerging technologies, and optimizing opportunities for implementing research results and for developing innovative activities;
- Establishing medium-term competitive advantages for CC participated organizations carrying out research and innovation activities as well as for those who will apply their current developments.

Within WP 2, cooperation will be developed with international partners from Europe, USA and Asia which are leaders in the field of security systems building, as well as international standardization. At national level, in addition to the partners in this project and the Bulgarian Defense Industry Association member organizations, it would be useful to deepen the relationships with the interested national structures both in the management of security and defence, and the management of critical infrastructure. The outlined areas of cooperation development are as follows:
Through their participation in many national and European projects in recent years, specialists from IMSETHC-BAS have developed various types of sensors and sensing systems for security. The more important ones, which represent the structural basis of the intelligent security system and their parameters, will be optimized during the project are [6]:

- Development of hardware for security systems – sensor elements, tools for wireless data transmission; tools for data visualization and means for the system cyber security;
- Development software model/models for the security systems – sensor elements, tools of wireless data transmission; tools for data visualization; means for the systems’ cybersecurity; decision/decisions in complex risk situations and software for management of the entire system;
- Preparation of functional documents for the security systems operation;
- Development of a simulator of the security systems;
- Training of specialists from the interested structures (institutions, enterprises, institutes and universities) to work with the security systems;
- Coordination of the processes of the security systems development and construction and the Business Continuity Management (BCM) of the critical infrastructure;
- Development of a business model for the management of scientific research and innovations in the organization;
- Protection and transfer of intellectual property among the participants as a result of the developments.

3. Areas of impact of the results of the planned scientific researches and experience of the IMSETHC-BAS

As a result of the scientific activity, on a national and global scale, there are different technologies that are used in the protection systems of both critical infrastructure and sites of local importance. For example, for the creation of nuclear security, various approaches such as “Estimate of Adverse Sequence Interruption (EASI)”, “Systematic Analysis of Vulnerability to Intrusion (SAVI), or “Analytical System and Software for Evaluating Safeguards and Security” ASSESS) “, developed by US research institutes and laboratories, but they represent an acquainted picture (in a two or three dimensional reality) for only one direction of impact on the objects (or in a separate, probable direction). This means that the technological responses we have today are insufficient to cope with the scope and potential severity of possible threats (terrorism or natural disasters). Instead of using technology to keep pace with the emerging dangers and the changing circumstances, we should rather anticipate the realization of possible threats and develop “superior” security systems that protect citizens, guarantee their freedoms and do not hamper travel and commerce [3]. Developing technologies to "overcome" the possible risky events requires vision and strategy, and good strategy makes it difficult to choose.

On the basis of the above, the structure and content of research and technology in the field of intelligent security systems can be defined, but is not limited to, the following functional areas: sensors and sensor systems; analytical support and decision making systems; protection and prevention systems; response, recovery and reconfiguration systems; new and emerging threats and vulnerabilities; design of modern infrastructure architecture and systems; human and social problems and others [4]. Innovation activities that will be realized within the WP2 related to the opening of new integrated approaches to the development of intelligent security systems of critical infrastructure and sites of national, regional and local importance, which will show their specificity. These systems will be distinguished by: extended autonomy of operation; minimizing the impact of environmental and working factors on technical characteristics; ability to self-control and indication of violation of system element parameters; wireless data transfer and cybersecurity processes; element mobility and compatibility with the functioning national and European security systems in the field of CI protection and the environment. Greater emphasis will be placed on ensuring critical infrastructure sustainability [5] through intelligent security systems.

IMSETHC-BAS experience

Within WP 2, the main types of organizations in the field of research and innovation we plan to develop cooperation with are the research institutes from BAS and the universities, training specialists in the field of informatics, electronics and security. For the implementation of a specific link with the business – national and international – we will direct our efforts to optimize the relationships with companies from Spain, Greece, UK, France, Romania, USA, which are leaders not only in the theoretical aspect of critical infrastructure security systems building but also have and improve their own and developments in this area.

type of research and innovation organisations for cooperation

In the period 2001–2013, in the conditions of implementation of the project “DEVELOPMENT OF TOOLS NEEDED TO COORDINATE INTER-SECTORAL POWER AND TRANSPORT CIP ACTIVITIES AT A SITUATION OF MULTILATERAL TERRORIST THREAT. INCREASE OF THE PROTECTION CAPACITY OF KEY CIP OBJECTS IN BULGARIA – BULCIP”, ref. # HOME/2010/CIPS/AG/019, specialists from IMSETHC-BAS specialists from the institute developed and successfully tested an integrated security system model. Through this model is presented matrix of minimum mandatory requirements for building a reliable system to counter potential threats (manmade risk events or natural disasters) leading to an increase in the security and protection of critical infrastructure.
leading technology companies and research organisations for developing a strategic cooperation

As a result of the participation in the preparation and implementation of national and international projects and contracts, successful relationships have been established and developed with many organizations operating in the field of education, science and research and business organizations. The strategic cooperation with them will be used in terms of creating abilities and their subsequent development in the field of security systems, as follows:

- R&D organisations: University of Cuprus, Department of Civil and Environmental Engineering, School of Engineering (www.ucy.ac.cy/cece/en); Kauno Technologijos Universitetas (Kaunas University of Technology) – Lithuania (http://ktu.edu/en); NTNU Sustainability Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology – Norway (https://www.ntnu.edu); Technical University of Cluj Napoca – Romania (www.utcluj.ro/en); Democritus University of Thrace – “Production and Management Engineering” Department, Greece (http://duth.gr/index.en.shtml); Athena Research and Innovation Center in Information, Communication and Knowledge Technologies – Greece (www.athena-innovation.gr/english.html).

- Business organisations: SYNYO GmbH – Austria (www.synyo.com); DEVERYWARE – France (www.deveryware.com); NIER Ingegneria S.p.A – Italy (www.niering.it); D’Appolonia S.p.A – Italy (www.dappolonia.it/en); IES Solutions – Italy (www.ieszolutions.eu); ACCENT PRO 2000 s.r.l. (AP2K) – Romania (www.acent.ro).

- Bulgarian Defence Industry Association - through the involvement of member organizations implementing security and defense activities;


4. Expected results and potential for their implementation

- Expected results

Within the framework of WP 2 the realization of a complex of activities it is envisaged in the following directions:

- Significant modernization of existing specialized research infrastructures necessary to meet the needs of research and innovation workers;

- Structuring of the processes and business models to manage research and innovation activities in the interest of organizations / enterprises to increase their competitiveness;

- Comprehensive research and innovation capacities establishment, integration of planned research with the development of new and emerging technologies and optimizing the possibilities for implementation of the results of research and development of innovative activities;

- Establishment of medium-term competitive advantages for organizations involved in the Competence Center and conducting research and innovation, as well as those who will apply their state-of-the-art developments.

- Potential users of scientific results

Potential users of scientific results are the national organizations responsible for the maintenance of critical infrastructure (national and European), defense industry enterprises, central and local administration buildings, higher and secondary education establishments, theaters, important transport centers and etc. The themes of the security systems and the innovative approaches for implementing the management of the continuity of the organization’s activities are of interest to the curricula of the higher education institutions, the “G. S. Rakovski” National Defence College, the “Vasil Levski” National Military University and the Nikola Vaptsov Naval Academy, the Academy of the Ministry of Interior, the Ministry of the Interior and Ministry of Defence, as well as the state administration agencies with security responsibilities, incl. critical infrastructures.

- Necessary upgrade actions to use the results

After performing complex functional tests of the security system models developed within the WP 2, an analysis of what has been achieved will be carried out. For developed models will seek commercialization through negotiation with partner organizations at national and international level. In this way optimization of the upgrade of the developed models of the system is also expected, depending on the additional requirements of the partners.

- Opportunities to implement the results of research and development of innovative activities

The results of innovative research and development within the WP 2 are complex interest - both for producers and for consumers. After conformation the technological readiness level achieved, security system models will be offered to interested national and international organizations.

5. Conclusion

Within the framework of WP2, the research program of the CC in the field of intelligent security systems has an undeniable advantage to start not from scratch but from the height of built basic level of competence and extensive experience, including international experience of participants. Precisely in that way it is expected improvement in the value chain - from research and development passing through the market applicability of research results and reaching solving socio-economic and security challenges.

Investment in skills, research infrastructure, research and innovation will support competitiveness, will remove obstacles to increasing efficiency and will stimulate innovation capacity to achieve convergence with other EU countries.

Literature:


STANDARDIZED APPROACHES FOR THE INTEGRATION OF MANAGEMENT SYSTEMS OF THE CRITICAL INFRASTRUCTURE OBJECTS

Abstract: Over the past few years by the International Organization for Standardization (ISO), were developed different standards for management systems, aiming to manage different sectors of activities of organizations (businesses). Practice shows that despite many common components, they are not sufficiently coordinated, which hinders stakeholders to streamline and integrate their management systems. That’s why, in this paper, authors will present a systematic research process of integration texts into existing standards, in the area of requirements for Management Systems and especially for the Business Continuity Management, with the leading role of Quality Management System, in the organizations which essentially represent objects of critical infrastructure.

Keywords: QUALITY MANAGEMENT SYSTEM, BUSINESS CONTINUITY MANAGEMENT; CRITICAL INFRASTRUCTURE, SECURITY AND PROTECTION.

1. Увод


Като следствие от този факт, обнародваните и в нашата страна стандарт БДС EN ISO 22301:2015 - “Сигурност на обществото. Системи за управление на непрекъснатост на бизнеса. Изисквания” се явява пилотен в тази област и изготвен съгласно изискванията на Ръководство 83 [2].

По традиция и следвайки добрите практики, в днешно време се разработват отделни фирмени системи за управление, за решаване на въпроси като качество, околна среда, здраве и безопасност на труда, финанси, човешки ресурси, информационни технологии и защита на данните.

От какво е продиктувана необходимостта от създаване на Система за управление на непрекъснатостта на дейността на обекти от КИ? Непрекъснатостта на бизнес-процесите и системите съдържа в себе си управленчески дейности и интегрирани планове, които съдържат условия за поддържане на непрекъснатост на критичните за дадена организационна/обект от КИ процасти [3].

Тази област обхваща всички аспекти на една организационна единица, които участват в поддържката на критичните процеси, а именно: личния състав; стадийни фондове; доставчиците; материалите; технологиите; данните. Нейната определяща роля особено се засяга, когато става въпрос за гарантирането на непрекъснатото функциониране на критични инфраструктурни обекти и най-вече на тези, които се определят като тази в енергетиката и транспорта.

Гарантирането на непрекъснатото функциониране на критични инфраструктурни обекти, е една от заложените иди в създаването в Република България на Център за компетентност “Квантов комуникация, интелигентни системи за сигурност и управление на риска” (Quasar) по Проект BG05M2OP001-1.001-0006, финансиран от Европейски Съюз по Оперативна програма „Интелигентен растеж“.

2. Същност на проблема

Съществуват многобройни подходи, начини и средства за създаване на условия за непрекъсната дейност на такива инфраструктурни обекти, които в различна степен отразяват тяхната специфика. От тях, налице са и различни степени и нива на сигурност за гарантиране на непрекъснатостта на бизнес - развитието им.

Усъвършенстването на теорията и практиката за планиране на непрекъснатото бизнес развитие, както и обмъцването на опит и добри практики, допринасят за повишаване на сигурността на съответните икономически или организационни субекти, но липсата на единни модели за еднотипни обекти води до поява на несигурност по отношение на степените им на жизненостоносимост, т.е., липса обективен критерий за сравнение и оценка на степента на устойчивост на обекта в различни критични ситуации. Отчитайки факта, че такива обекти са в основата на критичната инфраструктура на всички страни-членки на Европейския съюз, от съществено значение е да бъдат създадени условия за надеждна оценка и постигане на нужната степен и ниво на сигурност за гарантиране на непрекъснатостта на развитието им.

Природните бедствия, екологичните аварии, технологичните грешки и кризите, предизвикани от човешки фактор показат, че тежки излискания може и ще се случват, което оказва въздействие както върху общественото, така и на частния сектор. Предизвикателствата надхвърлят обекта на плановете за реакция при извънредни ситуации или стратегии за управление при бедствия.

Организационите, от всички видове и големина, и особено тези които влизат в категорията критични, трябва да участват във всекидневния и систематичен процес на превенция, защита, готовност, смекчаване и отговор за осигуряване на непрекъснатостта на дейността и нейното възстановяване. Вече не е достатъчно да се изготви план за отговор, който предвидя и ще се случват, което оказва въздействие както върху общественото, така и на частния сектор. Предизвикателствата надхвърлят обекта на плановете за реакция при извънредни ситуации или стратегии за управление при бедствия.
Днес доброто управление на непрекъснатостта на дейността не означава принудително предприемане на мерки срещу външно въздействие, а по-скоро признаване на положителните ефекти от използването на добrite практики за непрекъснатост на дейността, показани на Фиг. 1, които са създадени в организацията [5].

Фиг. 1 Добри практики в областта на непрекъснатост на дейността

Приемането на ефективен процес за УНД носи полза в редица сфери от дейността на организацията, сред които са:
- защита на активите (собствеността);
- подобряване разбирането за дейността, постигнато чрез идентификация и анализ на риска;
- оперативна устойчивост, постигната като резултат от прилагането на подход за намаляване на риска;
- намаляване на прекъсванията, чрез дефиниране на алтернативни процеси и времеви подходи за реакция на непредвидени проблеми или рискове;
- свързани подходи, които могат да идентифицират и управляват алтернативните процеси;
- жизненоважни записи, които трябва да бъдат поддържани и защитени;
- последици за законодателството в областта на здравето и безопасността и задължения за полагането на грижи към персонала;
- подобрена ефективност във функцията на отделните организации;
- запазване на пазарите, като се гарантира непрекъснатост на доставките на стоки и услуги;
- подобряване на цялостната сигурност на организацията (обект КИ).

Вземането на решение за създаване на СУНД, на базата на БДС EN ISO 22301:2015, обикновено е приемливо, тъй като политиките и подобрият период за сертификация.

По правило организацията трябва да се прилага унифицирани план за осигуряване на непрекъснатост на дейността на всички елементи. За създаване на условия за даване на ефективен отговор, по отношение на поддържането на оперативна непрекъснатост, такъв план трябва да бъде подпомогнат към спецификите на организирания риск и катастрофални сценарии, които биха могли да вирият от загуба на основна стражда до локална повреда в системата за реализация или подръжка на основната дейност. По-групата задача състои във възникване, който да балансира изискванията на стандарт, потребностите на бизнеса и крайния срок за сертификация.

Не съществува единен план за прилагане на БДС EN ISO 22301:2015, който ще работи за всяка организация, но има някои общи стъпки, показани на Фиг. 2, които ще позволят балансиране на често противоречивите изисквания.
БДС EN ISO 22301:2015 е документ от нов тип, в който е осъществена на най-високо ниво пълноценна интеграция на структура и текст, в пълно съответствие с Ръководство 83 (ISO Guide 83) за стандарти за Системи за управление. Той е изготвен в отговор на критиците, че доколкото сегашните стандарти имат много общи компоненти, те не са достатъчно съгласувани, което затруднява организациите да рационализират и интегрират своите системи за управление.


БДС EN ISO 9001:2015 не съдържа изисквания, специфични за други Системи за управление - управление на околната среда, управление на здравето и безопасността при работа, управлението на финансовите или управлението на риска. Въпреки това, този международен стандарт дава възможност дадена организация/обект от КИ да съгласува или интегрира своята собствена Система за управление на качеството с изискванията на съответната система за непрекъснато управление на дейността. Възможно е обекта от КИ да приспособи своето (своите) съществуваща(и) система(и) за управление, за да създаде Система за управление на качеството, съответстваща на този международен стандарт [6].


5. Заключение

От показаното по-горе е видно, че основополагащ стандарт за системи за управление се явява БДС EN ISO 9001:2015. Това означава, че своевременното изграждане и пълнообемното функциониране на Системата за управление на качеството в една организация съдържаща основа за реализация на Системата за управление на непрекъснатостта на дейността. Именно осигуряването на непрекъснатост на дейността на всяка организация/обект от КИ е теория и практика, които водят началото си от не съвсем отдавна. Затова и опита да се покажат начините и способите за интегрирането на системата, която се изгражда за решаването на свързаните с непрекъснатостта на дейността въпроси, е категорично логичен и актуален.

Това от една страна ще позволи да се определи нейното място в палитрата от системи, формиращи съдържанието на едната Система за управление на дейността/бизнеса на всяка една компания или обект от критичната инфраструктура, а от друга, ще определи приюса, който тази система може да осигури за пълноценното, устойчиво и непрекъснато удовлетворяване на потребностите на тези които потребяват техните услуги/продукти.

Литература:
CONTENT SECURITY POLICY VALIDATION

L. Petkova, PhD
University of Library and Information technology (UNIBIT)
lilyanapetkova92@gmail.com

Abstract: Due to the unstoppable growth of security flaws, the developers need to pay attention and be patient in the integration of security defence in the application development! In most of the cases, they are either uninformmed or unqualified of implementing it which cause some huge breaks in the application! There are a lot of documentations/guidelines/tools free for use to help the developers in their work! For the last few years browsers have integrated certain security header controls to support the web application security! In the present research we will present, in our opinion, one of the most important http security response header - the one responsible for the security of the main base of a web application namely the content! Content Security Policy may help in preventing the some of the most vulnerable security attacks (XSS), but in the hand of an unexperienced developer it can breaks the entire application!

Keywords: HTTP HEADERS, SECURITY, CONTENT POLICY, VALIDATION

1. Introduction

The present article presents a mechanism for web applications to mitigate injection attacks and vulnerabilities, such as cross-site scripting (XSS). That type of attacks allows malicious scripts to be send to the end user to access sessions tokens, perform unauthorized activities, sensitive information, or even rewrite the content of the HTML page.[1][13]

Flaws that allow these attacks to succeed are quite widespread and can be occured on application with no data input validation. [1]

To add another level of security, here comes the Content Security Policy Http header. It declares from where the web application will load scripts, content, circumstances which will block any not declared script injected into the application.

Content Security Policy (CSP) is not intended as a first line of defense against content injection vulnerabilities. Instead, CSP is best used as defense-in-depth, to reduce the harm caused by content injection attacks.

2. Directives

CSP has over 20 different directives which can be used to restrict the load of content on the site! OWASP Secure Headers Project provides a full list of options with description for its purpose.

In our earlier research we have presented how to integrate the http security headers into an ASP.NET project!

This specific header, topic of the current article, can be added to the configuration by describing each directive one after another, separated with ‘;’ [13]. For every directive we should add a list of all content/scripts allowed to be loaded on the site! Anything other than the presented in the list will not be loaded!

Table 1: CSP Directives [2][3][12]

<table>
<thead>
<tr>
<th>Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-uri</td>
<td>Define the base uri for relative uri</td>
</tr>
<tr>
<td>default-src</td>
<td>Define loading policy for all resources type in case of a resource type dedicated directive is not defined (fallback)</td>
</tr>
<tr>
<td>script-src</td>
<td>Define which scripts the protected resource can execute</td>
</tr>
<tr>
<td>object-src</td>
<td>Define from where the protected resource can load plugins</td>
</tr>
<tr>
<td>style-src</td>
<td>Define which styles (CSS) the user applies to the protected resource</td>
</tr>
<tr>
<td>img-src</td>
<td>Define from where the protected resource can load images</td>
</tr>
<tr>
<td>media-src</td>
<td>Define from where the protected resource can load video and audio</td>
</tr>
<tr>
<td>frame-src</td>
<td>Define from where the protected resource can embed frames</td>
</tr>
<tr>
<td>child-src</td>
<td>Define from where the protected resource can embed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>CSP version</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-uri</td>
<td>CSP Level 2</td>
<td>Chrome 40+; Firefox 35+; Safari 10+</td>
</tr>
<tr>
<td>default-src</td>
<td>CSP Level 1</td>
<td>Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>script-src</td>
<td>CSP Level 1</td>
<td>Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
</tbody>
</table>

In our personal experience we have been influenced by Scott Helme - a security researcher and security tools developer. The table above provides information for all directives with the description to each one of them and the ones in bold are those which we have used in our workflow.

Further in the research we present idea of having different versions of the content security policy! Basically some versions have added some new directive which are not backwards compatible.

In the following table we present compatibility of some of the directives with the browsers versions and the CSP version it comes from.

Table 2: CSP Directives Values Browser Compatibilities [2][11][12][14]

<table>
<thead>
<tr>
<th>Value</th>
<th>CSP version</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-uri</td>
<td>CSP Level 2</td>
<td>Chrome 40+; Firefox 35+; Safari 10+</td>
</tr>
<tr>
<td>default-src</td>
<td>CSP Level 1</td>
<td>Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>script-src</td>
<td>CSP Level 1</td>
<td>Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
</tbody>
</table>
Table 3: CSP directives values[2][3]

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Wildcard, allows any URL except data: blob: filesystem: schemes</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Prevents loading resources from any source</td>
</tr>
<tr>
<td><code>self</code></td>
<td>Allows loading resources from the same origin, but not subdomains (same scheme, host and port).</td>
</tr>
<tr>
<td>data:</td>
<td>Allows loading resources via the data scheme (e.g. Base64 encoded images).</td>
</tr>
<tr>
<td><code>unsafe-inline</code></td>
<td>Allows the use of inline JavaScript and CSS source elements</td>
</tr>
<tr>
<td><code>unsafe-eval</code></td>
<td>Allows unsafe dynamic code evaluation such as JavaScript eval()</td>
</tr>
<tr>
<td><code>nonce</code></td>
<td>Allows script or style tag to execute if the nonce attribute value matches the header value. (investigated further in the article)</td>
</tr>
<tr>
<td><code>sha256</code></td>
<td>Allow a specific script or style to execute if it matches the hash. (investigated further in the article)</td>
</tr>
<tr>
<td>https:</td>
<td>Allows loading resources only over HTTPS on any domain.</td>
</tr>
<tr>
<td><a href="https://cdn.com">https://cdn.com</a></td>
<td>Allows loading resources only over HTTPS matching the given domain.</td>
</tr>
<tr>
<td>*example.com</td>
<td>Allows loading resources from any subdomain under example.com.</td>
</tr>
<tr>
<td>domain.example.com</td>
<td>Allows loading resources from the specified domain name.</td>
</tr>
</tbody>
</table>

3. Source List

The source list provides requirements for each directive what source can be loaded. Each directive can have multiple source values separated with a space. The one exception thought is the ‘none’ value which should be the only value declared.

3.1. Source List Examples

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>style-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>img-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>media-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>frame-src</td>
<td>Deprecated</td>
</tr>
<tr>
<td>child-src</td>
<td>CSP Level 2: Chrome 40+; Firefox 45+; Edge 15+</td>
</tr>
<tr>
<td>frame-ancestors</td>
<td>CSP Level 2: Chrome 39+; Firefox 33+; Edge 15+</td>
</tr>
<tr>
<td>font-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>connect-src</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>form-action</td>
<td>CSP Level 2: Chrome 40+; Firefox 36+; Edge 15+</td>
</tr>
<tr>
<td>sandbox</td>
<td>CSP Level 1: Chrome 25+; Firefox 50+; Safari 7+; Edge 12+</td>
</tr>
<tr>
<td>script-nonce</td>
<td>CSP Level 2: Chrome 40+; Firefox 35+; Edge 15+</td>
</tr>
<tr>
<td>plugin-types</td>
<td>CSP Level 2: Chrome 40+; Safari 10+; Edge 15+</td>
</tr>
<tr>
<td>report-uri</td>
<td>CSP Level 1: Chrome 25+; Firefox 23+; Safari 7+; Edge 12+</td>
</tr>
</tbody>
</table>

3.2. Hash

The Hash method is more suitable for static content. The browser hashes any inline JavaScript or CSS and executes its if the value matches the one in the HTTP header. [3]

Content-Security-Policy: script-src 'sha256-646840DCAA5....'

3.3. CSP configuration rule

As we have already investigated our past research titled Http Security Headers, there are two ways of configure http header rule in an ASP.NET project: through IIS platform and coding it in the web.config file of the web project!

Here is an example of CSP configuration written in the web.config of the project:

```xml
<remove name="Content-Security-Policy"/>
```

4. CSP Versions

Over the years due to the evolution of vulnerabilities and attacks the CSP has the need to evolve too. Some of the changes are related to the need of new directives, other to the need of more detailed violation reports. This leads to the separation of the CSP in several versions.

Initially CSP is designed to be fully backward compatible. But CSP version 2 has some explicitly-mentioned inconsistencies in backward compatibility. Browsers that don’t support it still work with servers that implement it, and vice-versa: browsers that don’t support CSP simply ignore it, functioning as usual, defaulting to the standard same-origin policy for web content. If the site doesn’t offer the CSP header, browsers likewise use the standard same-origin policy.[11]

4.1. CSP Level 1.0

CSP Level 1.0 was defined November 2012. The initial directives were: default-src; script-src; object-src; style-src; img-src; media-src; frame-src; font-src; connect-src; sandbox; report-uri. [8]

From now on every other version lays on all rules and directives from this one!

4.2. CSP Level 2.0

This version is proposed November 2016. Here are some of the changes applied on version 2.0; [9]

- The following directives are brand new in this revision: base-uri; child-src; form-action; frame-ancestors; plugin-types;
- If the loaded resource is a result of a redirect, the path component of the source is now ignored;
- Individual inline scripts and stylesheets may be whitelisted via nonces and hashes (presented in the article in point 3);
- A SecurityPolicyViolationEvent is fired upon violations;
4.3. CSP Level 3.0

CSP version 3.0 is barely new. It was proposed October 2018 which in our personal experience still makes it inappropriate to be used.

Some of the changes applied on version 3.0 are:[10]
- The frame-src directive, which was deprecated in CSP Level 2, has been deprecated, but continues to defer to child-src if not present (which defers to default-src in turn);
- New directives: worker-src; manifest-src;
- The URL matching algorithm now treats insecure schemes and ports as matching their secure variants. That is, the source expression http://example.com:80 will match both http://example.com:80 and https://example.com:443;
- Reports from inline violations will now report “inline” as the blocked resource; a sample attribute if the relevant directive contains the ‘report-sample’ expression;
- The report-uri directive is deprecated in favor of the new report-to directive;
- The ‘strict-dynamic’ source expression will now allow script which executes on a page to load more script via non-“parser-inserted” script elements;
- The ‘unsafe-hashes’ source expression will now allow targets to match hashes.

5. Browser Compatibility

The following compatibility table is structured according a global usage statistics from March 2019! The global usage of CSP Level 2 almost 10% over the one of CSP Level 1.0. The statistics show that around 88.69% of the browsers support CSP Level 2 and 7% from it support it partially! For CSP Level 1.0 those numbers are higher - 96.47% of the browsers support it and only 3% from it partially used it! The below table gives more details about different versions of CSP and their supports on 7 different browsers: Internet Explorer, Edge, Mozilla Firefox, Chrome, Safari, Opera and Android. [14]

Table 4: CSP versions Browsers Compatibility [2][14]

<table>
<thead>
<tr>
<th></th>
<th>IE</th>
<th>Edge</th>
<th>Firefox</th>
<th>Chrome</th>
<th>Safari</th>
<th>Opera</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Security-Policy Level 2</td>
<td></td>
<td>11</td>
<td>partial</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>partial</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content-Security-Policy Level 1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10+ Limited</td>
<td></td>
<td></td>
<td>Limited</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X-Content-Security-Policy Deprecated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X-Webkit-CSP Deprecated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As we see from the table CSP Level 2 is partially supported from version 18 of Edge browser and version 67 of Mozilla Firefox. And its usage on Internet Explorer is unknown! However CSP Level 1.0 usage on IE is partially supported on version 11! X-Content-Security-Policy and X-Webkit-CSP are deprecated and although some browsers support them, experts advised to avoid their use!

6. CSP validators

There are a lot security validation tools to help the developer in integrating the content security policy (along with the other HTTP security headers) and depending the developer’s resources, those tools can be free and paid.

In our personal experience we have worked with several free tools which provided the necessary results.

The extension we have used to help us in check the CSP integration on a site is called called CSP Evaluator and is used as an extension to the Chrome browser. It gives a live time report of the CSP integration on the loaded site. If the badge is in green color then the CSP with the supported version is integrated successfully on the site! Otherwise it gives a list of directives with its correct and wrong values to be fixed.

Image 1: CSP evaluator report

Another free tool is the one that can be found on the following Internet address: https://securityheaders.io/. It can be also added as an extension to the browser. It gives a full HTTP security headers report!

7. Results

During our research we made several security checks on a few selected web applications. As part of our research we have again used the ALEXA analytical insight to choose 6 website from an excerpt of 50 sites based on a selected Country category - Bulgaria. [7]

The sites selected for this articles were selected on a personal opinion based on the most advertised and the most commonly used website. We are not going to present the name of sites due to law and policies restrictions! [7]

Checking the selected sites with https://securityheaders.io/ we can see that 1 out of 6 websites are using the CSP policy to protect their site from XSS attacks and vulnerabilities.

Table 5: CSP security statistic [7]

<table>
<thead>
<tr>
<th></th>
<th>site A</th>
<th>site B</th>
<th>site C</th>
<th>site D</th>
<th>site E</th>
<th>site F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Security-Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

But if we run the CSP evaluator tool we can see that the CSP protection is not fully integrated which makes it not too secure:

Image 2: CSP for site A

The results show that the web applications we have selected are not secure from XSS attacks. And considering that we have selected some of the most commonly used website in Bulgaria, that makes us think how much the content we provide to those sites is safed and how much we are exposed to malicious actions.
8. Conclusion

The need of content security integration becomes larger with the evolution of technology! It does not fully protect our applications but it gives an extra level of security by restricting the attackers actions.

And from the analytics we have provided we have to consider that the poor CSP is not a giving the necessary level of protection. If it is not properly integrated, its purpose stays unachieved.

References

[1] OWASP, Cross-site scripting
[8] Content Security Policy 1.0, Brandon Sterne, Adam Barth, November 2012, W3C
[9] Content Security Policy 2.0, Mike West, Adam Barth, Dan Veditz, Brandon Sterne, November 2016, W3C
[10] Content Security Policy 3.0, Mike West, October 2018, W3C
[12] Content Security Policy, Mozilla Developers Network, April 2019
[13] 5 Practical Scenarios for XSS Attacks, Satyam Singh, October 2018
[14] https://caniuse.com, April 2019
ДОВЕРИЕ КАК ПСИХОЛОГИЧЕСКИЙ ФАКТОР БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ

Т.А. Zhalagina, E.D. Korotkina
Russia, Tver, FSBEI «Tver State University»

Аннотация: Показано, что в современных условиях доверие приобретает новое значение и рассматривается как необходимое психологическое условие безопасного взаимодействия в обществе. Анализируется проблема доверия руководителя и членов команды в организациях. Доказывается, что доверие руководителя к сотрудникам в ситуациях командного взаимодействия является условием эффективного управления в современных условиях.

КЛЮЧЕВЫЕ СЛОВА: ДОВЕРИЕ, БЕЗОПАСНОЕ ВЗАИМОДЕЙСТВИЕ, ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ, КОМАНДА, ПСИХОЛОГИЧЕСКИЙ БЕЗОПАСНОСТЬ

Abstract: It is shown that in modern conditions trust takes on a new significance and is considered as a necessary psychological condition of safe interaction. The paper is focusing on the role of trust in manager teams members in organizations. It is proved that the trust in team groups is a prerequisite for effective management.

KEYWORDS: TRUST, SECURE COMMUNICATION, EFFECTIVE MANAGEMENT, TEAM, PSYCHOLOGICAL SECURITY.

В современном мире потребность в безопасности становится все более актуальной в связи с нарастающим количеством угроз, возникающих в природной, экономической, политической и информационной среде. В связи с расширением социокультурных, межличностных, институциональных kontaktов, возрастает уровень неопределенности и непредсказуемости, которые способствуют возникновению угроз психологической безопасности [1].

Одним из ключевых методов исследования становится риск как важная характеристика технологического развития, а также субъективное осознание риска, связанное с его восприятием и оценкой. Психологическая безопасность личности опирается на психическую устойчивость и жизнестойкость индивида, а также создание психологически безопасной среды. В этих условиях возрастает значимость доверия как ведущего фактора безопасного взаимодействия на межличностном и институциональном уровне. Особая роль доверия обнаруживается при взаимодействии индивида в организационных структурах, где оно определяет характер коммуникаций и восприятие организационной среды как безопасной. Сотрудники различных организаций смогут эффективно работать, если выстроит доверительные отношения друг с другом, с руководством, подчиненными, клиентами. Доверие здесь выступает важнейшим фактором установления контакта, поддержания взаимоотношений, достижения договоренностей и удовлетворенности персонала. Поиск эффективных инструментов укрепления доверия становится важной исследовательской задачей.

В современной психологии нет единства в определение феномена доверия. Различают понятия «уверенность» (confidence) и доверие (trust). Уверенность описывается как субъективное состояние человека в отношении себя и своего поведения. Доверие связано с состоянием межличностных отношений, оно характеризует отношение одного человека к другому. Результаты исследований показали, что люди с высоким уровнем доверия к другим в большей степени ориентированы на сотрудничество, кооперацию, солидарность, достигают совместных результатов в работе.

Современные исследователи единодушно признают доверие важным для жизни организации психологическим фактором, способствующим ее развитию и повышающим эффективность деятельности [1; 2; 4; 6].

На наш взгляд, изучение проблематики доверия, уровня доверия руководителя и сотрудников в ходе командного взаимодействия является чрезвычайно актуальным направлением в силу смены парадигм управления. По мнению специалистов роль доверия в современном бизнесе становится все более ощутимой [2; 4; 5]. Неформальные горизонтальные связи признаются важнее официальных, а электронные технологии позволяют членам команд работать на больших расстояниях друг от друга и вне прямого контроля. Управляемость организаций все больше зависит от доверия между сотрудниками и руководством, а его границы проходят там, где доверие, постепенно снижающееся по мере удаления от центра компании, полностью заменяется расчетом и санкциями [5; 6].

Стоит меняться представление о внешней среде организации. Задачей становится не само по себе продвижение товара, а формирование маркетинга отношений – расширение базы постоянных клиентов, подрядчиков и партнеров. Управление качеством уже не сводится только к характеристикам товара или процессов в цепочке создания ценности – на первый план выходит качество отношений. Можно ли доверять компании, сотрудники которой не доверяют друг другу? [2; 5]

Идею командного менеджмента предложил Р. М. Белбин [7; 8]. В связи с усилием роли неформальных отношений между сотрудниками ее стали рассматривать как новую организационную основу эффективности деятельности. Именно командное взаимодействие, а не просто групповое, дает синергетический эффект взаимодействия ее членов. Рабочая группа (workgroup) — группа, взаимодействующая исключительно для распространения информации между членами группы и принятия решений, помогающая каждому члену выполнять свою деятельность в рамках сферы его ответственности [10; c. 121]. Рабочая команда (workteam) — группа, результатом усилий членов которой является такой уровень деятельности, который превосходит суммарный вклад ее индивидов [10; c. 121]. Таким образом, в группе люди работают сами по себе, лишь иногда взаимодействуя друг с другом, а в команде идет постоянная совместная работа. Команда рассматривается нами как разновидность малой группы с выраженной целевой направленностью, интенсивным взаимодействием ее членов и высокой продуктивностью и как высокопрофессиональный субъект совместной деятельности. Большинство отечественных и зарубежных исследователей отмечают, что командное взаимодействие базируется на сплоченности, взаимоподдержке, энтузиазме, тесном, открытом, целенаправленном сотрудничестве. Именно поэтому прочность и эффективность таких командных отношений определяются, во-первых, эмоциональными отношениями, а во-вторых, четким видением цели, как руководителем, так и его сотрудниками.

Практики в области психологии управления подчеркивают, что для формирования и поддержания командного взаимодействия в организациях руководителю недостаточно только занимаемой формальной вышестоящей должности. С точки зрения бизнес-процессов эффективное и продуктивное сотрудничество строится не столько на формальном деловом взаимодействии, сколько на
недобросовестных сотрудников, злоупотребления которых не только могут привести к серьезным убыткам, но и портят отношения в группе [5]. Ошибки и упущения в условиях излишнего доверия остаются незамеченными, перспективные возможности – нереализованными. В связи с этим авторы подчеркивают значимость умеренного доверия в ходе совместной деятельности, а также управление амбивалентностью доверия и недоверия в отношениях руководитель – подчиненные. При этом Lewicki R.J., McAllister D.J., Bies R.J. настаивают, что функциональное сосуществование доверия и недоверия является центральным компонентом отношений в высокопродуктивных командах [9]. Вполне очевидным является факт рассмотрения доверия руководителя и сотрудников в качестве условия реализации эффективной профессиональной деятельности в командах. Изучение проблем доверия на групповом уровне, детальный анализ результатов таких исследований могут способствовать глубокой диагностике организационных проблем и выявлению потенциальных направлений совершенствования командного управления. **Литература:**

1. Жалагина Т.А., Короткина Е.Д. Психологическая наука к концу третьего десятилетия XXI века: стратегии развития / Психологический журнал, 2017. № 5. С. 103-108.

**About authors**

Zhalagina A. Tatyana – Professor, Doctor of sciences (Psychology), Dean. Faculty of Psychology, Head of the chair “Psychology of work and clinical psychology”, director of University Liceum. Head of the Dissertation Council in Psychology of work and Pedagogics.

Korotkina D. Elena - candidate of psychological sciences, associate professor, head of the psychology chair FSBEI HE «Tver State University».
SECURITY SYSTEM CREATING IN CONDITIONS OF UNCERTAINTY AND RISK-
OUTLINE OF THE PROBLEM

dr M. Szyłkowska
Faculty of Logistics – Military University of Technology, Warsaw, Poland
monika.szylkowska@wat.edu.pl

Abstract: The article presents selected considerations in the field of the security environment with respect to uncertainty and risk factors along with the approximation of the strategy F.U.D. [fear, uncertainty and doubt].

KEYWORDS: SECURITY SYSTEM, F.U.D. STRATEGY, RISK FACTORS.

1. Introduction

The organization of the security system in its geospatial form until recently contained the areas: land, air and sea and space, but the dynamics of technology development meant that its fifth dimension became permanent broadly understood and defined cyberspace, thus creating a security environment. Digital space, penetrating the remaining areas caused a specific problematic network, which sets the need for a new way of organizing and shaping the security environment. All areas of the environment in the process of shaping the security system have common elements: identification of risks and threats, potential analyses and probability of their occurrence, and the preparation of appropriate forces and measures and restitution plans. Time is an additional common factor for all areas.

The security environment is affected by certain conditions, which includes: chances, challenges, risks and threats of the implementation of interests and the achievement of goals in the field of security. Chances include all circumstances (phenomena and processes), which are conducive to the implementation of interests and the achievement of the intended goals. Challenges include the decision-making dilemmas and choices that a given subject faces, including the necessity of incurring specific costs. Risks are uncertainties connected with a particular action and its consequences – including the potential risk of adverse effects of the action taken. The principle is to increase the level of risk directly proportional to the level of activity (e.g. an increase in terrorist threats due to involvement in international operations). For this reason, the skilful estimation and reduction of particular risks is becoming ever more important. While threats are the direct or indirect destructive influences on the subject. Threats are a classic environmental factor. The strategic objective of each subject is (or should be) to ensure safe conditions for the implementation of interests by: reducing identified risks, eliminating threats (external and internal), proper estimation of challenges and skilful use of the occurring chances by making proper decisions [1].

2. Organization of the security system

The organization of each security system depends primarily on the strengths, means the abilities possessed, but the possibility of its shaping depends on the identified potential, which in turn determines the preparatory and executive activities in this area. The pursuit of tasks defined by each entity – in particular states – in the area of security is their organizing, maintaining and preparing in an comprehensive manner as possible. The indicated activities take place at specific levels and are processed and implemented in them. These areas, in turn, define a specific way of managing the system – creating appropriate organizational and functional links.

In shaping the security system – apart from identifying the indicated factors in specific areas – risk identification and assessment play a key role. Risk understood as uncertainty associated with a specific action and its consequences – including the potential danger of adverse effects of the action undertaken. The principle is to increase the level of risk directly proportional to the level of activity in specific areas. The risk as a combination of the possibility of occurrence of any event and its consequences is determined not only by the need of identification, but also the determination of thresholds of significance of impact on the functioning of the entity with the preparation and undertaking actions aimed at reducing the negative consequences of its materialization.

Examples of risk thresholds are given in Tab.1.

<table>
<thead>
<tr>
<th>Type of risk</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>significant damage to the functioning and possibilities of the entity’s further operation</td>
</tr>
<tr>
<td>serious</td>
<td>serious deterioration or disruption of the entity’s operation continuity</td>
</tr>
<tr>
<td>significant</td>
<td>significant impact on the functioning or partial disruption of operation continuity</td>
</tr>
</tbody>
</table>

Table 1. Types and effects of risk

Threats are another factor in the security environment. The strategic objective of each entity is (should be) to ensure safe conditions for the pursuit of interests by: reducing the identified threats, elimination of threats, proper assessment of challenges, and skilfully using emerging opportunities by making appropriate decisions. The possibility of eliminating threats also precedes the need to identify them and analyse the potential of materialization. In addition to typology of threats, it is important that the estimation of their occurrence is also made in combinations (e.g. external and internal). However, it is crucial to prepare the action in the event of the occurrence and materialization of the effects of the threat. This is involved with, among others, known standards for business continuity (e.g. ISO/IEC 27002 or NIST SP 800-34).

Regardless of the area/sector of operation – for each entity, ensuring the security of information assets of business continuity is of key importance. They have a basic meaning independent of the type of critical processes of a given entity. The business continuity management consist of:

- an analysis of business continuity requirements and risks in the scope of allowable break times in the implementation of critical processes and requirements regarding the availability of assets necessary to carry out these processes. In this area, the risk assessment allows to identify and estimate events that may cause a breach of the continuity of the organization,
- preparation and implementation of the organization’s strategy within the scope of ensuring business continuity (defining the type of actions that will be taken to ensure business continuity and minimizing losses),
- development and implementation of plans allowing to restore the continuity of processes and replacement plans for critical assets,
- development of activities related to ensuring the entity’s readiness to respond to a crisis situation (reviews, tests, plans updates).

Principles related to ensuring business continuity analogy concern the comprehensive development of the security system.

Returning to the aforementioned time factor, it should be emphasized that it is of key importance especially in the case of the materialization of negative events – reactions to an event and restoring the state of full functionality from before the event. In this sense, the division can be assumed:

<table>
<thead>
<tr>
<th>Events</th>
<th>Time of unavailability</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>exceeding the permissible time of unavailability</td>
</tr>
<tr>
<td>serious</td>
<td>within the maximum period of unavailability</td>
</tr>
</tbody>
</table>

Table 2. Events affecting the time of unavailability of the entity. Developed based on NIST SP 800-34.

The time parameter will be determined to a different extent – mainly depending on the type of entity and defined critical processes for its operation.

3. Uncertainty

The starting point for the analysis of the conditions of uncertainty is the theory of U. Beck: Today and in the future we will have to live not so much in a world of previously unknown threats, as in a world that must decide about its future in the conditions of uncertainty created by itself. According to this theory, among others, the society will not be able to control the threats it poses – not because of neglect and failure of modernity, but because of its victories (e.g. increase in industrialization affecting the growth of greenhouse gas emissions) [2]. However, it is worth adding that uncertainty – as a non-measurable phenomenon in principle will also apply to threats that are not yet possible to determine (naming) (e.g. types of digital threats). F.J. Milliken distinguishes three types of uncertainty regarding the environment:

- uncertainty of state (misunderstanding of events and directions of development of the environment),
- uncertainty of the effect (no possibility to predict external influence on the organization), and
- uncertainty of reaction.

Fig. 1. Types of uncertainty

Uncertainty includes changes not only difficult to calculate and events that cannot be estimated, but above all – unpredictability. This fact causes significant complications in the possibility of shaping the security system at the stage of initial identification. In such a defined concept, it seems impossible to include an element of uncertainty in the analyses, however, one may attempt to adopt this category as a set preventing the adoption of preventive action plans, but enabling the undertaking of ex post actions (e.g. technical failures).

4. F.U.D. strategy

The F.U.D. [fear, uncertainty and doubts] is based on disinformation used, among others, in sales, marketing, politics, or broadly understood propaganda. The goal of the strategy is to influence perception by distributing negative ones and questionable or false information about the competition / opponent, etc.

FUD is an intended tactic of rhetoric and error, which was initially used in sales and marketing, especially in advanced technologies to discourage customers to consider competition products [beginning of the 1870s]. The idea was to convince buyers to use the safe equipment of a specific manufacturer, not competition equipment. The hidden coercion was based on reluctance to change, because change means risk, and risk can mean loss. An example can be a description of the system manufacturer: Our software is 100% compatible with the existing software. [implication: some competitive systems are not.] or: Our equipment is 100% compatible with current systems, or: Our systems have already been used by over 1000 companies similar to yours. It has been proven. [implication: competition systems do not have such evidence].[3] After 1991, this term was generalized, referring to all kinds of disinformation used as a competitive weapon, which is currently used in a wide range. Analogically to the previously indicated uncertainty factor, the FUD strategy aims to induce a subjective sense of fear, doubt and uncertainty.

Fig. 2. Elements of FUD strategy

Fig. 3. FUD strategy process

With regard to security, this factor can be of key importance in two ways: an example can be a reinforcement of a sense of threat in society, which results in restricting rights and freedoms [to the privacy contained in the Patriot Act, which formally ceased to apply in 2015 – work is under way over regulations defined in the so-called Freedom Act]. The tightening of safety regulations is not new and finds its justification, however, the risk factors and risks that would underlie the changes are often overinterpreted. In another respect, the implementation of the FUD strategy may cause social
unrest inspired by the services of foreign countries using, for example, social media.

In such context, the decisive aspect is also worth emphasizing. The decision-making process is based, above all, on information resources. The more reliable the information source – the more accurately the decision is made and the operation is more proper. The decision-making situation is influenced by both external conditions (general and task environment) and internal conditions (goals, structure, etc.) under which uncertain factors can cause the risk of making the wrong decision.

6. Results and discussion

Considering the unpredictability of uncertain factors – understood as unknown threats and risks, it can be assumed that the creation of a security system is objectively restricted in this respect. However, as mentioned, this category of uncertain events should be taken into account in management plans and – in particular, in ensuring the continuity of operation – using the analogy of effects as a tool. Then, taking appropriate actions would depend on the assessment of the impact of the given event. Regardless of objective reasons and barriers, identification of risks and threats should be subject to continuous updating as part of a dynamic and flexible adaptation of information resources and knowledge, as well as activities – to dynamically changing conditions of the environment and the security environment. Also in this case, the time factor is crucial – the faster identification, update and modification – the higher the level of the security system. The FUD strategy is today mainly associated with the sales and marketing sector, but its tools can be seen in all areas – especially in the area of information flows in cyberspace. Phenomena such as fake news, or hate news have permanently become part of online social media, becoming a tool of disinformation and propaganda. These are phenomena that require not only analysis, but also the adoption of remedies, because – as results from the research – the impact on shaping public opinion by means of electronic media is definitely stronger than their classic counterparts. In addition, each user can become the creator of any information, anywhere in the digital space. In turn, the recipients of information check credibility and the truthfulness of only those that seem most unreliable or controversial for them. According to the results of the research carried out in 2018 [Digital competences and the proliferation of threats, November 2018], the area of checking the accuracy of information found on the Internet – almost ¼ of respondents confirmed that they check only what is controversial for them, and over 1/5 very rarely analyse the accuracy of information obtained from the network. 4.0% of respondents admitted that they never check whether the information obtained online is true. Taking into account the indicated tools of the FUD strategy and the results of research, it can be concluded that in the process of shaping the security system, not only factors and uncertainty criteria should be taken into account, but also factors related to the potential effects of the FUD strategy together with the possibility of neutralization of its effect in the information sphere.

7. References

ENGINEERING, TECHNOLOGIES, EDUCATION, SECURITY, 2019

УПОТРЕБАТА НА ХИМИЧЕСКИ ВЕЩЕСТВА (ПРЕКУРСОРИ) ПРИ ИЗРАБОТВАНЕТО НА ИМПРОВИЗИРАНІ ВЗРИВНИ УСТРОЙСТВА И ИЗПОЛЗВАНЕТО ИМ ПРИ ТЕРОРИСТИЧНИ АТАКИ СРЕЩУ ОБЕКТИ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА

CHEMICAL MATERIALS (PRECURSORS) APPLIED IN IMPROVISED EXPLOSIVE DEVICES AND THEIR USE IN TERRORIST ATTACKS AGAINST CRITICAL INFRASTRUCTURE FACILITIES

MSC Vasileva, P. – PhD Student
Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski” - Bulgarian Academy of Sciences, Sofia, Bulgaria, vasileva.p@gmail.com

Abstract: In recent years, there has been an increasing trend in the use of improvised explosive devices (IED) worldwide. In this regard, the availability of accessible explosives and their possible use by terrorist groups is considered a significant threat. The likelihood of an IED to be used against critical infrastructure facilities is considered as a threat. The following report examines various aspects of the possibilities to impose control on easily accessible chemicals and preventing the occurrence of harmful consequences of their use as precursors for the making of improvised explosive devices.

Key words: improvised explosive devices, chemical precursors, terrorism, critical infrastructure

Увод
През последните години в световен мащаб се наблюдава тенденция на нарастваща употреба на импровизирани взривни устройства (ИВУ). В тази връзка като значимо заплаха се счита наличие на достъпни експлозиви и евентуалната им употреба за терористически цели. Затруднение представлява вероятността ИВУ да бъдат използвани спрямо обекти от критичната инфраструктура. Историята показва, че когато придобиването на конвенционални експлозиви е затруднено, то лицата, проявяващи интерес, се насочват към общо известни химикали и прекурсори, за направата на експлозиви. Сравнително трудно би могла да се ограничи употребата на химикали, които, при комбиниране, водят до създаване на взривно устройство, в което са използвани обществено достъпни химически прекурсори. Именно достъпността на химикали и прекурсори, за направата на експлозиви и взривно устройство, в което са използвани обществено достъпни химически прекурсори, като пример за небезопасни начини за непосредствено нанасяне на вредоносни последици, настъпили след употребата на ИВУ, надминават тези, нанесени от всякакъв тип експлозив взети заедно.

Например през 2016г. Action on Armed Violence (AOAV), води статистика за 19 246 смъртни случая и наранявания от цял свят, настъпили в резултат на употребата на ИВУ. Според информацията, ¾ или 74% от пострадалите са били цивилни лица. Това се равнява на 45% цивилни жертви на експлозии. Според данните ИВУ са довели до настъпването на тежки последици за населението в 48 държави и територии, което е най-високият брой за локации, поразени от ИВУ за периода на изследването. Общо за 2011 – 2016г. AOAV отчита 124 317 смъртни случая и тежки наранявания от употребата на ИВУ, от които 81% (1000 696) са на цивилни лица.

Следва да бъде отбележано, че данните на организацията Action on Armed Violence се базират основно на непосредственото изследване на ИВУ. Трябва да се вземе предвид, че щетите от подобни неконвенционални оръжия са много по-големи от първоначалните оценени, което влияе на социалното здраве, разрушаване на критичната инфраструктура, тежки психолого-психично страдания за близките на жертвите. Изброеното е само една част от отражението, което дава употребата на ИВУ при терористични актове.

В докладите си ООН отчита [3], че ИВУ нанасят непоправими щети на човечеството – човешки жертви, тежки психолого-психични травми, разрушават обекти от критичната инфраструктура, тежки политически и економически загуби. Изброеното е само една част от отражението, което дава употребата на ИВУ при терористични актове.

През последните години в световен мащаб се наблюдава тенденция на нарастваща употреба на импровизирани взривни устройства (ИВУ). В тази връзка като значимо заплаха се счита наличие на достъпни експлозиви и евентуалната им употреба за терористически цели. Затруднение представлява вероятността ИВУ да бъдат използвани спрямо обекти от критичната инфраструктура. Историята показва, че атаки са били извършвани ежедневно. От записите за 246 смъртни случая и наранявания от цял свят, настъпили в резултат на употребата на ИВУ, надминават тези, нанесени от всякакъв тип експлозив взети заедно.

Например през 2016г. Action on Armed Violence (AOAV), води статистика за 19 246 смъртни случая и наранявания от цял свят, настъпили в резултат на употребата на ИВУ. Според информацията, ¾ или 74% от пострадалите са били цивилни лица. Това се равнява на 45% цивилни жертви на експлозии. Според данните ИВУ са довели до настъпването на тежки последици за населението в 48 държави и територии, което е най-високият брой за локации, поразени от ИВУ за периода на изследването. Общо за 2011 – 2016г. AOAV отчита 124 317 смъртни случая и тежки наранявания от употребата на ИВУ, от които 81% (1000 696) са на цивилни лица.

Следва да бъде отбележано, че данните на организацията Action on Armed Violence се базират основно на непосредственото изследване на ИВУ. Трябва да се вземе предвид, че щетите от подобни неконвенционални оръжия са много по-големи от първоначалните оценени, което влияе на социалното здраве, разрушаване на критичната инфраструктура, тежки психолого-психично страдания за близките на жертвите. Изброеното е само една част от отражението, което дава употребата на ИВУ при терористични актове.

В докладите си ООН отчита [3], че ИВУ нанасят непоправими щети на човечеството – човешки жертви, тежки психолого-психични травми, разрушават обекти от критичната инфраструктура, тежки политически и економически загуби. Изброеното е само една част от отражението, което дава употребата на ИВУ при терористични актове.
Съгласно Закона за забрана на химическото оръжие и за контрол на токсичните химически вещества и техните прекурсори, прекурсор е всеки химически реагент, включително всеки ключов компонент на бинарни или многокомпонентни системи, който взема участие, на който и да е етап от производството и по какъвто и да е метод на производство на токсично химическо вещество. От друга страна Законът за забрана на наркотичните вещества и техните прекурсори дава различно определение на понятието прекурсор, чиято дефиниция е по-мисъл на чл. 2, буква „д”, от Регламент (ЕО) № 273/2004 и чл. 2, буква „д” от Регламент (ЕО) 111/2005 на Европейския парламент.

За целите на настоящото изследване разглеждаме прекурсорите, необходими за изработването на импровизирано взривно устройство, които са общодостъпни за всеки домакинство химически вещества - прекурсори, способни да произведат експлозия при правилно комбиниране. Общо казано това са химикали, които се намират в различен вид и имат широк приложение в ежедневието. Като цяло тяхната покупка, съхранение и употреба е напълно законна.

Прекурсорите са химически съставки или елементи, които могат да се превърнат в експлозивна смес чрез химическа реакция или серия от такива реакции. Голяма част от тези прекурсори се използват в ежедневието ни като акетон, бензил, пропан-бутан, метан, етилен гликол, глекеерин, йод, олово, амониак, живак, сярна киселина, азотна киселина, хлорна киселина, карбамид и др. Експлозивите, създадени от общодостъпни химикали, представляват както риск, така и заплаха за живота и здравето на населението, както и за сигурност и защита [4, 5] на обектите на критичната инфраструктура. Сравнително лесни са за производство и трудно могат да бъдат засечени. В допълнение към това самоличността на лицето, създадо бомбата, често остава неразкрита, поради липса на контрол върху изброените по-горе прекурсори, достигащи в ежедневието ни. Не бива да бъде пренебрегван и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебргнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебрегнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебргнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебргнат и фактът, че в световен мащаб ти е таймерът на пералнята може да бъде използван за целите на терористите да пренебр...
борба с тероризма
цялостната налична информация между всички служби, имащи
всички сектори за постигане на ефективност в предприемането
gолемите индустриални производители на химикали, на трето
бдителност както сред търговците на дребно, така и сред
от друга провеждане на кампания за повишаване на
с такъв тип заплахи, и не на последно място, на персонала на
бдителност както на населението, така и на всички държавни
нелетални
включително
предотвратяване и
на тази мярка.
се прецени коя държавна институция ще следи за прилагането
списък на веществата, които представляват загриженост от
продукти, съдържащи конкретни химически прекурсори. За
проследяване на продажбите, закупуването и/или поръчките на
предприемането на адекватни мерки в световен мащаб.
заплахата. Нейният асиметричен характер налага
заявка, че международната общност осъзнава значимостта на
на Общото събрание на ООН, цитирана по-
проактивни действия. С приемането на Резолюция A/RES/72/36
инфраструктура да бъде насочено към предприемане на
групи спрямо населението и обекти от критична та
противодействие на употребата на ИВУ от терористични
kritichnata infrastruktura.

изводи
В световен мащаб жертвите на експлозии от импровизирани взривни устройства са стотици хиляди. Това налага необходимостта всички държави да работят върху мерки, насочени към противодействие на този вид неконвенционални заплахи. Усилията следва да бъдат насочени както на държавно ниво, така и в световен аспект. Както е посочено в цитираните изследвания ИВУ причиняват най-
много човешки жертви – повече от всички други видове оръжия с експлозии. В тази връзка международната общност не бива да допуска да остане разделяна и неактивна в предотвратяване на употребата на импровизирани взривни устройства среда населението и обектите от критичната инфраструктура. Предприемането на мерки не бива да бъде отложено. Необходимо е тяхното реализиране в рамките на конкретни мерки, които ще включват сразу на страните в рамките на съветската система за противодействие на тероризма. Импровизирани взривни устройства, включително оръжия за автоматично взривяване (например, самоделни взривни устройства, смесена връзка), са най-часто използвани в терористични актове.

списък на използваната литература
The threat posed by drones and improvised explosive devices used against critical infrastructure

MSc Vasileva, P. – PhD Student
Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski” - Bulgarian Academy of Sciences, Sofia, Bulgaria, vasileva.p@gmail.com

Abstract: In recent years, there has been rapid technological development in the capacity and capabilities of the Drones or “Unmanned Aircraft Vehicles”. Given the technological advances, the drones were quickly adopted as devices suitable for the execution of terrorist acts. There is a tendency for drones to be used by terrorist groups as means of delivery for improvised explosive devices (IEDs). This report examines the implications and possible options for respond to such a threat.

Key words: unmanned aircraft vehicles, drone, improvised explosive devices, terrorism, critical infrastructure

Увод
През последните години се забелязва бързо технологично развитие в капацитета и възможностите на дроновете или „безпилотните летателни апарати” (БЛА). Предвид извънредните технологични предимства, дроновете бързо бяха възприети и като устройства, подходящи за осъществяването на терористични актове. Вероятността дрон да бъде използван от злоумерени лица, които целят да нанесат щети или разрушения в особено големи размери, нараства. Малки летателни апарати могат да бъдат използвани както за разузнавателни цели, така и за транспортиране на експлозиви, чрез които да се нанесат щети върху обекти от критичната инфраструктура като например ядрени съоръжения, такива от газовата или електропреносната мрежа, мостове, жичи, телекомуникационни мрежи и други асистенции, чието разрушаване би имало отслабващ ефект върху безопасността и сигурността на обществото.
Следва да се отчете, че се забелязва тенденция през последните 2-3 години във всичко от дрона до дроновете да бъдат използвани от терористични групи като средства за доставката на импровизирани взривни устройства (IVU). Методите, които се прилагат за трансформирането на любителски дронове в неконвенционално оръжие от нов вид, се оказват лесно изпълними и ефективни.
От друга страна, технологите и системите за минимизиране и/или елиминиране на риска от такова атака все още са в процес на разработва и не са така широко разпространени и приложими. Размерът на взривното устройство, което може да бъде поставено в дрон, е сравнително малък в сравнение с повечето ИВУ. Въпреки устройство, което може да бъде поставено в дрон, е разпространени и приложими. Размерът на взривното устройство, което може да бъде поставено в дрон, е сравнително малък в сравнение с повечето ИВУ. Въпреки

Дронове в историята
Употребата на дронове за напасане на терористични удари срещу населениелото звучи като сравнително нова концепция. Както по отношение на много от терористичните похвати, историята показва, че това, което се счита за нововъведение, всъщност не е такова.
Първото въздушно нападение с БЛА е било проведено от австрийската армия на 22 август 1849 г., като хвърля, по предложение на артилерийския офицер и откривател Франц фон Ухатиус, запалителни бомби върху Венеция от 110 балона с горещ въздух. Ухатиус успява да „програмира“ полета на балоните като преди това пуска по-малки такива, с които изчислява скоростта и посоката на вятъра. По време на Втората световна война подобни устройства са били използвани както от британците, така и от японци.
След края на Втората световна война разработването на БЛА е било преимущество за правителствата на определени държави, които разполагат с бюджета и достъпа до високи технологии, необходими за разработването на тези оръжия. Но през последните 4-5 години технологията стана по-достъпна и евтини за обществото като цяло, което от друга страна поставя злонамерени лица в позиция да използват БЛА за целите на тероризма. Размишването на границите между разработваните от държавни правителства БЛА и употребата на такива от недържавни субекти се отчита през последното десетилетие, когато Хищулла започва да използва ирански и руски дронове на дроновете за напасане на терористични похвати в Ирак и Сирия.

Дифениция
Думата дрон е чуждина в българския език и произлиза от английската “drone”, като има няколко различни значението.
сигурност и отбрана. Що се отнася до въздействието до първата половина на 2014г. Интернет терористични групи, в които се вижда употребата на враждебни действия.

обекти от критична инфраструктура и др. за да се повиши това налагало разработването на системи за защита нарушаване периметъра на физическа сигурност и критична инфраструктура и военни съоръжения, за информационна, за уязвяване сигурността на обекти от представяат опасност за защитата на класифицирана мисия срещу правителствени интереси. Могат да бъдат гарантират, че дроновете са полезно средство за провеждане сигурност. Мобилността и ниската степен на засичане креативни начини за достъпване на зони с високо ниво на момента най голямото предизвикателство за тях на бойното поле, тъй като изоставането си по отношение на бързо развиващите се

като демаскиращите признаци на малоразмерните БЛА са ограничени [5]. Голямата реална заплата обаче произтича не от употребата на дроновете на бойното поле, а от възможността терористите да ги използват за транспортирането на ИВУ до планираната цел, която с далеч от военните действия, а с разположена сред място население.

Напредъкът на технологии

Напоследък развитието в технологиите подобрява модерните дронове и възможностите, които осигуряват на терористите. Такава например e технологията за дистанционно управление, използвана като средства за разузнавателни цели при операции, за които има изключително важност. Проектът e претървал съществени промени през последните години.

Модерните дронове използват и част от радиочестотните технологии, които днес са един от най-разпространените и效力ни инструменти, коитo позволяват на операторите да управлят роботите, оборудвани с несмъртноносни оръжия, със същите познания за опериране с хеликоптер с дистанционно опериране.
мащаб. този вид БЛА представляват пред правителства в световен мащаб.

Приложение в тероризма
Приложението на всички описани по-горе нововъведения е от особена значимост за терористичните групи. Задачата да се ограничи или предотврати достигнат до тези технологии на терористи ще се окаже, ако не носимо, точно трудна за решаване. Безпрецедентният бързото развитие на дроновете може лесно да бъдат адаптирани за целите на терориста, за което се изискват минимални инженерни познания.

Предвид високата скорост, развивана от дроновете, те могат да бъдат използвани за бързо преодоляване на стандартните мерки за сигурност, както е установено на примерет за сигурност. Повишена точност при управлението им означава, че, която преди не са били съобразени с уязвими по-външни характеристики, днес са уязвими. Напълно овладяването на дроновете може да използва оръжейни системи като мярка за сигурност. Ето защо, в тази връзка, при заплаха от дрон трябва да бъдат гъвкави и интегрирани както по време на изпълнение на обхвата на системата оставя пилота далеч от зоната за сигурност, в която се навлиза. Това явление нарушава съществената сигурност, която се установява около вече проверена и наложена зона, след което се оценява и налага мерки за сигурност.
Заплахата от дронове може да се характеризира с висока динамичност. Ако дрон, или дронови рои, се приземи в съоръжение в непосредствена близост до уязвима зона, производителността на системата за сигурност и защата ще бъде потисната значително. Тези уязвими точки могат да бъдат използвани като отправна точка за злоупотреба с дрона, като се правят манипулации с имитация, надушеност или наваждане на човешките съвременни системи за сигурност и защата. Някои системи могат да се активират или да бъдат привлечени от дроновете, което може да доведе до заминаване на системата за сигурност и защата, като се правят манипулации със системите за сигурност и защата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата.

Заключение

Обектите на критичната инфраструктура работят като една единица, които взаимодействат на различни равнища и се оказват като една цел за атаки. Населението очаква и разчита на функциониращи институции и служби за своето здраве, безопасност, сигурност и икономически процеси. При това е необходимо да се има предвид, че дронът може да се създаде с различна намерение, като се използват различни технологии и системи за сигурност и защата. Тези технологии могат да бъдат използвани за неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата. Тези манипулации могат да доведат до неприятни последствия, които могат да доведат до създадение на заплаха за гражданите и инфраструктурата.

Използваната литература

A CONCEPTUAL MODEL OF LAW ENFORCEMENT USE OF FORCE

Assist.-Prof. Dr. Eng. Tumbarzka, A.  
Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski” –  
Bulgarian Academy of Sciences, Sofia, Bulgaria, E-mail: y.toumbarski@ims.bas.bg

Abstract: Use-of-force models are utilized in many countries for training law enforcement officers to determine the appropriate level of force which is necessary to gain control over a situation, while respecting law and use of force policies. The present work proposes a generalized model of police use of force, outlining the place of most used non-lethal weapons. The model development is based on data of their effectiveness and safety from police practice and independent research. Since the public perception of the use of force and the non-lethal weapons is often based on insufficient awareness, leading to misinterpretation of police actions, the purpose of the proposed model is to provide an appropriate framework for understanding the process of assessing the situation and taking decision by a police officer to ensure the public safety using adequate means.

Keywords: USE OF FORCE MODEL, FORCE CONTINUUM, NON-LETHAL WEAPONS, LAW ENFORCEMENT

1. Увод

Използването на сила е понятие, за което не съществува общоприета дефиниция. Според Международната асоциация на полицейските началници, силата може да се опише като количеството усилия, необходими за да се постигне подчинение от страна на некооперативен субект. [1] Не съществува и универсален набор от правила, регулиращи кога и колко сила трябва да приложат служителите на полицията, но като цяло се приема, че трябва да се използва само такова ниво на сила, което е необходимо за смекчаване на инцидент, извършване на арест или защита на служител и/или друго лице или група. Голяма част от правоприлагащите органи в САЩ и в други страни имат собствени политики за използване на сила и модели илюстриращи тези политики, наричани също „концептуални на силата”, чиято цел е да се улесни определянето на подходящите нива на реакция в зависимост от ситуацията.

Международното право задължава всяка държава да уважава, защитава и спазва правата на човека, вкл. да гарантира, че органиите на правоприлагането и техните служители уважават и защитават правото на живот [3]. Кодексът за поведение на служителите на реда, приет от ООН през 1979 г., изисква да се посочат всички усилия за извършване на негръбоземно оръжие „освен когато заподозренят нападател оказва въоръжена съпротива или по друг начин застрашава живота на другите, и по-малко екстремни мерки не са достатъчни за неговото възприемане или задържане”. [4] Затова правителствата се насърчават да разработват и осигуряват служителите на реда с оръжия, „които биха позволили диференцирано използване на сила и негръбоземни оръжия”, включително несъмртоносни. [5]

Несъмртоносните (нелеталните) оръжия, наричани в правоприлагането в някои страни „по-малко съмртоносни” (в България – „помощни средства”), заемат изключително важно място в контингуата на сили, запълвайки празнината между „викането” и „штетен”. Това означава, че те се използват когато непредвиждането на активни действия може да доведе до сериозни последствия за полицейските служители или странични лица, а използването на съмртосъдържащи оръжия е неоправдано или несъществено. Като се има предвид, че вербалните команди имат необходимия ефект в малка част от случаите на неправомерно поведение, с което се сблъскват служителите, а до използване на огнестрелни оръжия може да се прибегне само в крайни случаи, значението на нелеталните оръжия като ефективни средства за контролиране на различни ситуации и предотвратяване ескалацията на сили, при това с намален риск за всички участници, е безопасно.

В настоящата работа е предложен концептуален модел за използване на сила в правоприлагането при конфронтации от типа „един срещу един” с цел да се осигури подходяща рамка за тълкуване и разбиране на процеса, чрез който служителят преценява дадена ситуация, взема решение за използване на подходящи средства и след това предприема действия за осигуряване на обществената и собствената си безопасност.

2. Обществените нагласи към използването на сила и към несъмртоносните оръжия

По своята същност правоприлагането на сила представлява полицейско правоовомение, с чието помощ полицията осъществява своите функции. Част от тези правомощия, които са правоприлагането на сила, са определени в Международно право включително в Конвенцията за правата на човека, включително вътрешните права на гражданите. Полицията като цяло се определя като орган на правоприлагане, който има възможността да използва сила против демонстранти, за задържане на демонстрантите при конфронтации, за осигуряване на обществената и собствената си безопасност.

Основната философия на използването на сила от страна на полицията спрямо гражданите е, че сила трябва да се прилага само когато е абсолютно необходимо. Предпочтеният вариант е постигане на доброволно подчиняване. Концепцията за „убеждаване, съвършуване и предупреждаване” обаче може да възникне само когато съдържащата с равният ефект не може да бъде постигната, а от друга страна държавата трябва да гарантира особените средства за осигуряване на обществената и собствената си безопасност.

Обществената виждаемост за използването на сила на полицията може да се определи като обществено понятие, което включва както осъзнатостта за неговата необходимост, така и осъзнатостта за нейното значение и ролята, което е правоприлагането на сила във връзка с обществената сигурност. Полицията като вътрешен орган, действащ в пространството, което е специфично за обществото, включително в областта на управлението на престъпността и предотвратяване и прекратяване на престъпленията.

Всяка организация в обществото има своите особености в социалната структура, в която действа, което води до различия в обществената виждаемост. Обществената виждаемост на полицията в конкретна страна може да бъде различна от обществената виждаемост в друга страна.
политики.

"прекомерна сила"

погрешна обществена нагласа

свързани с нелеталните оръжия, се основава на използване на тези оръжия, отколкото в...

индивидите, които не представляват сериозна опасност за себе си

скоро в тактиките, процедурите, политиките, обучението и

страни са регистрирани примери на опит

предназначени за различни по характер и интензивност

сила"

органи са оборудвани с широк набор от такива оръжия, много случаи и съдебни дела за използване на "прекомерна

по света от 60

нелетални оръжия често предизвиква негативни реакции, а в

предназначени главно за временно деактивиране или спиране

правата на човека, насърчава държавите да осигурят

обратими ефекти. В контекста на правоприлагането те са

обекти и околната среда. В съответствие с това, нелеталните

по проект "Полицейско използване на сила" в САЩ (линейни, но с

разпределението на силата по концепцията за непрекъснатост на съпротивата. Това позволява на служителите да пропускат

пътеки, които не превъзхождат нивата на съпротивата, като нивата на съпротивата на нелеталната оръжия, което ги позволява да възприемат какво количество сила е необходимо. Това може да бъде изпълнено чрез спиране на принципа за използване на минималните необходими нива на сила, при което концепцията за непрекъснатост на сила, описваща кога и колко сила трябва да бъде използвана, може да бъде много полезна.

Моделите за използване на сила са създадени през 80-те години на ХХ-и век, за да подпомогнат обучението на служителите в агенциите по правоприлагане и се използват успешно и досега (военните сили в САЩ и други страни също използват подобни модели под наименованието „скалка на сила“). Независимо, че съществуващите модели са различни като съдържание и дейност, целятата е едини от тях е да даде представа за подходящите нива на сила, които да се използват в дадена ситуация. За да улесни правилните и да предотвратят неправилните отговори, такъв модел трябва да показва: връзката между действията на субекта и правилната употреба на сила на офицерите; или непрекъснатата връзка (континуум) между прилагането на силовите алтернативи. Тези модели се използват както при обучение на служители, така и в разследвания на инциденти в резултат на употребата на сила.

Част от моделите илюстрират политики за ескалиране на силия по континуума при нарастваща съпротивата на заподозрените или десквалифициране на съпротивата. Това позволява на служителите да пропускат стъпки в рамките на континуума, ако е необходимо, напр.

крайността на съпротивата, като в случая нишо на съпротивата е прилагане на сила, която да се използва в дадена ситуация. За да улесни правилните и да предотвратят неправилните отговори, такъв модел трябва да показва: връзката между действията на субекта и правилната употреба на сила на офицерите; или непрекъснатата връзка (континуум) между прилагането на силовите алтернативи. Тези модели се използват както при обучение на служители, така и в разследвания на инциденти в резултат на употребата на сила.

Част от моделите илюстрират политики за ескалиране на силия по континуума при нарастваща съпротивата на заподозрените или десквалифициране на съпротивата. Това позволява на служителите да пропускат стъпки в рамките на континуума, ако е необходимо, напр. когато привидно сътрудничещ заподозрян неочаквано изважда пистолет и заплашва полиция или друг лица. Друг тип модели показват нива на съпротивата на субекта и съответните нива на отговор на служителя. Според [15], политики включващи подобен модел дават ясни насоки за това какво ниво на сила е подходящо при определени обстоятелства, така че то да бъде пропорционално и да не е по-голямо от нивото на съпротивата на заподозрената. Графичното представяне на моделите е доста разнообразно. От оригиналната концепция [16] (1981 г.), представяващая линеен модел, разработението впоследствие модели са еволюирали в модифицирани линейни (подобни на линеарните, но с разклоняваща се структура) и нелинейни (кръгови) модел.
толкова по разлика от конвенционалните оръжия, чиято ефективност е използвана оръжия, тактиките не са разгледани подробно, а данните за наранявания.

това заключение е вторично (след като субектът е бил повален или ограничен по друг начин), от данните не може да се съди за способността на тези оръжия да прекратят дадена ситуация.

Предложеният модел (Фиг.1) е разработен на базата на различни съществуващи модели, като обединява ескалацията на силата и нивата на сила прилагани в отговор на определен спектъра е използването на огнестрелни оръжия, което има голема ефективност на успех, но е свързано с голема вероятност за причиняване на нежелано нараняване. Използването на палките е подходящо на Ниво 5. Тук могат да бъдат поставени и електрошоковите устройства, които чрез проводници доставят импулсен ток с високо напряжение, причинявайки неконтролируеми контракции на мускулите (невро-мускулна недеспособност). Заради високата ефективност и безопасност, доказана от многобройни изследвания, нейната ефективност е вторично (след като субектът е бил повален или ограничен по друг начин), от данните не може да се съди за способността на тези оръжия да прекратят дадена ситуация.

Познаването на ефективността на оръжията и тактиките е от решаващо значение за правилното подреждане на нивата на силата, тъй като в противен случай те могат да се окажат неефективни в дадена ситуация или да причинят ненужни загуби от двете страни в битката. Нещо повече, използването на ОС намалява вероятността за наранявания на субекта със 70 %. По такъв начин, ако събитието се избяга, използването на ОС ще бъде по-ефективно от физическия контрол с голям ръчен и по-малко рисковано за субекта и служителя от използването на палка. Предвид това, най-подходящото място на лютин спрей е на Ниво 4 от модела. На това ниво следва да бъдат поставени и електрошоковите оръжия с директен контакт с тялото на субекта (палки, пистолети, контра). Правозащитни организации, обаче, не подкрепят разпространеното убеждение, че това оръжие носи значителен риск от нараняване – по [8, 15, 19, 20, 21, 22] например, този риск е по-малко в сравнение с ръчния палец или физически контрол „с пръсти ръце”. Мястото на това оръжие е на Ниво 5, непосредствено преди огнестрелните оръжия. Полицийските палки имат сравнително добра ефективност, но и най-висок потенциал за нараняване. При тях употребата на борбен ефект е ограничена, за сметка на сравнително ниска възможност за наранявания. Използването на оръжията е подходящо на Ниво 5, тук могат да бъдат поставени и борбените оръжия за унтерлейтенант. Необходимо е трайно обучение, за като се използват в конфронтации от разглежданите типове. В този смисъл, ефективността на нелеталните оръжия тряба да се разглежда като способността на оръжийците да прекратят сблъсъка още при първото му използване, без да се налага повторно използване или прилагане на по-високо ниво на сила, при това без увреждане на субектите и служителите. Освен това, трябва да се подчертее, че ефективността на нелеталните оръжия е функция на редица променливи, в т. ч. от уменията на конкретния служител за борбено оръжие. В съществуващите модели изолираните видове нелетални оръжия или не са идентифицирани, или всички са поставени на едно и също ниво, или има несъответствие между тяхната ефективност и нивата на сила. За да се определят точните места на най-често използваните видове нелетални оръжия в модела, при разработването му са използвани данни за тяхната ефективност и безопасност от практиката на полицията в САЩ и Канада – [8, 15, 19, 20, 21, 22], както и от предходни изследвания, коментирани в тези разработки. Тъй като при неколкократно прилагане на дадено нелетално оръжие му се повишава, но същевременно може да се повиши рискът от нараняване, туку са взети предвид само данините от първото използване на оръжия. Същото така, понеже обемът на настоящата работа не позволява подробно излагане и интерпретация на данните от проучванията, по-нататък са призвани обобщени данни от литературата, според създаването за смърт или нараняване. Ефективността на нелеталните оръжия е функция от голяма колкото по разлика от конвенционалните оръжия, чиято ефективност е използвана оръжия, тактиките не са разгледани подробно, а данните за наранявания.
Моделът е представен като пирамидална структура и съдържа 6 нива. На Ниво 1 събитет е кооперативен, поведението му отговаря по подходящ начин на присъствието, указанията и контрола на полицаите, затова не се налага използване на сила. Това ниво се счита за най-добрия начин за разрешаване на ясна критична ситуация – самото присъствие на усъвършенстван служител на реда е сериозна предпоставка за предотвратяване на престъпление или смесуване на ситуацията. На Ниво 2 се използват спокойни, незаплашителни команди като пояснение на документ за самоличност и/или показване на относителния размер. Ниво 3 е твърдо нашествие. Субектът може да окаже съпротивление, като не се движи в указаната посока, при което се използват „твърди техники“ – удари, ритане, или нелетални средства от типа на спрей, концентриран ефект или оценка на сила. На Ниво 4 се използват „меки техники“ – удари, ритане, нелетални средства, при което се използват „меки техники“ – удари, ритане, нелетални средства от типа на спрей, концентриран ефект или оценка на сила. На Ниво 5 се използват „меки техники“ – удари, ритане, нелетални средства от типа на спрей, концентриран ефект или оценка на сила. На Ниво 6 се използват „меки техники“ – удари, ритане, нелетални средства от типа на спрей, концентриран ефект или оценка на сила.

Заключение

Навсякъде по света има случаи с неправилно поведение на правоприлагащите органи на правоохранителните органи. Тези случаи са основание за разискване на нивото на сила, необходимо за преодоляване на тези протестствания. За да се определи правилно нивото на сила, необходимо е да се приложат начини за използване на сила, които съответствуват на нивото на сила, необходими за преодоляване на тези протестства. За да се определи правилно нивото на сила, необходимо е да се приложат начини за използване на сила, които съответствуват на нивото на сила, необходими за преодоляване на тези протестства.

5. Заключение

Навсякъде по света има случаи с неправилно поведение на правоприлагащите органи на правоохранителните органи. Тези случаи са основание за разискване на нивото на сила, необходимо за преодоляване на тези протестствания. За да се определи правилно нивото на сила, необходимо е да се приложат начини за използване на сила, които съответствуват на нивото на сила, необходими за преодоляване на тези протестства. За да се определи правилно нивото на сила, необходимо е да се приложат начини за използване на сила, които съответствуват на нивото на сила, необходими за преодоляване на тези протестства.

Предложен е концептуален модел за използване на сила в правоохранителното при търсяне или разпитване на отделни лица, основи се на ефективността на най-често използваните оръжия и тактики. Този модел, адаптиран към политиките и системите за защита на критично инфраструктурна, е подпомаган от проект Quasar, финансиран от Европейския Съюз по Оперативна програма "Интелигентен растеж."
OPPORTUNITIES FOR RADIO-ELECTRONIC COUNTERACTION TO SATELLITE NAVIGATION OF UNMANNED AERIAL VEHICLES WITH A SMALL RADIUS OF ACTION

Prof. Dsc Georgiev, N.L. and Eng. Todorov, O.D.
Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A.Balevski” – BAS,
67, Shipchenski prohod St., 1574 Sofia, Bulgaria, E-mail: nikol611@abv.bg

Abstract: The paper analyzes the satellite navigation systems of unmanned aircraft and some basic approaches to the radio-electronic counteraction against them. The feasibility of their interference by a phase-manipulated random signal has been proven. A method is proposed for creating imitating disturbances by transmitting real signals from satellite navigation systems. Also, the weaknesses of the MAVLink land center communication protocol used by a number of unmanned aircraft are shown. The paper aims at identifying some basic parameters of the radio-electronic countermeasures that will be created and/or explored within the framework of the Quasar project, BG05M2OP001-1.001-0006, financed by the European Union under the Intelligent Growth Operational Program.

Keywords: UNMANNED AERIAL VEHICLE (UAV), SATELLITE NAVIGATION SYSTEM, RADIO-ELECTRONIC COUNTERACTION, IMITATING DISTURBANCE

1. Увод

Увеличаването на способностите на безпилотните летателни апарати (БЛА) е един от най-динамичните процеси в областта на съвременната авиация. Бурното развитие в тази област може да се сравни с бурното и високоскоростно развитие на безжичните комуникации през последните 25 години.

Съвременните безпилотни летателни апарати са оборудвани със сложни радиоелектронни средства (РЕС), позволяващи им да изпълняват с висока ефективност широк кръг задачи – от наблюдение и разузнаване на земната повърхност, до целуказване и нанасяне на огневи удари. Те са важен компонент на все по-нарастващите рискове от нерегламентирани и злонамерени действия в различни сфери на дейности. Особен интерес представят радиоелектронни средства за противодействие срещу този тип заплаха, както и да се преосмислят политиките, стратегиите и тактиките за противовъздействие срещу този тип заплаха, както и да се разработят редица средства за противовъздействие срещу БЛА [1,2,3,4,5]. Настоящият материал е насочен към определяне на възможностите за РЕП на среден радиус на действие на БЛА с малък радиус на действие.

2. Обща класификация на БЛА

През последните години значително нарасна броя и типа на безпилотните летателни апарати (БЛА) и употребата им в различни сфери на дейности. Особен интерес представляват БЛА с малък радиус на действие, произведени и използвани за професионални нужди. Те са малки и широко достъпни, което ги прави обект за използване за нерегламентирани дейности – от трафик на наркотици и снимане на развлекателни събития, през терористични дейности и блокиране на летища до използването им за разузнаване, нелегално или незаконно проникване в военни и граждански обекти. Това наложи редица автори да преосмислят политиките, стратегиите и тактиките за противовъздействие срещу този тип заплаха, както и да се разработят редица средства за противовъздействие срещу БЛА [1,2,3,4,5]. Анализът на възможностите за РЕП на среден радиус на действие на БЛА с малък радиус на действие преминава през няколко основни аспекти.

На базата на стандарти на ИКАО и НАТО (STANAG) е възможна обобщена класификация на БЛА по най-важните, базови признаки, а именно [6,7,8]:
- категория с отчитане на полетното тегло и максималния радиус на действие;
- максимална далечина на полета;
- височина на полета;
- временно предназначение.

Независимо от типа на БЛА, съществуват следните разлики в техния принцип на действие:
- устройство за видео, инфрачервено, лазерно и радиолокационно разузнаване;
- приемник на сигналите на спътникова навигация (GPS/ГЛОНАСС/GALILEO/BEIJGOU);
- командни и навигационни радионавигации;
- радионавигации за предаване на видео, радиометрична и други информация.

През последните години значително нарасна броя и типа на безпилотните летателни апарати (БЛА) и употребата им в различни сфери на дейностите. Особен интерес представляват БЛА с малък радиус на действие, произведени и използвани за професионални нужди. Те са малки и широко достъпни, което ги прави обект за използване за нерегламентирани дейности – от трафик на наркотици и снимане на развлекателни събития, през терористични дейности и блокиране на летища до използването им за разузнаване, нелегално или незаконно проникване в военни и граждански обекти. Това наложи редица автори да преосмислят политиките, стратегиите и тактиките за противовъздействие срещу този тип заплаха, както и да се разработят редица средства за противовъздействие срещу БЛА [1,2,3,4,5]. Анализът на възможностите за РЕП на среден радиус на действие на БЛА с малък радиус на действие преминава през няколко основни аспекти:

На базата на стандарти на ИКАО и НАТО (STANAG) е възможна обобщена класификация на БЛА по най-важните, базови признаки, а именно [6,7,8]:
- категория с отчитане на полетното тегло и максималния радиус на действие;
- максимална далечина на полета;
- височина на полета;
- функционално предназначение.

Независимо от типа на БЛА, съществуват следните разлики в техния принцип на действие:
- устройство за видео, инфрачервено, лазерно и радиолокационно разузнаване;
- приемник на сигналите на спътникова навигация (GPS/ГЛОНАСС/GALILEO/BEIJGOU);
- командни и навигационни радионавигации;
- радионавигации за предаване на видео, радиометрична и други информация.
определен начин и с подходяща мощност, така че да се попречи на нормалната работа на РЕС на БЛА (наричани смущаващи сигнали) насочено активно действие чрез излъчване на радиосигнали. Апарати БЛА в най общия случай може да се определи като още едно нещо, което се подчинява на известни правила за използване.

Въпреки че се определя като РЕС, БЛА в най общия случай може да се определи като няколко от следните резултати: навигационно съобщение, смущаващи сигнали, създаващи хаос, а обикновено са различни типове РЕС.

По този начин можем да определим какво представлява РЕС, благодарение на следните характеристики:

- РЕС на БЛА да получава хаотични и периодични лъчи или вълни със сигнали, които се излъчват и/или предават на разузнавателния потенциал;
- да преустанови получаването на данни от състава на БЛА, което е необходимо за работа със смущаващи сигнали, като начало на неправилна работа на БЛА;
- РЕС на БЛА да преустанови изпълнението на задачи и най често да се причина, като БЛА се идентифицира по някой разузнавателен код, който се различава от другите кодове на БЛА;
- да се нарушат възможностите за работа на навигацията и инфраструктурата на БЛА.

Един от основните показатели за РЕС на БЛА е това, че тези РЕС се преименуват в навигацията. Системите за навигация са предназначени за определение на местоположението на БЛА в пространствената среда. Приемниците се определят като системи за приемане на радиосигнали, предавани от различни източници, като спътници или други радиоисточници.

Системите за навигация са разделени на две основни категории: земни и космически. За тази цел се използват различни носители на информация, като спътници, земни роботи и други източници. Като пример за навигационна система можем да използваме GPS, която е разработена от美国, но се използва в целия свят.

GPS е система за навигация, която използва сигналите на спътници, разположени в космоса, за определение на местоположение на потребителя. Системата се състои от спътници, които излъчват радиовълни, които се接收 в земната сфера и се преобразуват в навигационна информация. Тази информация се предоставя на потребителя във формата на съобщения, които се използват за определяне на местоположение, скорост и други данни.

GPS-сигналът се състои от следните съставни части:
- основен път (P1 и P2), които се използват за определение на местоположение;
- псевдослучайни псевдослучайни кодове (PRN code), които се използват за идентификация на спътника и за определение на местоположение;
- носещи сигнали, които съдържат данни за местоположение, скорост и други данни.

GPS-сигналът се използва за определение на местоположение на потребителите и за определение на местоположение на полета, като се приема като основен показател за навигацията. Този показател е широко прилаган в различни сфери, като логистика, военни операции, туризъм и други.
Изложеното се вижда, че информацията в различните съобщения на сателитните навигационни системи е с фазова модулация, при което:

- C/A кодът е 1023 бита с повторение 1 милисекунда (четоста 1.023 Мгц), т.е. 1 бит е с продължителност от 0.97752*10^-6 секунди.
- Ρ-кодът за военни цели със с цикъл 266.4 дни и е от 2,3547*10^8 бита. Отчитайки, че 266.4 дни са 23016960 секунди, то един бит от този код се излъчва за 0.97746*10^-6 секунди, т.е. 97.746 наносекунди.
- Навигационното съобщение е със 37.500 бита които се излъчват за 12.5 минути (750 сек.), т.е. един бит от този код се излъчва за 0.02 сек., (или 20 милисекунди).

Отчитайки изложеното може да се заключи, че е целесъобразно РЕП на сателитните навигационни системи на БЛА да използва случайни фазови манипулирани сигнали по един от следните три варианта:

Вариант 1 (пренючелтен) - фазовата манипулация се осъществява на всяка носеща четоста на съответния навигационен канал в три различни периоди – през 20 милисекунди (за навигационното съобщение), през 0.97752 микросекунди за L1 и през 97.746 наносекунди за L2 и L5.

Вариант 2 (пренючен) - създаване на фазово манипулирани смущения, като се премахват тези за навигационното съобщение (не се формира смущение с фазова модулация през 20 милисекунди), а се създават само такива със случайни фазови манипулиране за L1 (през 0.97752 микросекунди) и за L2 и L5 (през 97.746 наносекунди).

Вариант 3 (най прост) – създаване на фазово манипулирано смущение предизвикано само за навигационното съобщение. Поради факта, че навигационното съобщение съдържа във всички кодове за навигация (L1, L2 и L5), то най простият вариант за РЕП е чрез формиране само на фазово манипулирано смущение за този канал през 20 милисекунди.

В общия случай блокова схема на система за РЕП на БЛА е показана на Фиг. 1.

Фиг. 1. Блокова схема на система за РЕП

В зависимост от това на кои навигационни канали ще се противодейства, то и параметърите на нискочестотен генератор (НЧГ), манипулатор и модулатора ще зависят от световното целосъстояние на системата. Най-честа ситуация е с лента, която недостига от модулатора и осигурява изходна мощност между 5 и 200 Вт.

Както вече беше посочено, целесъобразно е смущаващият сигнал да е с комбинация от амплитудна модулация и фазова модулация по един от посочените по-горе три варианта.

Случайната фазова манипулация за съответния навигационен канал е целесъобразно да се извърши на ниска четоста и преди амплитудната модулация.

(Най-разпространените типове генератори и модулатори за амплитудна модулация са VCO, DDS и формират на псевдослучайната цифрова гаусова шума.

VCO (Voltage Control Oscillator) генераторът формира тринючелна напрежение. При този генератор ширината на четостотната лента е различна – обикновено 10, 20 или 30 МГц и зависи от амплитудата на входящият в VCO напрежение.

DDS (Дискретен цифров синтезатор) е цифрова симуляция на дискретен VCO. Интерферентният сигнал съответства на аналогоизация VCO. Чрез ударно генериране в широка четостотна лента се постига почти полредно възстановяване сигнала на навигационното средство на БЛА. Приемането на системата е ясно и едночленна четостотена лента за създаване на усъвършенстване и по-добра способност за управление на ключа на системата.

Формираният на псевдослучайната цифрова гаусова шума използува технология на цифров кодирани или чипове (Field Programmable Gate Array) чипове с програмируема логика за високоскоростно решаване на сложни математически операции) чипове, като в определена четостотна лента се създава смущаващ сигнал.

Друга възможност за РЕП на средата за навигационна система на БЛА е чрез формиране на GNSS имитирания сигнали. Имитираният сигнал могат да бъдат използвани за застъпване на сателитните навигационни системи на БЛА, в резултат на което последният може да катастрофира, да се приземи, да се върне на изходната си позиция, или да бъде отключен, следвайки координатите на имитирания сигнал.

GNSS имитирания сигнали могат да бъдат произведени и използвани за целите на РЕП по обаче начини.

Първият начин е чрез приемане и преизлъчване на оригинални GNSS сигнали в реално време (Фиг. 2).

Фиг. 2. Създаване на имитиращи сигнали чрез преизлъчване

В този случай БЛА, при облъчване с имитирал сигнал с по-голяма мощност от тази на спътника и предаващ координати, близки до получените до този момент от БЛА, навигационната система на последния ще започне да приема и обработва по-силни имитирани сигнали. Времето на закъснение на имитиращия сигнал ще е по-голямо от това на истинската пропорционално на разстоянието между БЛА и преизлъчващото средство. Обикновено това закъснение е на порядъка на няколко километъра, което ще доведе до полет на БЛА със значителни грешки в определяне на действителните координати. Ако се приеме, че чувствителността на GNSS приемниците на БЛА е около 160dB [7,8], тогава в зависимост от разстоянието на средата за РЕП ще е необходимо мощност на имитиращия сигнал да е между 25 до 35 dBm, което е относително прост техническа задача. Основен проблем при реализирането на този метод е в необходимостта от преизлъчване на влиятелния сигнал върху приемника на GNSS сигнала. Това може да не бъде постигнато както на отделни захранващи устройства, ако пренебрегото на компонентите на отделните
навигация и имитират реалните сигнали създавани от тях. Ако такъв симулатор на GNSS сигнали се използва за целите на РЕП, то ще е необходимо усилие на изходящия сигнал до необходимото минимално ниво 25–35dBm в зависимост от разстоянието от излъчвател до БЛА. Този начин е най-скъп и най-надежден за формиране на GNSS имитационни сигнали чрез използване на GNSS симулатори. Тези симулатори се използват от конструкторите на системи за спътникови комуникации чрез MAVLink. Според редица автори [9,10] този протокол се очаква да стане стандартен в рамките на проекта Drone Code. Понякога този протокол е част от текущия проект на Drone Code, управлуван от Linux Foundation и се използва от хиляди разработчици. Той се използва и в много системи, базирани на автопилот която ArdupilotMega, px4MU Autopilot и SLUGS Autopilot [9,10].

Комуникационните пакети на протокола MAVLink се двусочни с потвърждение. С него могат да бъдат управлявани БЛА, летящи в мрежа от наземни станции. Разстоянието от излъчвателя до БЛА. Този начин е най-достъпен за реализиране в почти всички области на стопанско приложение е в почти всички области на стопанско и употреба на БЛА с малък радиус на действие. Тяхното на базата на съвременни високотехнологични решения от направата на концепция на заземен модул, намеса, поради което РЕП създава необходимостта от високо квалифициран екип за формиране на протокола. Вторият начин за формиране на GNSS имитационни сигнали като най-лесен за реализиране е този, чрез преизчисляване на усилен приет сигнал.

Посочено е, че подходите и методите за РЕП на имитатора на GNSS сигнали създават възможност за използване на GNSS сигналите като най-лесен за реализиране с този, чрез преизчисляване на усилен приет сигнал.

Вторият начин за формиране на GNSS имитационни сигнали като най-лесен за реализиране е този, чрез преизчисляване на усилен приет сигнал.
SAFETY OF THE ENTITY’S FUNCTIONING IN THE CONTEXT OF THE IMPLEMENTED QUALITY MANAGEMENT SYSTEM IN ACCORDANCE WITH ISO 9001:2015 – A CASE STUDY ANALYSIS

M. Dąbrowska-Świder, Msc.
Logistics Department – Military University of Technology, Poland
malgorzata.dabrowska-swider@wat.edu.pl

Abstract: The aim of the article is to present what benefits for the entity result from the implemented quality management system in accordance with the ISO 9001:2015 standard and whether having such a system is about organizational security and is effective protection against threats related to its functioning.

KEYWORDS: SAFETY OF THE ORGANIZATION, THREATS, ISO 9001:2015 STANDARD, QUALITY MANAGEMENT SYSTEM

1. Introduction

The history of the development of humanity describes many spectacular examples of projects among which those that were carried out with great impetus and had political, scientific, economic and military significance deserve attention. And so, in this good company, next to the invention of a computer, sending the first man into space, constructing a nuclear submarine, or digging a tunnel under the English Channel, the introduction of standards from the ISO 9000 family is mentioned [1].

Initially, these were standards aimed at improving the quality of products (products, services) based on the developed own standards of the organization and the procedures needed to achieve these standards. The reason for this type of activity was the high pressure of the organization’s environment, which demanded the repeatability of processes as a result of which products or services of the highest quality level were to be created. It was the result of using the PDCA (Plan-Do-Check-Act) cycle, which as it turned out quickly could apply to all processes and to the quality management system as a whole. The application of a process approach associated with the PDCA cycle and a risk-based approach is a perfect integration with the requirements of other management system standards. As it is easy to understand the essence of this type of activities was to ensure the safety of any organization that has implemented this type of standard and to improve the competitiveness of its operation on the market. Originally, the introduction of quality standards was to serve the military sector as one of the main pillars of ensuring the safety of the aviation industry. It was about the safety of users of military equipment, that is, soldiers, as well as the increase of the failure-free level in terms of manufactured equipment. It quickly turned out that such standards could be implemented in the automotive sector, also in order to increase the safety of users of motor vehicles. The next important step in the use of quality standards was the implementation of their requirements in order to improve the quality of medical services, and thus to improve the quality of patients’ health care. This was to be done by developing appropriate procedures to facilitate medical staff to apply a high-quality level of treatment. As in every innovative implementation, there were no problems related to overcoming obstacles of human nature, that is, convincing people that the implementation and learning of certain organizational solutions will improve the effectiveness and efficiency of actions, and the measurable effects of such applications will quickly become known in the form of improving the competitiveness of the methods of operation of the medical facility, which took the risk of implementing such solutions in relation to the one that did not date to take such a step. Examples of the possibilities of effective application of the requirements of quality standards in various economic fields allowed to understand the usefulness of such solutions in virtually every area of human life and, consequently, to understand the ease with which they can be assimilated in almost every organization. Thus, the universality of simple system solutions can become the guardian of the safety of any organization. A lot of companies do not even realize that the activities and solutions developed by it and the solutions for the organization of various processes are nothing more than a form of applying systemic solutions with the characteristics of the requirements of quality standards. They just need to be recorded in a skilful manner and distributed among the employees as part of the trainings and monitor the effects of the application in order to make continuous improvements. Despite the voluntary application of quality standards, it should be remembered that the constantly changing environment of the organization and the development of the level of organizational culture evoke the ever-growing need to improve the quality of services and products that are the basis of the international business.

2. Analysis of selected areas of the ISO 9001:2015 standard in the context of ensuing the organization’s safety

The evolution that has taken place in the last two decades, accompanied by the constant development of the organization, has made significant changes in the thinking process in understanding the needs and expectations of stakeholders (section 4.2 EN ISO 9001:2015[2]). It can be proven by the fact that it is becoming easier to convince the top management about the need to implement ISO 9001 at a time when large purchasing companies around the world are beginning to demand the implementation of the standard by their suppliers. An example of this kind of procedure indicates that having the implemented standard constitutes a greater security of the organization in the face of increasing globalization. Today, there is no need to convince the presidents of large corporations or directors of small and medium-sized business entities of the need to make quality efforts due to the existence of such reasons as rising legal requirements, growing market demands and constant development of marketing advantage. An important driving force for the implementation of quality standards is the fact that the customer simply demands it. This kind of approach results directly from point 5.1.2 of this standard [3], which speaks of customer orientation perceived as meeting legal requirements and existing regulations, which should be strictly defined and understood. It is easy to guess that in the case of a disputed case resolved in court, a big advantage of any organization will be that it acts in accordance
with the law and it will undoubtedly increase the possibilities of defense regardless of whether the issue concerns the responsibility for the product or service. In this aspect of the organization’s operation, it is another element that increases its security in the functioning on the market. Another important element on the way to increase the safety of each organization’s functioning is to conduct a thorough risk analysis. A new look at the action regarding risks and opportunities (point 6.1 of this standard)[4] highlights the fact that any observed risks associated with the operation of an economic entity may, in addition to triggering actions to prevent them from occurring, also lead to the observation of a worrying phenomenon. On this basis, an economic entity may, at a later stage of the procedure, implement elements of action to eliminate the source of risk, and if it finds that it cannot be stopped, it may implement such elements of its operation as: searching for new partners, changing the profile of products or services, acquiring new customers or changing the technologies used. Sometimes it may be to make an informed decision recognizing the existence of such a risk and not taking any action in the hope that this risk is a constant element of the functioning of our organization. An important element constituting the framework of action of each organization is the establishment of a quality policy (section 5.2 of this standard)[5], which includes obligations to meet the applicable requirements, and its availability to employees and interested parties demonstrates the transparency of all activities and provides further confirmation as a permanent commitment to continuous improvement of the quality management system. The essence of such an approach, however, is not the fact of creating a heap of bureaucratic documents for the purpose of obtaining a satisfied face of an external auditor, but introducing a well-functioning system that consistently allows solving significant organizational problems. This kind of innovative solution came with the last amendment of the ISO 9001:2015 standard, which entered into force of September 15, 2018. A bow towards treating people as important entities on whom everything in the organization depends is the fact that the dry record of point 7.1.2 of this standard [6] is entitled “People”. In contrast to the standards associated with product certification, where people employed in the organization are referred to as “staff”. As is clear from this type of description, the authors of the standards for the certification of products treat the organization’s employees in an objective manner. Returning to the ISO 9001:2015 standard, it should be noted that behind every type of activity or process being carried out, there is a man with his knowledge, competences, skills, training and a number of other assets that determine his value to the organization. This is an important element proving that the new edition of the ISO 9001:2015 standard has been provided with a new humanistic form. Establishing this kind of approach to an employee may be the fact that point 7.2 of this standard [7] talks about competences, and this is also an example of increasing the sense of security of the organization’s customers because it defines the way in which the organization cares for the development of personnel development through continuous training or concluding contracts with employees being experts in a given field of knowledge, if needed. Point 7.3 [8] is an inseparable element strictly related to maintaining competence referring to “consciousness”. This is, of course, about maintaining a certain kind of specific relationship with employees of the organization resulting from identification with the organization by understanding common goals, knowledge of all procedures, instructions and methods of implementation of processes and benefits resulting from efficient operation and consequences of non-compliant activities that may lead to the occurrence of negative phenomena. A further stage of building customer confidence in the organization comes in point 7.4 [9] regarding the “communication” understood as a competent and professional approach to internal and external contacts. The importance of the area in the field of the organization’s operation is an example of how to approach the customer, there are known cases where the person is responsible for external contacts, instead of acting as a positive business card of his company, through his turbulence contributes largely to the organization’s presentation outside in a very bad light. It is worth thinking about how to bring employees closer to the importance of this area and create positive behaviour patterns regarding a professional way of communicating over the phone and using elegant forms of answers to e-mails. No less important is the method of mutual contacts between employees within the organization itself, here also one should take care of the form of the relationship, which if required by the situation, should be impeccable and polished as part of integration meetings. Very often employees do not realize that the first conversation with a company representative, with the desire to establish a business contact or the first visit to such an organization may determine whether we will become a client of such an organization or we will abandon it for fear of being exposed to bad treatment. We will go somewhere where we will be served at a level that will satisfy us and which we expect. Although within the requirements of the standard we will not find any statement related to the ability to create teams for the proper functioning of the organization, but under the terms of competence, awareness, communication lies precisely this area. An ideal solution would be a situation in which employees of the organization would be focused around leaders and formed teams based on existing informal ties developed during joint problem solving or remedial and improvement activities. It is in crisis situations that some employees have the skills that distinguish them from the environment that allow them to manage teams. If we add to this the re-naming of informal leadership over a group in making such a person a formal leader, i.e. entrusting him with managerial functions, then we can be sure of the success of such a team. The security of the organization’s functioning is also a way of storing and developing the scope of information that should be defined as necessary for the functioning of the quality management system. A lot depends on the type of organization, its size, type of processes, the need for contacts with suppliers, the number of customers and stakeholders, the products and services produced and the competences of the people employed. At this point, the ISO 9001:2015 standard also comes to the aid by defining a framework for the supervision of documented information (section 7.5.3 of this standard)[10]. The requirements of the standard for this very difficult area determine the need for appropriate actions regarding the distribution of documented information, access to it, searching and use, making it available outside, if necessary, storing and decommissioning, maintaining records in the sense of protection against unintentional changes, hence introducing control of each subsequent version of documents. There is also the resolution of the issue related to the determination of confidentiality. The use of a verbal form of what the organization “should” do indicates that it is an obligatory requirement. It applies to all points of the International Standard cited so far. A lot of points are devoted to operational activities, the implementation of which determines the safety of the activities of organizations that have a direct impact on the level of processes being implemented, and thus on the level of manufactured products and services. It is impossible to refer to all significant areas related to planning, supervision, design, production and delivery of services, release of products and services, and
supervision over non-compliant solutions. One thing is certain, namely that each of these points refers directly to protecting the organization from improper conduct, and thus protects both the security of the client and the organization itself. At the end of this short journey in selected areas, it is worth mentioning the requirements of point 8.5.2. [11], which concerns identification and traceability. This type of requirement refers directly to the maintenance of an appropriate level of standards of manufactured products and services. It does not allow for the situation in which anonymity would allow the concealment of an incompatible product. Such solutions safeguard the security and protection of the client’s interests, and on the other hand, give the organization itself the possibility to exclude negative phenomena that may occur during the implementation of processes. In addition, they initiate changes of an innovative, breakthrough and reorganization nature, which are part of continuous improvement.

3. Strengths and threats resulting from the economic entity having the implemented quality management system

The implemented quality management system increases the values of functioning of each company in relations to its competitors. This results from many aspects to which one should include greater credibility of such an organization on the market and a higher level of customer trust to use the services of such an organization. Ensuring the safety of the organization’s activities is additionally raised by the whole range of tools that are included in point 9 of this standard [12]. These activities consist of all kinds of actions related to monitoring, measurement, analysis and evaluation processes. The organization should constantly assess customer satisfaction in the form of feedback on products and services provided in the form of questionnaires, documents confirming meetings with customers, praise or complaints, all kinds of reports on commercial matters closely related to conducting market activities and all market analyses. The organization should also conduct internal audits, scheduled at a specified frequency, and in the case of sensitive areas with the probability of an increased number of irregularities, conduct appropriate corrections and corrective actions, while this type of activities should be confirmed by the reports applied, stored as evidence of implementing the results of audits and the audit program. An important form of implementing activities related to maintaining a proper level of the organization’s functioning is the management review of the top management. The transparency of this type of undertaking is closely related to the assessment of the effectiveness of the organization’s activities. The highlights and shadows shown in the course of a reliable management review confirmed by the relevant report serve to ensure constant compliance of objectives and set directions for action related with meeting requirements and increasing customer satisfaction. The level of higher trust in an organization with a quality management system is additionally confirmed by the obligation to undergo an external audit carried out by independent external auditors who are selected by the audit organization by random selection. But as in any case, there are also significant threats here, resulting not so much from the existing system solutions, but regarding the area related to the integrity of people involved in such activities. It may happen that the internal audit will be carried out in an unreliable manner, firstly because of significant competence deficiencies of the employee selected for this type of undertaking and maybe it is not the greatest threat, the case where there is a pressure on the positive result of the audit by the supervisor of the employee conducting the audit is much worse, an even worse dimension of this phenomenon appears when the result of the audit may be influenced by the top management in order to cover the existing gross irregularities. It is difficult to clearly state the occurrence of this type of cases, the more so that the documented information prepared on the basis does not confirm any violations, and the more difficult it is to capture because the essence of the audit is to collect and evaluate the samples. This means that on the basis of a correct sample obtained during the audit, we acknowledge that the organization has correctly implemented and maintained a quality management system. Sampling, as it can be seen, is one of the areas that poses a threat of wrong assessment of the process under analysis. In the case of external audits, there is also a threat resulting from the actions of an external auditor and this is not a lack of competence, because these are confirmed by the certification body and always the audited entity may request their presentation. A much greater threat may be obtaining positive audit results based on an agreement with an external auditor in exchange for obtaining material benefits or other types of intangible benefits (job offer in the organization for a family member of an auditor). Such situations are very difficult to capture, and the effect of such “positively” passed audit by the organization may be the confirmation of the irregular functioning of the economic entity and irregularities that increase in it, which instead of being removed or corrected cause the piling up and consequently may lead to unpredictable occurrences of negative phenomena. Another threat may be the phenomenon of familiarity, which means that the organization attaches itself to the auditor, and this person, in turn, recognizes that he knows all the nooks and crannies of his routine and as a result of this type of activity he may not notice any malfunctioning of the system.

4. Summary

The presented problems are only a short journey describing what tool is the application of the requirements of the ISO 9001:2015 standard in order to counteract threats occurring within the organization itself as well as in its immediate environment. The very implementation of the standard in the organization significantly improves the safety of its operation, but it should always be borne in mind that the adoption of this type of solution will not guarantee full security to any organization. A lot depends on the system’s maturity and the approach to system solutions demonstrated by employees. Even the best system solutions invented by humans can make a significant contribution to increasing the level of security, but we know perfectly well that unfortunately this is not a sufficient condition. So far, no one has yet invented such a system that allows to guarantee protection against human errors. It is easier to introduce technical security measures informing about failures, irregularities in the functioning of the equipment than to determine when the employee failed. And it is not about making mistakes, it is a human thing to be wrong, but about much more difficult areas related to the employee’s ethics and integrity. Of course, one can develop the most perfect Employee Ethics Codes, but they will remain only dry records if lucrative proposals are made by competitors, which in this way may seek to destroy or hostile takeover of our organization’s potential, often built for decades by the honesty of employees. Therefore, the future must be built on the creation of criteria that everyone should observe, something like the idea of “fair play” in sport. It is about creating a system of motivation that would reward organizations and, of course, employees employed in it, e.g. “honest
businessman” or “irreplaceable employee”. These types of activities are not a kind of utopia or phantasmagoria, but a guarantee of business activities that lead to success. An important role should be played by the “National Certification Units”, which of course are not new, but it is a matter for the creation of such a mechanism that would guarantee their total independence and objectivity. Such an entity would have to help organizations, and not only to deal with judging their way of conducting business in a way far from friendly and partner-like treatment of business entities. Since it has been possible at the European Union level to prohibit the production of plastic disposable accessories and work to improve people’s awareness, it is even more possible to make appropriate changes at the EU level to increase the flexibility and improve the work of Certifying Units operating in the Member States. Someone must be the first and it remains to be hoed that appropriate solutions in this matter will defend themselves and quickly find imitators among other units on other continents. The current and unanticipated danger is the fact that a group of people may emerge who, having received appropriate tools at the EU level guided by their own interests, will encompass their knowledge needed to implement management standards and will lead to the ISO 9001:2015 standard instead of creating economic development will cause its stop [13].

Another equally important issue is the fact that up to now organizations that have implemented quality management systems, in addition to bragging about this on their websites, unfortunately do not share their knowledge and experience by treating each other as potential opponents. Maybe it’s time to change this fossilized mindset in organizations. There are, after all, various industrial sectors that are united by the same goal – customer satisfaction and development. It is not the custom of modern organizations to build an organizational culture based on providing help in the area of advice or guidance. It would be easier to join forces in related organizations and on this basis to make a diagnosis in the area of developing common procedures and solutions. But as can be seen from the presented problems, we still have a long way to go in creating a system that would allow both the national and international level to preserve the identity and traceability of certificates in order to allow an equivalent assessment of certification procedures. The International ISO 9001:2015 standard is a framework diagram of an “ideal organization”, although everyone realizes that the ideal in the modern world is the pursuit of its achievement by developing tools and instruments that are based on many years of experience. The creators of quality standards were guided by the idea of helping to discover the path to the ideal product and service, and recent years show that this is also the way to create the perfect employee, the ideal leader (in this role there is the highest management in the meaning of point 5.1 [14] talking about leadership and commitment) understood as a conscious and committed participant in social life and a satisfied customer aware of own needs. At the end, a question arises regarding ensuring the safety of the organization by implementing a quality management system in the field of supplying full-value products top own clients. Certainly, the standard itself will not do it, but it will show the right way in the pursuit of high quality solutions. On the way to achieving full success, actions are still needed from all interested parties, supported by the development of strong ethical principles. This approach will surely strengthen the clients’ trust in the organization and consolidate its market position.

5. Bibliography

[4], [5], [6], [7], [8], [9], [10], [11], [12] Polish Committee for Standardization: PN-EN ISO 9001:2015
DEFENSE PREPARATIONS AS THE STATE SAFETY CONDITION – SELECTED LEGAL DOCUMENTS

Dr Wojnarowska-Szpucha S.
Military University of Technology, Poland
Email: sylwia.wojnarowska-szpucha@wat.edu.pl

Abstract: Defense preparations are an antidote to emerging political and military threats. They cover, in accordance with applicable legal regulations, the military, economic and administrative area, as well as entrepreneurs and individual citizens of the state. They are mostly based on defensive tasks, that is, special benefits and personal and material benefits in accordance with the law on the general obligation to defend the Republic of Poland.

The article presents selected legal documents regarding this issue in the Republic of Poland.

Keywords SECURITY OF THE STATE, DEFENSE OF THE STATE, DEFENSE PREPARATIONS, DEFENSE TASKS, DEFENSE BENEFITS

Introduction

The current situation in the world, the possibility of various types of threats1 that in the future may lead to conflicts, wars will force states and nations to care for the broadly understood security2. [Security is the foundation of the functioning of every state, its provision is an important factor for the existence and survival of the nation]3, it is one of the most important functions of the state. Therefore, in times of danger, states prepare themselves in the event of their occurrence.

Defense preparations in Poland cover a wide range of planning activities defining tasks, preparing forces and means for their implementation by all elements of the defense system of the state4, which is part of the national security system of the Republic of Poland. As M. Kuliczkowski rightly points out […] defense preparations are an interdisciplinary undertaking covering all areas of state functioning, and the scope of these preparations has significantly expanded into important non-military areas, especially political, economic, ecological, cultural, etc.]5.

The important activities of the organs of executive and public administrative authorities in these preparations are aimed at securing the state against armed attack and creating opportunities for survival for the population in crisis and war situations by providing authorities, administrations and people with a communication system, medical care, food and security. One should therefore be aware that a well-prepared state must engage all possible and necessary forces and means to prepare for the event of a crisis or war.

Selected legal documents regulating the defense preparations of the state

For the purpose of efficient and regulated preparation of defense in Poland there is a number of legal documents regarding these issues. The basic and at the same time starting is the Act of November 21, 1967 on the general obligation to defend the Republic of Poland, where art. 2 specifies that the defense of our country, the preparation of people and state property in the event of war is the task […] of all organs and government administration and other state bodies and institutions, local self-government bodies, entrepreneurs and other organizational units, social organizations as well as every citizen in the scope defined in the Act.6 Another more detailed executive document to the above-mentioned Act is the Regulation of the Council of Ministers of June 15, 2004 on the conditions and mode of planning and financing tasks performed as part of state defense preparations by government administration bodies and local self-government bodies, where conditions and the mode of planning tasks that are performed as part of defense preparations, their financing and the principles of imposing defense tasks7. The division of defense tasks can be made on the basis of stages of their implementation, starting from tasks of a preparatory nature, through tasks to react to the existing situation and ending with reconstruction tasks related to restoring the original state or using the second division defining the purpose of activities,8 or using the second division defining the purpose of activities, where defensive tasks can be divided into preparatory and executive9. In addition, this document specifies in detail what defensive planning is10 that includes the performance, arrangement, updating of operational plans11 and defense programs12.

1 [Threat – a situation in which the probability of creating a dangerous state for the environment arises. Assuming areas in which a threat may arise as the foundation, military and non-military threats can be distinguished.


3 Security is: [a state of non-threat, peace, confidence]—J. Stańczyk, Contemporary understanding of security, ISP PAN, Warszawa 1996, p. 15.


5 [The defense system of the state is a coordinated set of steering elements and executive elements, as well as the functions and processes implemented by them, and the relations between them. SOP is created by all forces and resources intended for the implementation of defense tasks, organized, maintained and prepared appropriately for these tasks]. Defense strategy of the Republic of Poland 2009, Ministry of Defense, Warszawa 2009, chapter 3, point 57.


9 Ibidem, p. 21.

10 Defense planning is: [defining the ways of performing defense tasks by government administration bodies and local self-
A significant part of defensive tasks as part of defense preparations is attributable to entrepreneurs doing business in the territory of the Republic of Poland, including entrepreneurs of special economic and defense importance. The tasks of entrepreneurs for the defense of the state are activities in the scope of:

1. economic mobilization;
2. militarization;
3. operational planning;
4. defense training;
5. resulting from the obligations of the host state. All these undertakings involve entrepreneurs of special economic and defense importance who conduct their activities in an area larger than one province or perform tasks in the field of: transport, including the operation of the state road network, telecommunications services, manufacturing, distribution and transmission of natural gas, liquid fuels and electricity. The Act on organizing tasks for state defense carried out by entrepreneurs in its records also refers to the economic mobilization program, defining the tasks of government administration bodies and entrepreneurs in securing the functioning of the economy. Armed Forces and other entities that will conduct security and defense activities of the state, also providing the population with vital needs. An equally important document is the Regulation of the Council of Ministers of September 21, 2004 on the defense readings of the state in which three states of defense readiness have been defined, the rules for implementing these states and tasks and their implementation related to the change of defense readiness of the state. According to the above-mentioned regulation, the following conditions apply: the state of permanent defense readiness of the state, the state of functioning of the state in time of peace, when there are no serious threats, during this time all planning, training government bodies and the use of necessary forces and resources for this purpose, including operational planning and defense programming – Regulation of the Council of Ministers of June 15, 2004 on conditions and the mode of planning and financing tasks performed within the framework of state defense preparations by government administration bodies and local self-government bodies, Journal of Laws of 2004, no. 152, item 1599, § 2, par. 6.

Operational plans are performed as part of operational planning which includes [...determining activities related to the preparation and operational tasks of government bodies of local self-government bodies in conditions of external threat to state security and during war, included in sets of operational tasks, as well as determination and measures necessary for their performance] – Ibidem, § 2, point 7.

Defense programs are carried out as part of defense programming, which includes [...] defining defense tasks carried out in peacetime, for a ten-year planning period, starting in an odd year, included in material and financial measures, to maintain and develop the defense potential of the state and the preparation of the Armed Forces, government administration bodies and local self-government bodies to operate in conditions of an external threat to state security and during war, as well as designing budget funds allocated for this purpose] – Ibidem, § 2, point 8.

The list of entrepreneurs of special economic and defense significance and government administration bodies to which they are subject is in: Regulation of the Council of Ministers of November 6, 2017 amending the ordinance on the list of entrepreneurs of special economic and defense importance, Journal of Laws of 2017, item 2143.

17. North Atlantic Treaty, Art. 5 [The parties agree that an armed attack on one or more of them in Europe or North America will be considered an assault against them all, and therefore they agree that if such an armed assault occurs, then each of them in part of executing the right to individual or collective self-defense, recognized under article 51 of the United National Charter, will assist the Party or Parties under attack, taking, immediately, independently and in agreement with other Parties, actions it considers necessary, including the use of armed forces, to restore and maintain the security of the North Atlantic area].

18. In Poland, martial law is introduced by the President of the Republic of Poland at the request of the Council of Ministers, cf. the Act of August 29, 2002 on Martial Law and on competences of the Supreme Commander of the Armed Forces and the principles of its subordination to the constitutional organs of the Republic of Poland, Journal of Laws of 2002, no. 156 item 1301.


20. Public administration – is a set of activities, actions and organizational and executive undertakings carried out for the public interest by various entities, bodies and institutions on the basis of law and in legal forms or a system composed of people, organized for a steady and systematic orientation towards the future implementation of the legal code as a public mission consisting mainly (but not exclusively) on the current performance of acts, equipped for this purpose with the state authority and material and technical resources. Source: http://www.sejm.gov.pl/Sejm8.nsf/BASLeksykon.xsp?id=3B2030ED865DCB98C1257A780044A4CE&litera=A (access 25.04.2019).
support special users)\(^{21}\). To meet these requirements, defensive communication systems are created using: [departmental telecommunications networks, telecommunications networks of telecommunication entrepreneurs, dedicated telecommunications networks, postal operators’ infrastructure, military field post, special mail and courier services subordinated to the minister component for internal affairs and courier services subordinated to the minister of foreign affairs]\(^{22}\).

The health service is also obliged to prepare in the event of threats to national security through the implementation of the following tasks: [...] increasing the number of beds in the hospital base and changing its profile, creating substitute hospital places, performing outpatient health services, determining the manner of securing staffing needs and employment rates in medical entities, using the services of public blood banks, determining the method of sanitary and epidemiological protection, determining the method proceedings in the event of a radiation emergency, defining the manner of providing services for the needs of units subordinated to or supervised by the Minister of National Defense and the minister competent for internal affairs and for the needs of the Head of the Internal Security Agency, determining the manner and scope of record keeping and medical reporting in the conditions of mass inflow of the injured, wounded and sick people, defining the manner of providing services for medical entities carrying out defensive tasks]\(^{23}\) as well as their coordination and cooperation in the implementation of these tasks with other bodies. Many of these tasks are coordinated, organized by the voivode\(^{24}\), who is responsible for, at least, determining the location and number of substitute hospital places, approving plans created before the bodies of territorial self-government units regarding the implementation of tasks for defense purposes, possible increase in the number of hospital beds\(^{25}\), drawing up a balance of medical staff in the province and presenting it annually to the minister responsible for health matters, as well as drawing up a plan for the possible transfer of medical personnel in the province.

As part of defense preparations in the Republic of Poland, defense training is organized, in which all entities involved in ensuring state security are involved\(^{26}\). The binding legal act on training is the Regulation of the Council of Ministers of October 8, 2015 on defense training, defining which subjects are obliged to undergo defensive training, what scope of subjects should be included in the training program and the competence of the authorities regarding planning and implementation of training\(^{27}\).

State defense preparations are also readiness to protect facilities of particular importance to state security and defense implemented on the basis of the Regulation of the Council of Ministers of June 24, 2003 on the objects particularly important for security and defense of the state and their special protection, which distinguishes two categories of objects (the first one is subject to the Minister of National Defense and the other to the Minister of Home Affairs), tasks within their protection and competences of the authorities in these matters. [Preparation of special protection of facilities includes conceptual, planning, organizational, logistic, technical, training and control works]\(^{28}\).

In order to increase the defense capabilities of the Republic of Poland, ensure the efficient functioning of the departments of state administration and national economy and organizational units performing extremely important tasks from the point of view of security and defense as part of defense preparations, existing and specially created units will be subject to militarization\(^{29}\). The units will be militarized that carry out tasks within the framework of: [production of goods, services and implementation work and expertise necessary to secure defense needs of the state, military transport and logistic support of the Armed Forces and allied reinforcement forces under the responsibility of the host state, operation of communication systems, transport, power industry, gas industry and the fuel sector, as well as performing functions resulting from supremacy in the Polish airspace, construction, development and reconstruction of the state’s defense infrastructure, as well as the collection and maintenance of mobilization reserves for the technical protection of facilities of special importance for security and state defense]\(^{30}\), that is all entities which, by their actions, strengthen the security of the state and contribute to its defense.

All undertakings, defensive tasks, in order to be able to be quickly and well implemented, require human and material resources. In order to provide these resources in the Republic of Poland, there are legal regulations that give the state the possibility to use the resources of the national economy, to secure them in peace through the imposition of personal and material benefits. The basic document in this regard is the Act of November 21, 1967, mentioned at the beginning of this article, a general obligation to defend the Republic of Poland and an executive document issued by the Council of Ministers of August 11, 2004 on personal and material benefits for defense in the event of an announcement of mobilization and during the war. The personal benefit is the performance of a certain type of activity, work for the defense, whereas the material benefit consists in putting into use the real

defense training. Own study based on: RRM of October 8, 2015 on defense training, Journal of Laws 2015, item 1829, the Act of November 21, 1967 on the general obligation to defend the Republic of Poland.\(^{31}\)

\(^{21}\) See the Regulation of the Council of Ministers of August 3, 2004 on the preparation and use of communication systems for defense purposes of the state, Journal of Laws of 2004 no. 180, item 1855.

\(^{22}\) Ibidem, § 6.

\(^{23}\) Regulation of the Council of Ministers of June 27, 2012 on the coordination and manner of preparation and use of medical entities for the defense needs of the state and the competence of the authorities in these matters, Journal of Laws 2012, item 741, § 1.

\(^{24}\) The voivode is: [...] a representative of the Council of Ministers in the voivodeship, head of the government’s combined administration in the voivodeship, a supervisory body over the activities of territorial self-government units and their associations in terms of legality, a government administration body in the voivodeship, whose properties belong to all matters regarding government administration in the voivodeship not reserved in separate acts to the properties of other bodies of this administration, a representative of the State Treasury, in the scope and on the terms specified in separate acts. [...] The Act of January 23, 2009 on the voivode and government administration in the voivodeship. Journal of Laws of 2009 no. 31, item 206, art. 3.

\(^{25}\) [The planned number of hospital base beds in a voivodeship should be less than 75 hospital beds per 10,000 inhabitants, while 50% of which should be the treatment beds, including beds provided for uniformed services]. The Regulation of the Council of Ministers of June 27, 2012 on the conditions and manner of preparation and use of medical entities for the defense needs of the state and the competence of the authorities in these matters, Journal of Laws 2012, item 741, § 4.

\(^{26}\) The training is attended by representatives of government administration at all levels as well as local government administration and entrepreneurs. However, according to the Act on general obligation, citizens of municipalities participate in self-

\(^{27}\) Ibidem, § 1, 6, 9.

\(^{28}\) Regulation of the Council of Ministers of June 24, 2003 regarding objects of special importance for the security and defense of the state and their special protection, Journal of Laws 2003 no. 116, item 1090, § 5, par. 2.

\(^{29}\) Militarization – transferring the rules and methods of military organization and to bodies and organizational units of the public administration and national economy, applying some elements of military discipline in them and giving them military character by appointing people to serve in militarized units [...]. Ed. J. Pawłowski, Dictionary of terms in the field of national security, AON, Warszawa 2009, p. 66.

\(^{30}\) Regulation of the Council of Ministers of November 24, 2009 on the militarization of organizational units performing tasks related to national defense or security, Journal of Laws 2009 no. 210, item 1612, § 3.
estate or movable property. The regulation specifies how benefits can be collected, who is authorized to impose them, on what basis the reimbursement of expenses for services rendered and issues related to the payment of possible damages are made.

Summary

Due to the volume of the article, only the legal documents selected by the authors regarding the defense preparations of the state were presented. However, one should be aware that the issue of defense preparations is very broad, affects many spheres of the state, institutions, entrepreneurs and citizens, and therefore there are many other legal and strategic documents regulating these issues.

In order to prepare the state in the event of danger and war, use all available forces at your disposal, prepare them properly, plan in peace time, so that the state is ready to counteract various crisis and war threats of varying magnitude and scope.

Bibliography

Kitler. W., (scientific dir.) Local self-government in the national defense of the Republic of Poland, AON, Warszawa 2015


The Act of August 21, 2001 on the organization of tasks for state agility carried out by entrepreneurs, Journal of Laws 2001 no. 122, item 1320

The Act of August 29, 2002 on martial law and on the competences of the Supreme Commander of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws 2002 no. 156 item 1301

Regulation of the Council of Ministers of June 15, 2004 on the conditions and mode of planning and financing tasks performed as part of state defense preparations by government administration bodies and local self-government bodies, Journal of Laws of 2004 no. 152, item 1599

Regulation of the Council of Ministers of November 6, 2017 amending the ordinance on the list of entrepreneurs of special economic and defense importance, Journal of Laws 2017, item 2143

Regulation of the Council of Ministers of April 27, 2004 on the preparation of the national security management system, Journal of Laws of 2004 no. 98, item 978


Regulation of the Council of Ministers of June 27, 2012 on the conditions and manner of preparation and use of medical entities for the defense needs of the state and the competence of the authorities in these matters, Journal of Laws of 2012, item 741

Regulation of the Council of Ministers of October 8, 2015 on defense training, Journal of Laws of 2015, item 1829

THE SECURITY ENVIRONMENT AND THE CHALLENGES TO THE EUROPEAN UNION AND NATO IN THE FIELD OF SECURITY

Colonel PhD. Eng. Ivaylo Angelov
National Military University „Vasil Levski“, Veliko Tarnovo, Republic of Bulgaria
ivailoaa@abv.bg

Abstract: There are three key moments for the development of security and defense globally: First is dynamics of events in the new security environment; second is the importance of so-called “Events leading to change” in the environment and third is the degree of ability of the Parties to anticipate certain situations related to security challenges.

The need for a strategic reconsideration of the security environment and for EU-NATO interaction calls for consideration of the challenges and problems facing the CSDF and the Alliance to improve their joint security work.

Keywords: ECONOMIC, SECURITY, DEFENCE, POLITICAL POINT OF VIEW

1. Introduction

Following the onset of the economic and financial crisis, the focus of both the leaders and the citizens of the EU and the US shifts to addressing its consequences.

As part of a public opinion poll conducted in 2011, the question of who should be the priority of the US president and the European leaders - both sides of the Atlantic identified as a major problem the tackling of the economic crisis. Secondly, the issue of dealing with international terrorism was raised. Thirdly, combating climate change is becoming more and more important for European leaders and the EU’s population.

If these questions are raised today, following the situation in Ukraine and the Middle East, the answers may be different, but it is interesting to note that in 2011 relations with Russia were mentioned as a priority by only 1-2% of the US and the EU citizens.

This outlines three key moments for the development of security and defense globally:
- Dynamics of events in the new security environment;
- The importance of so-called “Events leading to change” in the environment;
- The degree of ability of the Parties to anticipate certain situations related to security challenges.

The need for a strategic reconsideration of the security environment and for EU-NATO interaction calls for consideration of the challenges and problems facing the CSDF and the Alliance to improve their joint security work.

2. The challenges from an economic and financial point of view

2.1. The effect of the reduction of national budgets allocated to defense

As a result of the financial crisis, defense expenditure in most Western European countries is decreasing with the start of the excessive deficit procedure. In the Central and Eastern European countries, however, the reduction in military spending is faster and in larger volumes as they are economically weaker and harder to maintain high levels of budget deficit.

The high degree of interdependence between Member States, due to integration policy, economic and social cohesion, implies that appropriate decisions are made for closer contact, exchange of information and agreement on strategic priorities across sectors.

In the long run, even if the economic crisis is overcome, the challenge of defense budgets will continue to be on the agenda as military equipment is becoming more expensive and prices are rising faster than inflation and gross (GDP) of the Parties.

Intelligent Defense Initiatives and Merging and Sharing are the possible working solutions of NATO and the EU, as the two organizations are finding it increasingly difficult to acquire new ones and retain their current capabilities. On the other hand, the finance ministers and the national parliaments of the Member States having the final say in voting on their budgets are less and less inclined to return their defense levels to their previous levels and at best keep them at present.

An additional argument for the need for pooling and sharing, making smart decisions within both organizations - NATO and the EU - is the proportion of defense spending between NATO and EU allies showing a strong imbalance between US funding and European Union - especially in the period of the economic crisis. The frequent appeals, mainly stemming from the United States, that 2% of GDP being earmarked by Alliance member countries, are often ignored. This leads the Americans to ask whether their allies have the will and the potential to mobilize the resources needed for their common security. From the US point of view, Europe is demilitarized and has the impression that it is divided and focused on itself. Insufficient EU defense budgets obstruct overall security objectives.

In recent years, European defense budgets have been decreasing, releasing resources for other economic sectors. At the same time, the parties can not afford, through financial restrictions and deprivations, a security deficit. An interesting trend in this direction is also observed in the study of the so-Transatlantic trends, namely that when asked by Europeans whether their governments need to increase, maintain current levels, or reduce defense spending in general, the majority of respondents choose the option of maintaining or reducing overall [2].

It is therefore necessary to spend money in a new way, focusing on multinational cooperation and decision-making through prioritization and specialization.

2.2 The future of the European defense industry development

The development of a single European defense production market (EOPP) is gaining momentum in recent years due to Europe’s lagging behind in the defense technology industry. This trend is mainly the result of the strongly reduced investment costs of EU member states and the excessive share of duplication of effort and investment. The existence of many independent national military-industrial complexes and defense markets forms a fragmented, economically inefficient and uncompetitive European Defense Technological and Industrial Base (EOTB).

The EU merger and sharing initiative depends on two factors:
- effective liberalization of the European defense market leads to more competition between companies in the sector, which requires overcoming national controversy over a common defense budget;
- the need for significant improvements in European defense cooperation with the aim of diversifying technical military equipment.

The lack of a single European arms market as well as the existing restrictions direct the focus entirely to the defense national interests of member states and their industries, which often leads to duplication and low level of compatibility in pan-European operations and missions.

It is clear that there is a lack of strategic evaluation in the EU on a European Defense Technological and Industrial Base, in view of the high level of cohesion, the differences in the national
strategic culture and the lack of coordination among the Member States, especially in the acquisition of new technologies.

In this way, EU hard-hitting businesses can compete with those of the United States and the world market respectively, as national governments have a strong influence on company strategies and not always national interest is in the context of pan-European and/or transatlantic. At the same time, they are coordinated only for certain cases, in the absence of a strict and clear mechanism [3].

The dynamics of the real EU policy show that the new requirements for the Armed Forces of the EU Member States are related to the acquisition of capabilities across the spectrum of missions and tasks. The increased requirements of international and multinational operations, network operations and cyber security, space-based systems, intelligence and early warning systems and strategic air transport require the development and deployment of new technologies.

For the EU to be a global player in the defense industry, it is necessary to define the strategic priorities for individual Member States, which are the key competences for each of them, but in the context of the whole, of the European defense system and oriented towards efficiency and effectiveness.

The conclusions reached by many stakeholders are that the patronage of national industry leads to loss and inefficiency. In this respect, a more open market would help European defense industries to be more efficient and cooperate to a much higher degree. Intelligent defense in this regard could be of further benefit in the implementation of joint projects.

2.3. European financing of operations

The regulatory framework for financing civilian ESDP operations is contained in the Commission's Communication to the Council and Parliament on the financing of civilian crisis management operations[4]. It differentiates between: missions (delivery of humanitarian aid, consolidation of democracy, etc.), which are financed by the Community budget, in view of which the EP has strengthened control powers. But missions related to disarmament, support to local police authorities, etc., where part of the funding is possible to absorb from the budget of individual member states, are under scrutiny by MEPs.

The joint action adopted by the Council sets out the way in which the costs between the Community and the budget of the Member States should be allocated. It is possible that expenditure will be borne by Member States when the EU joint operation is specific in view of its location and objectives. In these cases, there is some difficulty, as there is no Community mechanism to manage and direct national funding.

With regard to military operations, the funding of "Community expenditure" through the ATHENA mechanism should be distinguished from that of individual Member States. The ATHENA mechanism, set up by the Council in 2007, is a joint fund at European level to finance military operations under the Security and Defense Policy. Generally speaking, not only those for the preparatory phase, such as exploration and acquaintance missions (transport, accommodation) but also costs in the active period of action, should be understood. These costs are secured by advance payments by the Member States through the ATHENA mechanism in the form of installments determined on a percentage basis according to their Gross Domestic Product.

In the European budget 2014-2020, the so-called The Union’s Multiannual Financial Framework (MFF) provides the opportunity for EU research and technology related to dual use of industrial products which provides a good perspective and enables a more coherent and coordinated approach among Member States, and to achieve real interaction in the field of defense research.

The development of this opportunity in turn would help build the necessary capabilities to protect peace, prevent conflicts and strengthen international security as well as crisis management activities, strengthen the defense technological and industrial base and improve efficiency of military expenditure. This would increase efficiency in the use of research and development, facilitating the pooling and sharing of capabilities, functional specialization, building joint capabilities, multinational joint management of forces and resources, etc. In this respect, in the new EU Research and Innovation Program (2014-2020) Horizon 2020, a recommendation has been made for more research and investment in dual-use technologies. A similar call was made in a number of European Parliament documents.

Taking into account that technology and science are at the root of defense, investment in research and development currently being earmarked by Member States is extremely limited[5].

At a time when the challenges are global, nearly 80% of European research and development is carried out through national programs. However, if a larger share is spent on multinational projects, then the effect would be greater and smaller resource-intensive countries would contribute to the overall effort by taking advantage of an information infrastructure that they would not be able to build on themselves. This requires a strategic vision and a rethinking of the European Security Strategy, taking into account the above.

Currently, the European Defense Agency has defined the following areas where efforts should be made to build capacities of member states:

- Ground surveillance;
- Cyber security;
- Development of unmanned aerial systems;
- Health (telemedicine and robotics);
- Energy;
- Crisis management.

A major challenge is also the difference between the "old" and the "new" EU member states in terms of their abilities and resources devoted to defense. The armaments and operational procedures of the latter in a transitional period between standards, in line with their former commitments under the Warsaw Treaty and the new standards of modernization and investment of large resources. The set NATO criteria for 2% of GDP to be earmarked for defense are incomparable in real terms with the same percentage in the old member states. This leads to a lack of sufficient resources for the purchase of new equipment whose prices are formed on the free market, despite the strong need for modernization.

Challenges from an economic and financial point of view demonstrate the need for better coordination between actors, specialization and standardization, optimization of resources and costs, i.e. not spending more, but spending wiser. This implies synergy between NATO intelligent defense initiatives and EU unifying and sharing, reducing defense expenditure by increasing multilateral forms of cooperation.

3. The challenges from a political point of view

3.1. Obstacles to the EU-NATO in the context of Cyprus-Turkey relations

Turkey is one of the countries that participated in EU missions, counting a significant contribution to the largest Althea military operation in Bosnia and Herzegovina at the time.

However, cooperation in the area of CSDP has important problematic and unresolved issues. The occupation of Northern Cyprus, the state of relations with the state of Israel, and the Kurdish issue are still on the agenda of EU-Turkey relations.

Another major problem is that Turkey is not allowed into the European Defense Agency's planning and decision-making process, as there is no agreement signed with Norway, also a member of NATO. There is a tendency to isolate Turkey from participating in the EU decision-making process on planning and conducting EU operations under the CSDP without regard to its status as a candidate country and a major player in European operations.

Turkey, in turn, does not officially recognize the Republic of Cyprus and does not maintain diplomatic relations with it. For its part, Cyprus does not participate in the Partnership for Peace (PfP) program and therefore there is no signed agreement with NATO on the exchange of classified information.
Under the rules set out in the 2002 Copenhagen EU Council Declaration, only NATO member states or PIP members can participate in the discussions on security and defense issues falling within this framework, and which have signed agreements for the exchange of classified information with the Alliance.

This gives Turkey a formal reason to block Cyprus' access to NATO classified information, which significantly impedes the exchange of information and the development of operational cooperation between NATO and the EU. On the other hand, the EU believes that Turkey needs to take more visible steps to normalize political-military relations in line with established practice in all democratic countries.

Potential proposals to improve cooperation have strengthened and a meaningful dialogue between the EU and Turkey; further enhancing cooperation on capabilities; signing a security agreement with Ankara and Turkey's participation in the work of the European Defense Agency; full and full participation of Cyprus in the strategic dialogue between the two organizations.

3.2. Trust in politicians and public opinion

Due to the danger of electoral exodus in public criticism for increased defense spending and/or loss of autonomy and sovereignty in the defense field, many politicians, especially European, tend to reduce security and defense. They also prefer to be more cautious in supporting and participating in more internal integration initiatives. For this reason, defense expenditure is very often limited, but no long-term analysis is needed on the need for specific reductions. At the same time, maintaining public support for national, regional and global security engagements is of fundamental importance.

Looking at the information environment today, it is clear that it is different. In the era of high technology and the Internet, it is almost impossible to distort information and spread propaganda that is characteristic of a previous historical period. Of course, this is also related to the education of critical thinking in the citizens, so that they can sift the facts of the "distorted truth" in the vast amount of information.

But at the same time, the power of social media and the importance of the virtual world are also being used by radical, terrorist groups influencing people's fears, beliefs, souls and minds. The speed of transmission of information and subsequent reactions is of great importance. This, in turn, is both a challenge and an opportunity for collective defense and security organizations to take a different approach to implementing their policy, notably through public diplomacy and numerous information campaigns for the public.

In modern democracies, where media and public opinion are key components to policy making, transparency in meeting EU commitments across borders is very significant in generating support among their citizens. It is very important for governments, national parliaments and European institutions to be able to explain the importance of contributing to "home security" through the participation of missions outside the EU. In this connection, increasing efficiency gains the so-called an integrated approach to crisis planning and management, where interaction between civilian and military forces is observed. Civilian-military missions are more easily grounded in the public space and find greater political support. In financial terms, they allow funding from the European Commission, including the acquisition of assets, technical assets and services necessary for the operation, while military operations are provided by Member States through ATHENA.

In operational terms, in order to compensate for some of the more specific weaknesses of the existing mechanisms in the EU, a permanent civilian-military structure should be developed to bring together both the preliminary preparation of potential crises and the fulfillment of the tasks planning and managing operations at a strategic level.

In the context of NATO-EU interaction, it is necessary to develop criteria to help deciding which organization has a leading role in what kind of crises, in order to protect the security and defense of citizens. This clarity would contribute to generating public support for the missions and operations of the two Unions.

In this respect, more public diplomacy, transparency, and community information campaigns are needed to accrue more support for security and defense expenditure and the necessary reforms to be made to ensure the security of European citizens. Forming a European identity on European defense and security issues is an additional element to be built through such instruments.

3.3. Different perceptions of threat and security

The present-day security risks and threats are a complex tangle of variable hazards. International terrorism, proliferation of weapons of mass destruction (WMD), fragile states, stubborn unsolvable conflicts, organized crime, cyber-space and energy supply threats, natural disasters and man-made accidents, pandemics pose security risks.

The definition of a unified approach and action of the EU on the global stage is also related to the question of what Europeans perceive for the world [6]. This in turn is related to the formation of a European identity in the area of security and defense.

In this regard, it should be noted that there are two interesting differences, on the one hand, in the perceptions and attitudes of the member states themselves, part of the EU and NATO, and on the other hand between those of the United States and the European countries. The great powers naturally look different to the world, unlike the small ones. They identify risks and threats differently, define security in different ways, and build different levels of tolerance towards insecurity. Those with greater military power perceive power as a useful tool in international relations while the weaker ones perceive it in a slightly different way.

In fact, the strong ones trust strength more than necessary. On the other hand, states deprived of military power face the reverse danger. The viewpoints and the psychological attitudes of power and weakness explain a lot, though not everything, of what today separates the United States and Europe to some extent and provoke their different approaches to threats. Confirmation of what has been said can be traced back to exploring the views of EU and US citizens and leaders, pointing out the unequivocal differences between the views of those on both sides of the Atlantic.

To the question to what extent do you agree with the following: Under certain conditions, war is necessary to triumph justice? 46% of US respondents have responded "fully," while only 9% of EU citizens have said "totally agree" [7].

The existing differences between Europe and the United States are not value-based, more or less they lie in politics.

After the damage caused by two world wars in the 20th century, Europeans have an instinctive desire to avoid military conflict as a way of solving problems. Europe is guided by the "logic of peace" in contrast to the US "logic of war".

A further example that policy analysis is at the heart of different approaches is the European understanding of the UN as the sole source of legitimacy for an armed conflict or the international recognition of a government. This is not covered by the American view of US freedom in the use of military force. The principle of "preventive strike" laid down in the American doctrine is met with recognition of a government. This is not covered by the American
should be countered as a criminal activity - to treat terrorists as criminal criminals and to fight them by respecting the laws and human rights. The main institutions in this case are judicial and law enforcement, but especially the police and special services. While the role of the army, the military is only complementary and auxiliary.

A similar trend is also observed in the European Commission’s proposal for a European Security Program, which proposes to strengthen the role of Europol through the establishment of a European Counter-Terrorism Center for the exchange of information between national law enforcement authorities, based on the successful experience of the European Cybercrime Center. Particular attention is paid to the fact that in the context of the crises and conflicts in Syria, Iraq and Libya, terrorist groups are joined by European citizens who, on their return home, can pose a significant danger [8].

The very focus on “threats” distinguishes Americans from their European counterparts. Americans, writes Stephen Everetz, talk of external “threats” such as “spreading weapons of mass destruction, terrorism and bandits” called by Bush “Axis of Evil”. While Europeans are focusing on “ethnic conflicts, migration, organized crime, poverty and the destruction of the natural environment”, challenges to which they have the potential to respond [9].

According to a number of politicians, the EU is perceived primarily as a “civilian” force, with mainly economic and diplomatic means, which can “win without an army”. EU concentration on “soft aspects of security” can have comparative advantages. These include the beneficial impact of the enlargement of the Union, the considerable funds earmarked for development aid, peacekeeping and funding of programs for international institutions, in particular all possible non-military means of preserving stability and security.

Despite the above mentioned differences in perceptions and approaches, today more than ever requires close transatlantic co-operation to be made by American and European decision-makers. The EU should create its own concepts within the transatlantic alliance and develop its own institutional process and capabilities so as to further contribute to the development of the Alliance as an equal partner.

4. Conclusion

The progressive strengthening of integration processes in the field of European security and defense is inevitably linked to the assumption of new responsibilities and to the contribution to solving individual regional problems or crises. The successful EU entry into this framework is linked to strengthening the democratic control of the sector.

The challenges are related to two main points. On the one hand, with the low tendency of national parliaments, even after stabilization from the economic and financial crisis, to vote for higher defense budgets. That is mainly due to the prioritization of social and economic costs.

On the other hand, the gradually enhancing integration process in the defense sector could lead to a limitation of the role of the national state at a later stage and, respectively, to weakening the control powers of national parliaments.

As a problem with the defense policy of the European countries, the conservative approach and the delayed reform process that the new realities impose are noted. The somewhat strong influence of the military-industrial complexes in individual countries is also an obstacle to the reforms within them and to the so called intelligent defense. Moreover, the desire to sell production leads to exports to third developing countries, which in turn favors the emergence and maintenance of conflict points[10].

The increasing connectivity in the world leads to the fact that the boundaries between internal and external security are blurring. Climate change and resource shortages combined with demographic growth and weak statehood can also lead to conflict and instability around the world.

At the same time, transatlantic relations are changing. The task of improving European security is at the forefront of the European level. Together with the United States and with other countries, Europe is responsible for peace and security in the world. The EU must continue to work together with its partners, but we should be able to act independently if necessary.

Achieving Europe’s strategic independence requires that more resources be spent on defense and that the funds be used better and with the joint efforts of the Member States. In this regard, it can be said that the United States is already investing more than twice as much defense for all EU Member States combined and increasing its budget by almost 10% in 2018. China has increased its budget by 150% in the last decade , and in 2017 the increase is 7% while at the same time Russia invests 5.4% of its GDP for defense in 2017 [11].

EU leaders must make a commitment to strengthening the European security and defense that European citizens expect. Public opinion polls clearly show that security has become the greatest concern for most European citizens, although the causes of insecurity vary from one Member State to another.

Europeans also agree that collective action between European countries is absolutely necessary for their security. When goods, services, money and people move freely, security can not be considered alone or fully guaranteed by the Member States’ autonomous actions. The message of Europeans is extremely clear: security and defense should be an integral part of the EU’s core.

In a world that is interconnected, controversial and complex, EU Member States are simply too small to act on their own. Continental-size forces are much better suited than small- or medium-sized states.

This is even more important, provided that the pressure on national budgets remains high. The tension between fiscal constraints and competing public policy priorities continues to characterize the political economy of many Member States. At the same time, competition among global industrial forces is growing, which requires more efficient use of resources. If Europe wants to be competitive on a global scale, it will have to unite and integrate its best industrial and technological capabilities.

Technological changes dramatically alter the nature and picture of security and defense. Large information masses, unmanned vehicles and artificial intelligence bring revolutionary changes to the defense sector. They also increase the technological performance of the civilian defense sector. However, the availability of such relatively affordable technologies also allows the rapid growth of unconventional, transnational and asymmetric threats such as hybrid, terrorist, cyber, chemical, biological and radiological attacks. The sharp increase in Internet users has made cybercrime and Internet use for terrorism a new border of the 21st century war.

Looking ahead, an effective European security and defense policy must be based on the efficient coordination of significant R & D investment. This will help keep up with the new trends and create the technological and industrial capabilities that Europe needs in order to guarantee its strategic independence in security and defense.

References

1 Transatlantic trends: Leaders 2011 Partners GMF and Compagnia di San Paolo, Topline Data 2011: Q 23
2 "TNS Opinion" between 25 May and 17 June 2011 in the US, Turkey and 12 European countries: Bulgaria, France, Germany, Italy, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain, Sweden and the United Kingdom
3 Faleg, G. and A. Giovannini. The EU between Pooling & Sharing and Smart Defence, Making a virtue of necessity?. CEPS’s special report. May, 2012
7 Transatlantic trends: Leaders 2011 Partners GMF and Compagnia di San Paolo, Topline Data 2011; Q 60
8 European Security Strategy: Questions and Answers, Strasbourg, 28 April 2015
ANALYSIS OF DATA TRANSMISSION METHODS USING VISIBLE LIGHT FOR INFORMATION SECURITY

Shvyrev B.A. PhD. (Phys.-Math.), 1 PhD student Timonov D.A. 1  
Kuban State University of Technology, Krasnodar, the Russian Federation 1  
bor2275@yandex.ru, dmitrii-timonov@bk.ru

Abstract: We consider modern methods of transmitting messages by means of modulating the intensity of the flux of visible light from LEDs. The structure of data transmission and existing standards are analyzed. The possibility of using technology to organize a channel of information leakage has been determined. Discusses methods for countering information leakage by modulating the intensity of the light output of LEDs.

Keywords: LI-FI, VLC, MODULATION OF VISIBLE LIGHT, LED, INFORMATION LEAKAGE CHANNEL.

1. Introduction

Room lighting can be used to organize data transmission. This method of transmitting information can be used to form information leakage channels by means of modulating the visible light produced by the LEDs. This leakage channel allows you to transfer information from physically isolated from the communication lines of computing systems.

The transmission of information on the means of modulation of visible light has been known since 2011, when Professor Haar introduced the concept of Li-Fi [1,2]. This type of data transfer uses the transmission of information on the means of controlling the LEDs of lighting devices (chandeliers, lamps, etc., Figure 1).

![Fig. 1. The organization of communication systems using visible light](image)

The data transmission network based on this modulation of visible light is called Visible Light Communication (VLC) and is a new and promising communication method due to its high bandwidth and immunity to interference from electromagnetic sources [3-6]. The revolution in solid-state lighting leads to the replacement of fluorescent lamps with light-emitting diodes (LEDs), which further stimulates the use of VLC. Consider potential capabilities, organization architecture, modulation and standardization methods in VLC.

2. Overview of communication systems using visible light

Visible light communication systems (VLC) use visible light for communications, which occupies a spectrum from 380 nm to 750 nm, corresponding to a frequency spectrum from 430 THz to 790 THz.

The VLC receiver only receives signals if it is in the same room as the transmitter, so receivers outside the VLC source room will not be able to receive signals, which ensures the potential security of data transmission. Since the source of visible light can be used both for lighting and for communication, therefore, it saves additional power, which increases the transmission efficiency and increases the secrecy for outsiders, data transmission. VLC has high throughput and low power consumption.

When implementing VLC, there are a number of problems associated with interference from surrounding third-party light sources, interference between VLC devices, and VLC integration with existing wireless technologies. To overcome the identified problems, four JEITA CP-1221, JEITA Cp-1222, JEITA Cp-1223 and IEEE 802.15.7 standards have been developed.

In 802.15.7, only the channel and physical layers are defined for communication over a short distance using visible light. On the transmitter side, white light is generated at the wavelength of the LED. White light based on LEDs is generated in dichromatic, trichromatic and tetrachromatic modes. Data on the transmitter side is modulated by modulating the light; however, the modulation must be done in such a way as to avoid flicker. In addition, the dimming level selected for modulation must be such that it is supported by luminous LEDs. A typical VLC receiver consists of a gain circuit, an optical filter, and an optical hub.

The two integral parts of a VLC system: the transmitter and the receiver usually consist of three general levels. This is the physical layer, the link layer and the application layer. The reference model of the VLC communication system is shown in the figure. 2 [5]. In IEEE 802.15.7, only two layers (such as physical and channel) are defined for simplicity [6].

![Fig. 2. Layered VLC architecture.](image)

Tasks performed by the link level access control environment include [7]: support mobility, support dimming the LED, support visibility, support security, reduce flicker, support color functions, support network beacons, support installation and disconnection of the network, ensuring reliable communication between equal level link objects. Topologies supported by the link layer are peer-to-peer, broadcast and star-shaped.

The physical layer provides the physical specification of the device, as well as the relationship between the device and the carrier. Three different types of physical VLC implementations are given in IEEE 802.15.7. The capacity of the first, second, and third implementations, respectively, is 11.67–266.6 Kbps, 1.25–96 Mbps, and 12–96 Mbps, respectively.

![Diagram](image)
3. Countermeasures for information leakage

The main countermeasures consist of organizational and technical measures. Organizational measures include prohibiting the use of video cameras in the office, closing the LEDs, using more inertial incandescent or energy-saving neon lamps, and shielding windows. Separately, it is necessary to monitor compliance with the imposed administrative restrictions and regularly check them.

In most cases, organizational measures to counter information leakage are not enough to ensure the required effectiveness of information protection. It is necessary to carry out a set of technical measures to protect information, providing for the use of special technical means, as well as the implementation of technical solutions. Technical measures are aimed at closing information leakage channels by reducing the signal-to-noise ratio in places where portable acoustic intelligence devices or their sensors can be placed to values that ensure that the information signal cannot be extracted by the intelligence tool. Depending on the technical means used, passive and active methods of protecting information can be used.

Acoustic masking is effectively used to protect speech information from leakage through the direct acoustic channel by suppressing by means of acoustic noise (noise) microphones of reconnaissance equipment installed in such structural elements of the protected premises as the doorway, ventilation duct, space behind the suspended ceiling, etc. Vibroacoustic masking is used to protect speech information from leakage through acousto-vibrational and acousto-optic (opto-electronic) channels and consists in creating vibration noise in elements of building structures, window panes, engineering communications, etc. Vibroacoustic masking is effectively used to suppress electronic and radio-stethoscope as well as laser acoustic intelligence systems.

The creation of electromagnetic masking including optical low-frequency interference (low-frequency masking interference method) is used to exclude the possibility of intercepting speech information from allocated rooms using passive and active acoustoelectric information leakage channels, suppressing the channel by modulating visible light.

The ban on the use of LED lighting lamps is easily implemented, but leads to an increase in energy costs. It is worth noting that for the organization of office workplaces, open-air premises are often used, which involve the separation of workplaces only by partitions or the use of glass walls and partitions all this allows surveillance surveillance cameras to receive an optical signal from LEDs of lighting equipment and computers. Therefore, it is necessary to provide shielding of computer technology from getting into the field of view of video surveillance systems.

It is advisable to use technical systems of counteraction, including the monitoring of the state of the LEDs using a software or optical method. Detection of the use of LEDs for transmitting messages by external sensors is an ideal method, without informing the attacker of any information about the measures taken to ensure the protection of information. Such monitoring is passive and not detectable by an intruder. External detection of transmission is usually apparently very informative, but for a high probability of detection, it is necessary to know the frequency range and the type of modulation and coding of the transmitted message. We have to admit that the considered hidden optical channels of information leakage are unlikely, but they still remain difficult to detect.

4. Conclusion

The development of LEDs has made semiconductor lighting a growing area [8]. LEDs surpassed incandescent light sources in terms of reliability, power consumption and light output. The efficiency of LEDs is 20 lm / W more than incandescent efficiency [9]. LEDs and lasers are used as transmission sources for VLC. The LED should be used when communications and lighting should be performed using the same device.

The technical features of the considered transmission method such as high bandwidth, the absence of interference from radio wave radiation, the absence of harmful effects on the human body made communication in visible light an attractive promising technology and at the same time carrying the danger of organizing an information leakage channel.

Given the pace at which attackers use modern technology to breach information security, the area of VLC research in the interests of information security for its detection and suppression is relevant. All of these applications have made VLC an attractive area of research.

5. Literature

1. (http://purelifi.com/what_is_li-fi/the-li-fi-story/)
1. Introduction

The contemporary security issues, both globally and regionally, are linked to several factors:
- the persistent presence of local conflicts of varying intensity;
- increase of the number of highly motivated and highly aggressive terrorist groups that which go from anonymous acts to advertised direct attacks on civilians population and objects related to national security;
- a violent rise in organized crime, especially in the post-Soviet space.

These factors are interrelated and usually at least one of them is present in most critical situations. Against the security forces are now used not only pistols, but modern long-barreled guns with high striking capabilities against which the traditional defenses are not effective.

This calls for particular attention to be paid to the security of the army, the police and the other force structures in order to ensure safe functioning of critical infrastructure objects. The current task is to create reliable ballistic protection systems from affordable locally produced materials. The development and selection of new materials enables the realization of innovative solutions in this area.

2. Current state of the problem

The basic requirements for textile materials used in the development of protective structures are: low density to reduce the weight; high strength to increase resistance to destruction; high modulus of elasticity to reduce deformation [1, 2]. The most commonly used are fabrics of para-aramid high-modulus fibers: Kevlar (USA), Technora (Japan), Twaron (Netherlands), SVM (Russia), Armos (Russia).

Composite ballistic protection materials are multi-component materials consisting of a continuous matrix and discrete reinforcing material. The choice of matrix and of the reinforcing material determines the necessary combination of physico-mechanical, operational and technological properties. A special place in the group of composite materials for ballistic protection occupies those based on ultra-high molecular polyethylene. Unlike thearamids, they are not processed by weaving operations but are formed in the shape of sheets. High-modulus polyethylene fibers are commercially produced under the trade names of Dyneema (The Netherlands), Specta (USA), Techmilon (Japan), Espelen (Russia).

Textile and composite armors are effective against low-speed bullets but cannot provide protection from armor-piercing high-speed ammunition. That is why hybrid protective structures which include a frontal ceramic layer and a support lyre made of textile or of composite material are developed [3].

Ceramic armors are developed strictly for projectile resistance with a high hardness and compressive strength combined with an advantage of lightweight. The need for lighter protection materials for use by the military has given merit to the use of ceramic armor materials. Ceramics offer an advantage over steel in weight reduction, and over all metals in impact energy absorption. Detailed studies of ceramic armors and the basic properties of ceramics are given in [4-8].

The main physico-mechanical characteristics of ceramics for ballistic protection are shown in Table 1 [9].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Corundum AD85</td>
<td>3420</td>
<td>9.4</td>
<td>221</td>
<td>296</td>
<td>3.4</td>
</tr>
<tr>
<td>Corundum 1 AD998</td>
<td>3920</td>
<td>14.1</td>
<td>370</td>
<td>375</td>
<td>4.5</td>
</tr>
<tr>
<td>SiC</td>
<td>3200</td>
<td>24.5</td>
<td>460</td>
<td>570</td>
<td>5</td>
</tr>
<tr>
<td>B/C</td>
<td>2500</td>
<td>25.5</td>
<td>460</td>
<td>410</td>
<td>4</td>
</tr>
</tbody>
</table>

The most commonly used are high-purity corundum, silicon carbide and boron carbide, listed according to their increasing ballistic efficiency and price. Boron carbide is one of the hardest ceramic materials and is very suitable for use as a face layer in hybrid protective structures. Typical for it is that when hit by high-speed ammunitions, it behaves as a glass-like material, but this does not affect its excellent protective properties. The main reasons limiting its wide use are the high cost and the difficult manufacturing of products with complex geometry from it.

The hybrid protective structures consist in principle of a top layer with maximum hardness and high resistance against penetration which destroys partially or completely the armor-piercing ammunition and a back layer retaining the fragments of the demolished ceramics and the ammunition.

In Fig. 1 is shown schematically a hybrid protective structure and the mode of action of the armor-piercing ammunition [10].
Russian sources give the following features of hybrid protection structures providing protection against a Dragunov sniper rifle firing 7.62mm B-32 armor-piercing bullet:
- Corundum/polyethylene backing - surface density of 42 ÷ 46 kg/m², thickness of 19mm.
- Boron carbide/polyethylene support - surface density of 34 ÷ 36 kg/m², thickness of 20 mm.

The Institute of Metal Science, equipment, and technologies “Acad. A. Balevski” with Center for Hydro- and Aerodynamics at the Bulgarian Academy of Sciences has been working in the field of research and development of security systems for individual protection, in particular hybrid structures, including ballistic corundum and boron carbide ceramics, for many years. As a result of this research were obtained the materials, which were tested to assess their effectiveness against armor piercing ammunition, and were obtained the results, presented in the paper.

3. Experimental studies

2.1. Materials

2.1.1. Ballistic ceramics

Corundum ceramic was obtained by cold isostatic pressing at 127.5 MPa, followed by isothermal roasting at 1580°C for 2h.

Boron carbide ceramic was obtained by isostatic hot pressing at 200 MPa and isothermal hold at 2000 °C for 1h.

The average physicochemical properties of the ceramics used are given in Table 2.

<table>
<thead>
<tr>
<th>Material</th>
<th>Density [kg/m³]</th>
<th>Rockwell hardness “HRA”</th>
<th>Modulus of elasticity [GPa]</th>
<th>Bending strength [MPa]</th>
<th>Crack resistance coefficient [MPa.m¹/₂]</th>
<th>Sound velocity [m/s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al₂O₃</td>
<td>3890</td>
<td>65</td>
<td>385</td>
<td>301</td>
<td>4</td>
<td>10335</td>
</tr>
<tr>
<td>B₄C</td>
<td>2500</td>
<td>95</td>
<td>460</td>
<td>409</td>
<td>5</td>
<td>12000</td>
</tr>
</tbody>
</table>

For the testing of both materials are made plates with dimensions 50x50x8mm and 50x50x10mm.

2.1.2. High-modulus polyethylene Dyneema

Ultra-high molecular polyethylene Dyneema HB25 was used. The product is designed to produce solid ballistic protection elements. The surface density of the material is 127-134 g/m². Bundles of cut sheets are pressed using a 400-tonne press. The technological process, which includes pre-heating of the molds, heating of the Dyneema packages, maximum permissible temperature and change of pressure and temperature is according to the manufacturer's instructions. Finally the plates are cut to its final dimensions of 250x300x10mm using water cutting.

2.1.3. Auxiliary materials

Sikabond-T polyurethane adhesive Sika is used to glue the tiles and to pack the samples. Kevlar textiles are used for bandaging.

2.2. Test samples

The two types of ceramic tiles shown in Fig. 3 are glued to a back layer of Dyneema and are packed with Kevlar fabric. The general appearance and structure of the sample is shown in Figure 2.

The characteristics of the test samples are shown in Table 3.

Table 3: Test samples

<table>
<thead>
<tr>
<th>Sample</th>
<th>Dimen-ions [mm]</th>
<th>Ceramics</th>
<th>Dyneema</th>
<th>Total mass [kg]</th>
<th>Areal density [kg/m²]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corun- dum</td>
<td>250x300 x19</td>
<td>2.234</td>
<td>8</td>
<td>0.545</td>
<td>8</td>
</tr>
<tr>
<td>Boron carbide</td>
<td>250x300 x19</td>
<td>1.500</td>
<td>8</td>
<td>0.545</td>
<td>8</td>
</tr>
</tbody>
</table>

The tests were conducted in the Ballistic testing laboratory of the Institute for perspective defense research at the Bulgarian Ministry of Defense according to the requirements of NIJ Standard—0101.04 with ammunition 7.62x54R B-32.

The test results for corundum are shown in Table 4.

Table 4: Results of the ballistic tests of corundum ceramics with thickness of 8mm

<table>
<thead>
<tr>
<th>Shot No.</th>
<th>Ceramics</th>
<th>Paddling of Dyneema</th>
<th>Back packing of Kevlar</th>
<th>Footprint depth [mm]</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>4</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>5</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>6</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>fail</td>
</tr>
<tr>
<td>7</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>fail</td>
</tr>
</tbody>
</table>

The test results for boron carbide are shown in Table 5 and Table 6.

Table 5: Results of ballistic tests of boron carbide ceramic with thickness of 8 mm

<table>
<thead>
<tr>
<th>Shot No.</th>
<th>Ceramics</th>
<th>Paddling of Dyneema</th>
<th>Back packing of Kevlar</th>
<th>Footprint depth [mm]</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>4</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>5</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>6</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>7</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>-</td>
<td>fail</td>
</tr>
</tbody>
</table>

Table 6: Results of ballistic tests of boron carbide ceramic with thickness of 10 mm

<table>
<thead>
<tr>
<th>Shot No.</th>
<th>Ceramics</th>
<th>Paddling of Dyneema</th>
<th>Back packing of Kevlar</th>
<th>Footprint depth [mm]</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>2</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>4</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>5</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>6</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
<tr>
<td>7</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>40</td>
<td>pass</td>
</tr>
</tbody>
</table>
4. Results and discussions

Corundum ceramics: of the total 7 shots produced, there are two complete perforations of the sample after the fifth shot.

Boron carbide ceramics:
- for the 8mm thick test sample of the total 7 shots produced, there is one complete perforation of the sample after the sixth shot;
- for the 10 mm thick test sample of the total 7 shots produced, no perforation is observed.

Obviously, after each hit, changes in the structure and properties of the materials accumulate, leading to a deterioration of their protective qualities. The issue of sustainability against multiple hits is not fully understood. In addition to the number of shots, there is no clarity about time interval between the individual hits. Several years ago, studies have been conducted in the United States to specify this indicator and incorporate it in the NIJ Standard-0101.04 standard, but so far there are no concrete results.

The average depth of the footprint in the plastic block is 42mm, which meets the requirements for the degree of blunt trauma.

The conducted preliminary tests have shown that protection against the ammunition used is provided by 17 mm armor steel with an areal density of 133.5 kg/m2. The mass effectiveness of tested samples is:
- for the corundum sample with thickness of 8mm: 3.31;
- for the boron carbide with thickness of 8mm: 3.98
- for the boron carbide with thickness of 10mm: 3.45.

5. Conclusions

The results obtained show that boron carbide possesses better protective properties than corundum, both in multiple hit resistance and mass effectiveness. Both types of ceramics can be used in personal protective equipment, and the choice depends on the specific weight and price constraints.

5. References


[9]. https://www.coorstek.com/english/materials/#Engineered_Ceramics

PECULIARITIES IN CRISIS DECISION MAKING

Assos. Prof. Milen Ivanov PhD,
NMU „Vassil Levski“ Veliko Tarnovo, Bulgaria
e-mail milen_i1970@abv.bg

Abstract: An integral part of the current life of the individual, as well as of any organization, the decision is a natural act of the people, but especially of the leaders. This paper defines the concept of decision, the stages of the decision making, and the process decision-making itself in the sphere of crisis. The decision making is an important manager’s activity. It is a permanent and continuous activity performed by the managers. Besides their major functions, the managers take all the time managerial decisions concerning various problem and of various nature.

Key words: CRISIS, GEOINFORMATION TECHNOLOGY, GEOGRAPHIC INFORMATION SYSTEM, DECISION MAKING, LIDAR TECHNOLOGY.

1. Introduction

In decision making, the decision-making process is seen as an act of transforming information, including the steps to meaningfully addressing the problem, forming a list of possible actions (alternatives) and their consequences, choosing an alternative solution and analyzing the results of the decision. Often such a process is iterative, and the original set of alternative solutions can be corrected.

The solution is to choose a specific combination of goals, actions aimed at achieving this goal, and ways to use existing resources.

Within public systems, the solution is the result of analyzing, forecasting, optimizing and choosing an alternative to the many opportunities to achieve a particular goal.

The main objective of the management decision is to make a coordinating (regulatory) impact of the management system by executing basic tasks from the staff to reach the organization's goal. Reaching the depths of this task, the modern manager realizes the algorithm to fulfill his immediate duties. Here the following trends are being developed: creation of information base for timeliness of decision; setting limits and criteria for decision; organization of managed personnel. Unambiguously, decision making is a creative task mobilizing the intellectual potential of the manager.

Thus, the decision-making theory crystallizes as a certain amount of knowledge to develop, adopt and implement a managerial solution, to derive laws and principles, organizational forms, methods and technologies for the functioning of the organization's decision-making system.

Different factors (controllable or uncontrollable, manageable or unmanageable), which in most cases are random, influence a variety of factors in the decision-making process on the functioning of each real system. It is essential not only to analyze the operation of the managed system, but also to build automated information banks. In this way, the manager has the opportunity to receive relevant information on the managed system in a timely manner, as well as apostate information, by conducting an experiment or expertise, on the basis of which the stochastic nature of a number of factors associated with the functioning of the system and environmental conditions.

2. Decision and Information Assurance

The degree of information provision determines the nature of decisions not only in terms of criteria but also whether information is sufficient or inadequate, whether it concerns a limited or unlimited number of factors and whether the relationship between these factors and the outcome is in one or more dimensions.

Decisions in terms of information provision are divided into three types: secure, risky and insecure – fig.1.

Secure decisions are those where there is sufficient information, choices are known, the results of each alternative can be predicted with a high degree of certainty and there are no random elements. For example, such a decision may be the decision to draw a payroll bill of a brigade or department.

Risk decisions are related to situations where the results are not fully known but can be determined with some degree of probability. The probability is defined as the percentage chance of repeating certain events and the result of them, checked in a sufficient number of previous cases. For example, a company's decision to raise the prices of a particular product group by a certain percentage must be in line with the expected response from competitors. If, on the basis of our previous experience, we know that in 80% of previous cases competitors have done the same, there is a 20% risk that competitors will not raise prices or raise them by less than the projected% increase.

Uncertain solutions are associated with significant difficulties or inability to determine the probability of results. In these cases, there are too many variables and / or too many unknown variables, so the result can not be predicted, with any degree of probability. Such situations are present when innovations in production are introduced when entering new, unknown markets when a new senior manager is appointed in the organization, etc.

The contradiction between the economic needs for labor intensive use, material and natural resources and the limited safety of production processes inevitably increases the risk of emergency situations arising from natural disasters, technological breakdowns and / or human error.

Emergency management is one of the main tasks of the government to protect the population from the impact of natural disasters and accidents and to eradicate their consequences. This activity involves the structures of central and local government, as well as non-governmental organizations, such as the Red Cross and others. Historically, emergency management has always required the consolidation of the efforts of all responsible actors in order to achieve the desired effect on the protection of the population.

Figure 1: Three Levels of DSS Technology

\[\text{Specific DSS Applications} \quad \text{DSS Generator} \quad \text{DSS Tools}\]

1 Disaster Risk Reduction Strategy 2014-2020, Sofia, 2014
3. Concept of crisis.

The crisis situation is a particular legal regime that is introduced by the authorities designated by the law in certain areas or across the country before, during and after a threat has emerged for the purpose of using emergency measures to address and resolve the crisis and to overcome the consequences from her.

A crisis situation is introduced when the nature, intensity and extent of the crisis are particularly important and major and when it is necessary to mobilize considerable resources and knowledge to resolve it.

Resource or population crises have the following characteristics:
- most often they are unexpected;
- another feature is that they are developing rapidly, with an acute shortage of time to overcome the controversy that has arisen and to restore the system’s violated rules;
- crises and emergencies can only be managed if there is targeted information related to the emergence and development of the crisis.

Every extraordinary event is usually unique, whether it is a disaster or a security threat. On the other hand, crises usually resemble each other as they have similar characteristics, forms, structures and development. Situations that are considered to be extraordinary include a risk of escalation and may lead to unserviceable chain reactions.

In any case, any emergency situation is associated with a risk that is dependent on the direction of development and the intensity of the situation.

Intensity characterizes the magnitude of the crisis and ranges from zero to maximum values that are guaranteed to destroy the established system of rules.

By the term “crisis management” is meant a set of events that lead to putting the crisis under control. These are targeted actions to resolve the crisis in order to avoid the dangers it poses. They move its move into a favorable direction to prevent the crisis from going out of control and its transformation into conflict prevention also part of the crisis management process.

The essence of Crisis Management is the ability to exercise a controlled impact on each level of the manifestation of the crisis. Initially, it is routine to monitor, collect and analyze the information in order to promptly detect a change in the established situation that may lead to a disaster. This is a growing activity aimed at preventing the further development of the crisis, followed by reticence, a policy of limiting the influence of the country or countries, it is the active factor in crisis. The action of containment is characterized by a sustained increase of the effort and the voltage for control and elimination of the crisis and applied to switching to the next level and the latter type of actions are to build stability at a new level and to form the future relationships between the elements of the system, crises can be managed. It is necessary to do it without panic, organized and with the necessary firmness, analyzing facts and overtaking events.

The stages in which decision making passes can be considered as follows:
- Monitoring or obtaining situation-related information.
- Identification of the hazard. There are two principal issues: managing the situation itself and managing an emergency situation. In any case, strategic decisions are taken in a steady state, and in crisis situations anti-crisis decisions are taken.
- Managing and managing the crisis. The organizational approach to management requires: building a framework of competences, establishing links between decision-making centers, creating a critical information group, creating rules, and playing in practice.

The main objectives for emergency decision-making are as follows:

4. Crisis decision making.

The issue of decision-making in crisis management is extremely important because it usually depends on resources that will focus on eliminating the consequences of crises. In turn, what decision will be made in the crisis situation depends on the availability of the management potential with information. In terms of administration, decision-making is related to two other areas: hierarchical subordination; the need for publicity in decision-making.

In order to choose the optimum solution under risk conditions when the likelihood of realization of all scenarios is known, they determine the course of action associated with the best possible results. The standard formula of mathematical expectation is used:

\[ \text{Expected result (action) = Result (action, scenario) X (probabilistic scenarios (scenario))} \]

and the choice of the best solution that provides the maximum of the expected positive result or the minimum of the expected negative result (criterion for the optimal risk decision making).

The stages in which decision making passes can be considered as follows:
- Monitoring or obtaining situation-related information.
- Identification of the hazard. There are two principal issues: managing the situation itself and managing an emergency situation. In any case, strategic decisions are taken in a steady state, and in crisis situations anti-crisis decisions are taken.
- Managing and managing the crisis. The organizational approach to management requires: building a framework of competences, establishing links between decision-making centers, creating a critical information group, creating rules, and playing in practice.

The main objectives for emergency decision-making are as follows:


- reducing the negative effects on the population or eliminating the consequences of the damage;
- contributing to removing risk factors for security and stability, blocking and resolving current crises and conflicts, and permanently removing the prerequisites for the emergence of such crises in the future;
- preventing the development of different risk factors in indirect and direct threats to the security of Bulgarian citizens, society, the state and the nation.

In order to respond adequately, it is necessary:
- Preliminary preparation of the State and the system of action in crisis situations, "Preparation";
- neutralizing or reducing risk factors, "Correction";
- curtailing the escalation and spread of the crisis, "Counteraction";
- reducing the intensity of crises, "Reduction";
- Eliminating the consequences, planning and conducting actions to prevent new crises, "Reconstruction" - fig. 2.

Effective resolution of a crisis situation depends on timely and competent decision-making. It is essential that decision-makers have attitude, awareness and approach.

For uncertainty, one can speak of when a phenomenon / event is unknown or not yet known, therefore there is doubt about its future development. In this sense, uncertainty is a subjective characteristic of the environment, i.e., the degree of uncertainty is measurable to the knowledge and awareness of the person making the decision. The concentrated source of uncertainty in the market economy and civil society as a whole is uncertainty. As a characteristic of the environment influencing the activity of people and organizations, it is associated with ambiguous behavior and influence of the events from this environment. In real economic practice, this leads to the inability to determine all the inputs in the development of a given situation / event, or it is impossible to calculate the likelihood of different outcomes and consequences occurring. At the same time, the notion of "uncertainty" can be defined as a state of complexity and dynamics when uncertainty about the operating factors and mechanisms in the market economy has added to the uncertainty in achieving the desired state of the organization.

5. Making decisions in a geo-information environment.

Decisions are made on the basis of information and often information is needed about a certain location: where to go on holidays, where to build a new school, what is the closest hospital, what is the shortest route to work? Most of the daily decisions can rely on simple maps or route planners. But when more extensive and complex information has to be included in the decision making process, simple maps are not enough. More assistance is needed to handle the quantity of information that has to be taken into account. For this reason software has been developed that helps to store, maintain, visualise, simplify and analyse geospatial data, called Geographical Information System (GIS) software.

A Geographical Information System can be described as a computerised system that facilitates data entry, storage, analysis and presentation especially for spatial (geo-referenced) data. A GIS can assist in decision making when extensive and complex data has to be taken into account. For instance, when a company wants to know where to build a new store it needs information on:

- the distribution of its customers (where do my customers live);
- the infrastructure (can my customers reach the store, do I have easy access to my customers, can I supply my store easily);
- the availability of land (what parcels are for sale, at what price);
- the use of the available land (what type of soil, elevation, what kind of activities are possible and allowed).

GIS can play a vital role for analysis and in formulating the quick mitigation plans for high risk environments. GIS is one of the key tools in the environmental data framework for data validation, digital data transfer standards, data retrieval/dissemination and analysis. It can serve as the ultimate communication of environmental information to the public and policy makers since it is the technical basis for the multimedia approach in environmental decision-making.

Spatial data and associated technologies have been important for effective collaborative decision-making in disaster management. Nevertheless, challenges remain in spatial data-sharing in disaster management activities. Some studies have suggested the use of a Spatial Data Infrastructure (SDI) to overcome some of these challenges. One of the challenges of a data-sharing system is the establishment of technologies and standards for data management such that the technical staff of risk and disaster management institutions can access and use the data easily and rapidly. SDIs can be used to facilitate the development of risk assessment and relocation planning and can also support the establishment of disaster management plans to minimize damage from a potential natural disaster. The use of SDI in disaster management aids in creating the technology for web-based access to spatial information and involves organizations in disaster management as the main stakeholders for producing, updating and maintaining the required spatial datasets for disaster response. If these data are shared and exchanged, datasets will be accessible to a wider disaster management community. This collaborative environment is based on the concept of partnerships in spatial data production and sharing [12, 10].

7 Merrett H. C., Chen W. W., Applications of geographical information systems and remote sensing in natural disaster hazard, Geomatics, Natural Hazards and Risk, 2013 Vol. 4, No. 2, 145–163

The emergence of spatial data infrastructures (SDIs) is closely associated with the efforts of collecting and producing geospatial data, as well as the advancement of surveying and computer technologies. In the past decades, a large amount of geospatial data, such as remote sensing images and GPS locations, have been collected by government agencies. Meanwhile, the fast development of geographic information systems facilitates the derivation of various data products from the collected data, such as topographic maps, land cover data, transportation networks, and hydrographic features.

Spatial Data Infrastructure is an initiative intended to create an environment in which all stakeholders can co-operate with each other and interact with technology, to better achieve their objectives at different political/administrative levels. SDIs have become very important in determining the way in which spatial data are used throughout an organisation, a nation, different regions and the world.

Spatial Data Infrastructure is a strategically important issue for the countries of the European Union. Spatial Data Infrastructure (SDI) includes the following elements: technology, standards, policies and human resources.

The integration of information from satellite imagery with various other information layers allows:
- syncing a variety of data;
- verifiability check;
- updating and creating the opportunity to provide the basis for effective and sustainable governance.

The co-location of data from space and land-based sources, as well as permanent land-based monitoring (land cover and land use), enables information to be secure and reliable, end-to-end services and effective results from the accompanying analyzes, forecasting models and estimates.

A SDI can be used as an important framework to facilitate decision-making for disaster management. According to [13], an SDI is a set of mechanisms and standards for interoperability, exchange, access and data distribution. Designing an SDI model for a disaster management community, as well as the use of relevant information and communication technologies in disaster management, will improve decision-making and increase the efficiency and effectiveness of all levels of disaster management activities from mitigation to the preparedness, response and recovery phases. Governmental and non-governmental organizations are the producers and maintainers of different spatial databases. Once this set of data is shared, it can be accessed by the disaster management community to develop preparedness actions and to mitigate natural disasters.

An interesting intergovernmental initiative is the Global Earth Observation System of Systems (GEOSS), which comprises 88 nations, the European Commission and 64 international organizations and has the goal of promoting scientific networks for earth observation systems [8]. Another example of intergovernmental geo-information collection initiative was the Infrastructure for Spatial Information in Europe (INSPIRE), which emerged as an action of the European Commission and aims to promote the accessibility of geo-information in the formulation, implementation and evaluation of policies of the European Union [14].

Another aspect related to data sharing in the context of natural disasters is the Network-Centric Operations (NCO), originated in the US Department of Defense (DoD) in 1996. According to [13], network-centric can be considered as a set of necessary capacities for better sharing and access to information for people involved in risk management. According to the concept of NCO, the information is not distributed in a hierarchical way, which facilitates collaboration between the groups involved and the speed of data transmission. Thus, the implementation of a spatial data infrastructure becomes important for the organization and sharing of information, because this should be available at all levels and simultaneously through information networks.

Recent studies have discussed the use of spatial information in disaster management. In addition to traditional data from remote sensing, GNSS and cartographic maps used in GIS, non-technical internet users have recently been increasingly producing data, known as Volunteered Geographic Information (VGI), which performed well in recovery efforts; for example, after the Hurricane Katrina disaster, VGI generated mobile information using GPS technology and cameras with mobile sensors [4]. The United Nations is conducting an initiative through the United Nations Space-based Information for Disaster Management in Emergency Response (UN-SPIDER), to develop methodologies for the prevention and mitigation of natural disasters using satellite technologies, particularly orbital remote-sensing images.

6. Literature

3. Tepeliev Y. et al., Geographic Information Systems, Sofia, 2003
6. MC 296/4 NATO Geospatial Policy, 2017