

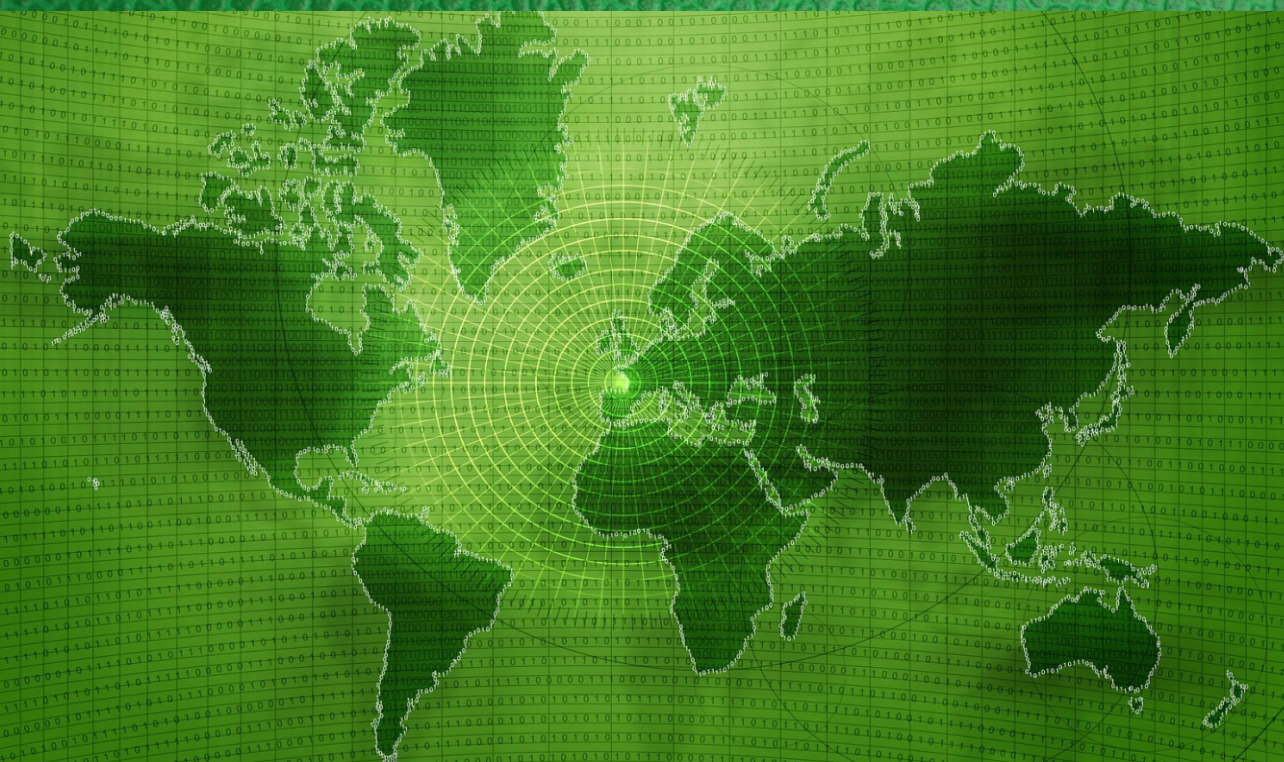
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

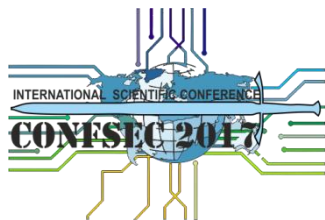
ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

YEAR III, ISSUE I/2019



**PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA**



INTERNATIONAL SCIENTIFIC JOURNAL SECURITY & FUTURE

PUBLISHER:
**SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING
INDUSTRY-4.0**

108, Rakovski Str., 1000 Sofia, Bulgaria
tel. (+359 2) 987 72 90, tel./fax (+359 2) 986 22 40,
office@stumejournals.com,
www.stumejournals.com

ISSN (PRINT) 2535-0668
ISSN (Online) 2535-082X
YEAR III, ISSUE 1 / 2019

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov
New Bulgarian University, Sofia, BG

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

CONTENTS

THEORETICAL FOUNDATIONS OF SECURITY

ARTIFICIAL INTELLIGENCE AND SECURITY. SECURITY 4.0

Prof. Radulov, N., PhD 3

CONTENT SECURITY POLICY VALIDATION

L.Petkova. PhD 6

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. 10

NATIONAL AND INTERNATIONAL SECURITY

COMPETENCE CENTRES AND INTELLIGENT SECURITY SYSTEMS IN BULGARIA

Chief Assistant Dr. Eng. Panevski V.S. 14

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

Colonel PhD. Eng. Ivaylo Angelov 17

STATE OF NUCLEAR WEAPON IN THE WORLD TODAY

Chief Assistant Professor PhD eng. Dolchinkov N. T. 22

ISLAM: THE FRIGHTENING RELIGIOUS OTHERNESS

Assoc. Prof. Dr Veselin Bosakov 25

INFORMATION SECURITY

ANALYSIS OF DATA TRANSMISSION METHODS USING VISIBLE LIGHT FOR INFORMATION SECURITY

Shvyrev B.A. PhD. (Phys.-Math.), PhD student Timonov D.A. 29

TECHNICAL FACILITIES FOR ENSURING SECURITY

COUNTER-DRONE ACTIVITY AS A SYSTEM

M.Sc. Csengeri J. PhD. Candidate 31

AGING OF THE ASC WHETLERITE TYPE GAS MASK CARBONS DURING STORAGE AND OPERATION – OVERVIEW

Assist. Prof. Dr. Eng. Liliya V. Manoilova, Mag. -Eng. Athanasios P. Chatzis, Ass. Prof. Dr. Eng. Radostin N, Nickolov 35

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 operations¹, to dispose explosive devices in terrorist activity² and even to destroy armed criminals³.

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.⁴ 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 robots⁵.

¹ <https://www.intechopen.com/books/search-and-rescue-robotics-from-theory-to-practice/introduction-to-the-use-of-robotic-tools-for-search-and-rescue>

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.

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 networks⁶, 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

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/photoz/.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 ⁷. 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 ⁸.

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 in 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

⁷ The Craft of Intelligence, 1963, Lyons Press; Reprint edition, May 1, 2016

⁸ <https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#58325e805d61>

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 ⁹.

Face recognition ¹⁰

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 them¹¹. 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

1. Dulles, A., *The Craft of Intelligence*, 1963, Lyons Press; Reprint edition, May 1, 2016
2. Goodman, Marc. *Future Crimes. Inside the Digital Underground and the Battle for Our Connected World*, Penguin Random House, 2016
3. www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photoz/g/web/glossary/bayesnet.html
4. www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/#58325e805d61
5. www.hSDL.org/?abstract&did=484061
6. www.intechopen.com/books/search-and-rescue-robotics-from-theory-to-practice/introduction-to-the-use-of-robotic-tools-for-search-and-rescue

7. www.roboticsbusinessreview.com/ai/ai-advances-facial-recognition-robots/

8. www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/

9. www.uclalawreview.org/policing-police-robots/

10. <https://watermark.silverchair.com/labmed39>

⁹ <https://watermark.silverchair.com/labmed39>

¹⁰ <https://www.roboticsbusinessreview.com/ai/ai-advances-facial-recognition-robots/>

¹¹ <https://www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/>

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 uninformed 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 occurred 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 “;”! 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]

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

	frames
frame-ancestors	Define from where the protected resource can be embedded in frames.
font-src	Define from where the protected resource can load fonts
connect-src	Define which URIs the protected resource can load using script interfaces
manifest-src	Define from where the protected resource can load manifest.
form-action	Define which URIs can be used as the action of HTML form elements
sandbox	Specifies an HTML sandbox policy that the user agent applies to the protected resource
script-nonce	Define script execution by requiring the presence of the specified nonce on script elements
plugin-types	Define the set of plugins that can be invoked by the protected resource by limiting the types of resources that can be embedded
reflected-xss	Instructs a user agent to activate or deactivate any heuristics used to filter or block reflected cross-site scripting attacks, equivalent to the effects of the non-standard X-XSS-Protection header
block-all-mixed-content	Prevent user agent from loading mixed content.
upgrade-insecure-requests	Instructs user agent to download insecure resources using HTTPS.
referrer	Define information user agent must send in Referer header.
report-uri	Specifies a URI to which the user agent sends reports about policy violation
report-to	Specifies a group (defined in Report-To header) to which the user agent sends reports about policy violation.

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]

Value	CSP version	Compatibility
base-uri	CSP Level 2	Chrome 40+; Firefox 35+; Safari 10+
default-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
script-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+

object-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
style-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
img-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
media-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
frame-src	Deprecated	
child-src	CSP Level 2	Chrome 40+; Firefox 45+; Edge 15+
frame-ancestors	CSP Level 2	Chrome 39+; Firefox 33+; Edge 15+
font-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
connect-src	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+
form-action	CSP Level 2	Chrome 40+; Firefox 36+; Edge 15+
sandbox	CSP Level 1	Chrome 25+; Firefox 50+; Safari 7+; Edge 12+
script-nonce	CSP Level 2	Chrome 40+; Firefox 35+; Safari 10+
plugin-types	CSP Level 2	Chrome 40+; Safari 10+; Edge 15+
report-uri	CSP Level 1	Chrome 25+; Firefox 23+; Safari 7+; Edge 12+

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.

Table 3: CSP directives values[2][3]

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

3.1. Nonce

The use of nonce value is more suitable for dynamically generated pages which requires the use of a sufficiently random and long nonce to prevent an attacker predicting the value for their own scripts. The use of the same nonce value on every script on the page is allowed but it needs to be re-generated and inserted into the header and all script elements on each response. [3]

The CSP directive which uses the nonce value would look like this:

```
Content-Security-Policy: script-src 'self' 'nonce-rand1234'
```

And any inline script on the page would use that value like the following one:

```
<script nonce="rand1234">...</script>
```

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:

```
<remove name="Content-Security-Policy" />
<add name="Content-Security-Policy" value="default-src 'self'
https://site.com/ *.googleapis.com www.gravatar.com player.vimeo.com
google-analytics.com googletagmanager.com blob: data;;
script-src 'self' 'unsafe-eval' *.googleapis.com www.google-
analytics.com 'unsafe-inline';
style-src 'self' 'unsafe-inline' *.googleapis.com;
img-src 'self' data: blob: www.gravatar.com *.gstatic.com umbraco.tv;
font-src 'self' blob: data: *.googleapis.com *.gstatic.com;
object-src 'self';
base-uri 'none';
frame-src 'self' site.com;
worker-src 'self' blob: data: filesystem;;
connect-src 'self' *.googleapis.com blob: file: data: filesystem;;"/>
```

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;

- A number of new fields were added to violation reports, such as **effectiveDirective**, **statusCode**, **sourceFile**, **lineNumber**, and **columnNumber**.

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 undeprecated, 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 event handlers, style attributes and javascript: navigation 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 Compatibilities [2][14]

	IE	Edge	Firefox	Chrome	Safari	Opera	Android
Content-Security-Policy Level 2	-	18 partial	67 partial	73	12.1	58	67
Content-Security-Policy Level 1.0	11 partial	18	66	73	12.1	58	67
X-Content-Security-Policy Deprecated	10+ Limited	12+ Limited	4+	-	-	-	-
X-Webkit-CSP Deprecated	-	-	-	14+	6+	-	-

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!

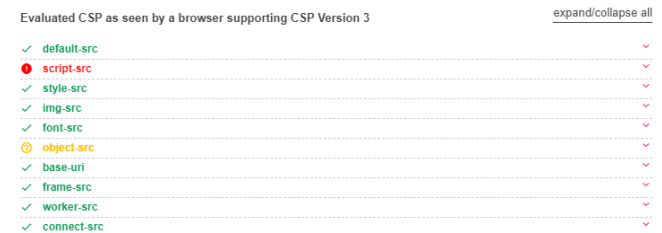
6. CSP validators

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 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]

	site A	site B	site C	site D	site E	site F
Content-Security-Policy	+	-	-	-	-	-

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 giving the necessary level of protection. If it is not properly integrated, its purpose stays unachieved.

References

- [1] OWASP, Cross-site scripting
- [2] Content Security Policy Reference, Founder Inc. 2012-2016
- [3] Content Security Policy - An Introduction, Scott Helme, November 2014
- [4] ICT Security Trends, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-766-2
- [5] Software testing, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-765-5
- [6] ICT Security Model, Willian Dimitrov, Sofia, 2018, Avangard, ISBN 978-619-160-950-5
- [7] HTTP SECURITY HEADERS, Lilyana Petkova, March 2019
- [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
- [11] Content-Security-Policy, Mozilla Developers Network, April 2019
- [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

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 dare 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 ensuring 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

- [1] M. Pawlak, *Project management*, PWN Scientific Publishers, Warszawa 2006.
- [2] Polish Committee for Standardization: PN-EN ISO 9001:2015
- [3] B. Rothery, *ISO 14000 and ISO 9000*. Publishing Information Agency, IPS Warszawa 1995.
- [4], [5], [6], [7], [8], [9], [10], [11], [12] Polish Committee for Standardization: PN-EN ISO 9001:2015
- [13] B. Rothery, *ISO 14000 and ISO 9000*. Publishing Information Agency, IPS Warszawa 1995.
- [14] Polish Committee for Standardization: PN-EN ISO 9001:2015

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:

- 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

– Areas of impact

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

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]:

sensors and radio modules (see Fig. 1 to Fig.e 7)



Fig.1
Sensor



Fig.2
PIR barrier



Fig.3
Microwave Barrier



Fig.4
Specialized camera



Fig.5
New generation of seismic sensors



Fig.6
Underground Pressure Sensor



Fig.7
Radio communication system

system solutions (see Fig. 8 to Fig. 10)



Fig.8
Jammer for underwater communications

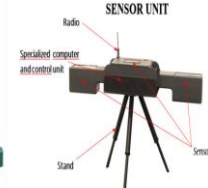


Fig.9
Anti-drone system ADD-400-1

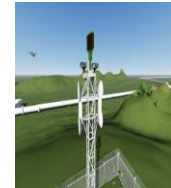


Fig.10
Pipeline Protection System

type of research and innovation organisations for cooperation

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.

integrated model for security and protection of critical infrastructure

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/cee/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.iesolutions.eu); ACCENT PRO 2000 s.r.l. (AP2K) – Romania (www.accent.ro).

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

- University of National and World Economy; University of Ruse “Angel Kanchev”, Academy of the Ministry of Interior, “G. S. Rakovski” National Defence College.

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 Vaptsarov 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.

• potential of the R&D development programme for increasing the private investments

The scientific programme of WP 2 of the CC creates opportunities for increasing the private investments in public R&D and for complementing the public expenditure with sources from public-private partnerships and projects, implemented in collaboration with the business sector. The opportunities can be grouped in two directions, namely:

- Use of the provided mechanisms through projects of the European Commission, Directorate-Generals of the European Commission, NATO, bilateral regional initiatives and international projects;

- Realization of national projects in the field of security of CI and/or protection of the population.

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:

- [1] OPINION European Economic and Social Committee, Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, [COM(2018) 630 final – 2018/0328 (COD)];
- [2] Contract BG05M2OP001-1.002-0006-C01 Creation and Development of a Center of Competence “Quantum Communication, Intelligent Security Systems and Risk Management” (Quasar);
- [3] Stoichev K., Security and Protection of Critical Infrastructure Objects. Business Continuity Planning (Monograph). Publishing complex at “Vasil Levski” National Military University, 2013, ISBN: 978-954-753-175-8, 444;
- [4] Stoichev K., Integrated model for security and protection of critical infrastructure objects. Proceedings of Third National Conference with international participation “Metal. Science, Hydro- and Aerodynamics, National Security”, 2013, ISSN:1313-8303, 309-323;
- [5] Dimitrov D.L. CRITICAL INFRASTRUCTURES RESILIENCE EVALUATION - RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS. Security and Future, 1/2018, Scientific Technical Union of Mechanical Engineering - Industry 4.0, 2018, ISSN:Print - 2535-0668; Online - 2535-082X, 7-10, p. 7 - 10;
- [6] <http://high-tech-ims.com/>.

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 CSDP 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 [1].

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 CSDP 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 are 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 uniting 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 PfP 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 restraint in most European capitals. Europeans also see a smaller relative role of purely military means in the fight against terrorism.

Europeans underestimate the psychological impact that the 11 September events have on Americans and decision-makers. The US desire to find and punish the "guilty" is enormous and the resulting actions are not always justified by Europeans. This also raises the question of Article 5 of the North Atlantic Treaty, which was first activated after the events of 9/11 - how much so. "General defense clause" in Art. 42 point 7 of the Lisbon Treaty would have the same application.

In defining the term "War on Terrorism" or "Combating Terrorism", there is also a difference in the US and EU approach to overcoming this asymmetric threat. In the first case, terrorism is defined as "War," respectively, the Laws of War are supposed and

enforced, and in the latter is defined as criminal activity, and that is why we are talking about "Fighting," in which the "Law of Peace" prevail. According to the United States, a war against terrorism has to be waged. The main role in this war is the army, through military operations, with the most powerful and modern weapons (i.e. it is the task of the Ministry of Defense). According to Europe, terrorism 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 Evertz, 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 processes 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

-
- 4 Communication from the Commission to the Council and the European Parliament 'Financing of civil crisis management operations'. Brussels, 28 November, 2001. COM(2001)647 final
- 5 Rasmussen, A. Building security in an age of austerity. Keynote speech. Munich Security Conference. 4 February, 2011 http://www.nato.int/cps/en/natolive/opinions_70400.htm
- 6 Brok, E. European security and defence: From common interests to a common identity. The path to European defence, new roads, new horizons. John Harper Publishing, 2009. p. 48
- 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
- 9 Everts, S. Unilateral America, Lightweight Europe? Centre for European Reform Working paper. February 2001 <<http://www.cer.org.uk/sites/default/files/publications/attachments/pdf/2011/cerwp9-2788.pdf>>
- 10 Brok, E. Parliamentary Control over European Security Policy. The European Union and Security Sector Reform, edited by David Spence, Philipp Fluri. John Harper Publishing. January 29, 2008. p. 141-150
- 11 European Commission COM (2017) 315 of 7 June 2017, Rue de la Loi / Wetstraat, 200 1040 Bruxelles / Brussels

STATE OF NUCLEAR WEAPON IN THE WORLD TODAY

Chief Assistant Professor PhD eng. Dolchinkov N. T.,
National Military University „Vasil Levski“, Veliko Tarnovo, Bulgaria,
National Research University "Moscow Power Engineering Institute", Moscow, Russia
n_dolchinkov@abv.bg

Abstract: *The problems of nuclear weapons in the contemporary international situation have been examined. The countries that own a nuclear weapon and those who have or are ready to produce and own it are presented.*

KEYWORDS: COUNTRIES, MILITARY, NUCLEAR WEAPONS, RUSSIAN FEDERATION, USA

1. Introduction

The issue of the dangers of nuclear weapons and its use today is particularly relevant in recent years. The threats of using this type of WMD arise from the fact that nuclear weapons are owned by a number of countries and are ready for their use for political, economic and other purposes.

The nuclear weapon is the main powerful weapon of mass destruction of the enemy.

The charge explosion energy of the normal explosive is released as a result of a chemical reaction during which explosive molecules become more resistant molecules of explosive products. In these explosions, the atoms do not undergo any change. In the nuclear explosion, the source of energy is nuclear reactions, as a result of which the atoms of some elements are transformed into atoms of other elements [nd word].

Nuclear weapons pose a huge threat to man and our environment. With its striking factors, this is one of the most deadly weapons ever created by man. Each of the striking factors could even alone kill thousands of people, break an ecological system, or destroy an infrastructure. [1]

2.1. Establishment of the nuclear weapon

Even before the creation of the atomic bomb and the emergence of the nuclear industry, the pollution of the environment with radioactive substances began. The harmful impact of radiation on living organisms and humans was not known at first, and its discoverers were one of the first victims. At the dawn of the nuclear age, as with almost all major discoveries, the public did not have the necessary information about this activity due to the secrecy of nuclear production, and it was not possible to accurately assess the impact and extent of this pollution [8].

Considering the nuclear madness of North Korea, what are the rules, whether official or hidden, which countries may have nuclear weapons and which ones? It is complicated, writes in The Washington Times. Victor Davis Hanson, a historian at the Hoover Institute at Stanford University. The issue of the proliferation of weapons of mass destruction (WMD) has never lost its relevance [3].

In the 1940s and 1950s when everyone was entitled, the original nuclear club included only countries with technological know-how, size and money to build nuclear weapons. These realities meant that by the early 1960s only the United Kingdom, France, the Soviet Union and the United States had nuclear capabilities.

The members of this small club did not worry that many other nations would make such weapons because it looked too expensive and difficult for most.

Actions that would be harmless under certain circumstances become a matter of life and death in the presence of radioactive material. To avoid such incidents or at least to reduce their number, strictly observe the laws and regulations outlined [5].

During the Cold War, the Soviet Union and the United States adhered to an unspoken rule that defeated World War II enemies - Germany, Italy, and Japan - should not have nuclear weapons. Irrespective of their financial and scientific ability to obtain them, all three former Axis forces had too much historical baggage to be able to obtain weapons of mass destruction. This silent agreement obviously still remains.

The Soviet Union and the United States also unofficially agreed during the Cold War that dependent allies who have the ability to become nuclear states, including Eastern bloc countries, most Western European countries, Australia and Canada, will not do so. Instead, they will depend on their supernatural patrons for nuclear deterrence.

A potential enemy with a YBC weapon can use it at a certain stage of the conflict. The use and consequences will be determined by the technical characteristics of the munitions, the desired impact on the course of operations and the environment. Risks and threats may include nuclear and radiological weapons, classical biological and chemical weapons, or new generation weapons as well as biochemical agents. It is quite possible that some of the funds were produced for commercial purposes and have not been pre-defined as YACH weapons [4].

In the 1970s, the realities changed again. Large and / or scientific entities such as China (1964), Israel (1967) and India (1974) became nuclear. Often such countries do this with the help of pro-Western or ProSotian patrons and sponsors. The rest of the world clearly shrugged, believing that it was inevitable that such nations would receive a nuclear weapon.

The next round of expanding the nuclear club, however, was far more irresponsible and more dangerous. Spreading depends on whether the poorer and more fragile states could get involved in uranium enrichment or secretly plutonium.

It has become clear that some countries are developing nuclear weapons, and have been stopped by preventive military strikes - such as Iraq and Syria. Others, including South Africa, Ukraine and Libya, were convinced to stop their nuclear projects. Therefore, it is imperative to use modern methods for assessing the radiation situation. The presence of detectors of different design and function allows for the timely detection, determination and measurement of all known up to now ionizing radiation [2].

Pakistan was a rare fraudster who managed to hide his nuclear enrichment, shocking the world when he tried a bomb in 1998. Pakistan rightly assumed that once a country proves its nuclear capability, it is considered too dangerous to be turned back by disarmament.

By 2012, eight countries in the world have developed and tested their own nuclear weapons. Five of these are officially recognized nuclear powers under the NPT.

Chronologically, these are the United States, Russia (inherited from the former USSR arsenals), Britain, France and China. Three more countries have tested atomic weapons outside the NPT - India, Pakistan and North Korea.

North Korea has been part of the NPT since 1985, but has not complied with the terms of the treaty and left in 2003. Israel neither denies nor confirms the possession of a nuclear weapon on its side, and has never tested it. However, many researchers suggest that Israel is a nuclear power. South Africa is the only state she owned and subsequently abandoned its nuclear arsenal.

This is a table listing the nuclear forces, the year of testing their first weapon, and the approximate number of nuclear warheads and bombs they have. This is the so-called. "Nuclear Club". Most of the nuclear units figures presented here are approximate, and in the case of North Korea, Israel and Pakistan may be quite inaccurate. It is also the number of nuclear weapons that are ready to go, and there is no mention of the number of those that are simply stored.

According to Rabohchiiska, the signatories of the Nuclear Non-Proliferation Treaty must strictly abide by all the terms of the agreement. The mechanism developed in the relevant multilateral multilateral nuclear proliferation treaties is binding on everyone and no one can interpret it in its own way [6]. Worrying is the exit from the treaty of the two major world powers - Russia and the United States.

Of nearly 65,000 nuclear weapons in 1985, just over 23,000 have remained today, of which only 4400 are available for use.

№	Country	Active nuclear warheads	Total Nuclear Heads
1.	Russian Federation	2430	11000
2.	United States	2150	8000
3.	Great Britain	300	350
4.	France	290	300
5.	China	Unknown.	240
6.	Israel	Unknown.	200
7.	India	Unknown.	100
8.	Pakistan	Unknown.	110
9.	North Korea	Unknown.	18

2.2. Nuclear weapons on the sides

The United States developed the first nuclear weapons during the Second World War. The Americans began work on the first atomic bomb in the early 1940s, with the cooperation of Canada and the United Kingdom. US military fears that Nazi Germany can develop its own nuclear weapons. The first bomb trial ("Trinity") was conducted in Alamogordo, New Mexico, in 1945.

The American land-based intercontinental ballistic missiles have stopped their development in the 70s of the twentieth century.

The only type of ground-based intercontinental ballistic missile that the United States has on arms is the LGM-30G "Minnet III". Each rocket carries a W87 nuclear power head up to three hundred kilotonnes (although it can carry up to three nuclear warheads). The last rocket of this type was produced in 1978, which means that the "youngest" among them is 38 years old. Rockets have been upgraded many times since then, and the intention is to be used by 2030.

The United States' new intercontinental ballistic missile system, known as the Ground-Based Strategic Deterrent (GBSD), or a ground based ground based nuclear deterrent system, seems to have frozen in its debating phase. The United States Air Force has requested \$ 62.3 billion for the development and production of new missiles and hopes for \$ 113.9 million in 2017. The White House, however, does not support this request. This idea actually has a lot of opponents. Development is essentially postponed by one year, and what will happen next with the Air Force plan depends largely on the outcome of the forthcoming presidential elections in 2016 [nd usa].

The USSR tested its first atomic bomb (RDS-1) in 1949. Part of the information needed for the Soviet project was acquired through espionage. The Russians set up their nuclear program to create a nuclear balance between the USSR and the United States after the Second World War. In 1953 a one-stage hydrogen bomb (RDS-6) was tested and then two-stage (RDS-37) in 1955.

Russia currently has a wide range of ground-based intercontinental ballistic missiles including mobile launching facilities. In 2015, the Missile Force with Strategic Purpose of the Russian Federation (RSCN RF) received 24 new missile complexes of the RS-24 "Yars" type (classified as SS-27 Mod 2 in the NATO classification) both in mobile and in shaft variant. These missiles can carry three or four self-directed nuclear warheads capable of penetrating missile defense systems. It can certainly be assumed

that the volume of supplies of such missiles in 2016 will not yield to the quantity delivered in 2015. So Russia will be able to replace the Topol missiles (which are basically the equivalent of the LGM-30G Missile III) with the latest generation of missiles specifically designed to overcome enemy missile defense systems [9].

Britain became the third nuclear power in the world in 1952, testing its first atomic bomb ("Hurricane") near the islands of Montebello, Australia. Nearly all of the scientific and technical information needed for the British nuclear program was acquired during the US Manhattan project. Britain sets up its nuclear weapons on the pretext that they would serve to protect in the event of a possible assault by the Soviet Union. Today, almost all British nuclear warheads are mounted on Trident missiles, which are transported by submarines.

France tested its first atomic bomb in 1960 ("Gerboise Bleue") and its first hydrogen bomb in 1968 (Operation Canopus). France's decision on nuclear weapons is motivated by its weakened status of Great Power after the Second World War and the first British nuclear experiment in 1952. After the end of the Cold War, the French cut their nuclear arsenal with 175 warheads and reformed their nuclear troops. Today, the French Army has deployed almost all its warheads of underwater missiles and bombers (such as Rafal). Some warheads are also mounted at the ICRB, fired by underground silos.

China becomes the last official nuclear power in the world. The first Chinese atomic bomb was blasted in 1964, and only three years later, the first hydrogen bomb (both attempts were made near Lop Nur). China is the first Asian nation to acquire nuclear weapons. For their creation, the Chinese government is motivated by the growing US power of the Cold War at the time.

Israel is not a member of the NPT, and does not recognize (but does not deny) the existence of its own nuclear program and weapons. Although Israel claims that the Nežjev research center near Dimona is a "research reactor," there are no published studies that have been conducted there. According to the Federation of American Scientists (FAU), Israel has nuclear material to produce a maximum of 200 atomic bombs, or they are already built. Satellite pictures reveal weapon bunkers, rocket launchers and mobile missiles, but traces of nuclear weapons have never been identified.

India is the first country to test nuclear weapons after the creation of the NPT. In 1974, a "peaceful atomic device" was blown up, as the Indian government calls it "Smile Buddha". The test was carried out near Poznań, Rajasthan. The creation of nuclear weapons in India may have been motivated by the military threat from neighboring China. India claims to have tested a hydrogen bomb in 1998, although most experts believe the test was unsuccessful because the power of the weapon was probably less than 50 kilotonnes of trotyl equivalent.

Pakistan kicks off its nuclear program in the early 1970s. The first Pakistani nuclear power plant was built in Karachi at that time, mostly with materials supplied by Western countries. Following the surrender of the Pakistani troops and India's victory in the 1971 war, Pakistani Prime Minister Zulfikar Ali Bhutto said the Pakistanis would build their own nuclear weapons even if they had to "eat grass." After the first Indian nuclear test, Pakistani scientist and metallurgist Abdul Kadir Khan steals the uranium enrichment centrifuge schemes from the Dutch company URENCO [12].

North Korea is the last country to test nuclear weapons. On October 9, 2006, North Koreans tested a small atomic bomb at 2000 meters underground. Since the power of the device is very small (about 1 kiloton), most experts believe that the experience has not been completely successful (see North Korean Nuclear Experience). The country was a member of the NPT but withdrew on January 10, 2003.

South Africa produced six atomic bombs in the 1980s but dismantled them in the early 1990s. It is possible that the 1979 test was a South African atomic bomb. South Africa signed the NPT in 1991 after the fall of apartheid.

Belarus gained 81 nuclear warheads after the collapse of the USSR in 1991. All were handed over to the Russians in 1996. Belarus signed the NPT the same year.

Kazakhstan inherits 1400 nuclear weapons as a result of the collapse of the Soviet Union. All weapons were handed over to Russia in 1995. Kazakhstan signs the NPT.

Ukraine inherited nearly 5,100 nuclear weapons after the collapse of the USSR, becoming the third largest nuclear power in the world. All weapons were voluntarily handed over to the Russians in 1996, and Ukraine signed the NPT.

Australia has had a joint military nuclear program with Britain since the Second World War. The Australian Government has provided the English for missile and nuclear sites, as well as expert assistance in the field of nuclear research. In the 1960s, however, the program was discontinued and Australia joined the NPT in 1971. Still, Australians maintain an Argentine research reactor capable of producing plutonium for atomic bombs [13].

Other countries also had nuclear technology development programs and projects, but at this stage of human development, they are members of international nuclear weapons constraints and do not formally work to develop nuclear weapons [14]. But international non-governmental organizations must monitor the actions of potential producers and make objective assessments of the situation without falling under the influence of this or any other country.

However, until the North Korea became officially a nuclear state in 2006, the nuclear club remained small (eight countries) and was believed to be manageable. Why?

First, it seemed unlikely that these nuclear states, which were relatively transparent and democratic (Britain, France, India, Israel and the United States), would start a nuclear war.

Second, it was believed that advanced, but autocratic nuclear states (China and Russia) would lose too much of globalized trade and national prosperity to start a nuclear war that everyone would lose.

Third, any fragile and violating international nuclear nations (Pakistan) are considered to be deterred and kept under control by a nuclear rival (India).

The nuclear power of dictatorial North Korea (and possibly theoretically Iran) is putting new dangers far beyond the simple arithmetic of "more nuclear peoples, a more likely nuclear war."

Neither North Korea nor Iran are democratic. None of them is a stable country.

Neither has an immediate nuclear rival to deter them and persuade them not to dare to use nuclear weapons. Both countries have begun secret nuclear programs. They both hate the United States and its allies.

More importantly, their apparent violations of Nuclear Non-Proliferation Agreements and their noticeable aggression will cause relatively powerful regional neighbors - such as Egypt, Japan, Saudi Arabia, South Korea and Taiwan - to consider developing their nuclear capabilities.

Then the club can get big fast [11].

Not all of these potential nuclear powers are democratic. But they share a pro-American perspective.

A disappointed America may feel that China and Russia have encouraged fraudulent countries such as Iran and North Korea to develop nuclear weapons programs, having self-assured that the missiles of these countries will be directed to the West and not to the East.

So now the United States is in a paradoxical position. They want to stop the full proliferation of nuclear weapons. But America also suggests that the next nuclear forces (unlike the previous one) will be pro-American - a kind of revenge to China and Russia that allow their uncontrollable friends to develop nuclear capabilities.

The United Nations and international non-proliferation organizations, albeit with good intentions, have so far proved impotent.

But despite the chaos, by 2006 there were implicit rules for the eight-member nuclear club. Now, following the crazy threats of North Korea, these general assumptions about nuclear poker are null and void. And nobody knows what to expect.

3. Conclusions:

1. Nuclear Weapons would reach the destruction of hundreds of planets like our Earth;

2. The presence of a nuclear weapon has a more deterrent effect on opponents than it would be in real use;

3. The development of nuclear weapons must be under control and the military-industrial complexes must not be uncontrollable. The control bodies must also be public and accountable to society to reduce the amount of space for weapons;

4. The use of nuclear weapons would be detrimental to the inhabitants of the Earth and terrorist organizations should not have access to such weapons.

4. Literature:

1. Гърдев Е., Н. И. Пъдарев. Реални заплахи от ядрено оръжие за мирното население, Сборник доклади от научна конференция на НВУ "В. Левски", „Радиационната безопасност в съвременния свят“, В. Т. 2017.

2. Димитров Б. Методи за наблюдение и регистриране на йонизиращи лъчения, Сборник доклади от годишна университетска научна конференция „Актуални проблеми на сигурността“, 10.2017 г. НВУ „Васил Левски“ – гр. В. Търново том 4, стр.140 -147 ;

3. Димитров Б. Развитие на системите за разузнаване, ранно предупреждение, мониторинг, специална и санитарна обработка, Сборник доклади от годишна университетска научна конференция „Актуални проблеми на сигурността“ 10.2018 г. НВУ „Васил Левски“ – гр. В. Търново, том 5, стр.226 -231 ;

4. Димитров Б. Специална подготовка за ядрена, химическа и биологическа защита – Монография – ISBN 978-954-753-286-1, 77 стр.;

5. Лилянова С., Н. Пъдарев, Радиационни инциденти с радиоактивни отпадъци Сборник доклади от научна конференция на НВУ "В. Левски", Том 4, В. Т. . 2018;

6. Рабочийска, М. Механизми за контрол по многостранните международни договори в областта на ядреното разоръжаване. – В: Белова, Г. и др. (ред). Право, управление и медии през XXI век. Том 1. [Юбилеен сборник от международната научна конференция по случай 20-год. на Правно-историческия факултет на ЮЗУ, Благоевград, 16-17 май 2012 г.]. Благоевград, Университетско издателство „Неофит Рилски“, 2012, 369-378;

7. Dolchinkov N. Radiation safety of Bulgaria in the contemporary international situation, Security and defence Quarterly No 4(13)2016, War Studies University, Warsaw, Poland, стр 3-14;

8. Dolchinkov N. History and development of nuclear weapons, International scientific journal: Security@future 1/2018, June 2018, ISSN 2535-0668 Стр. 32-35;

9. Dolchinkov N. Nuclear weapons in Russia, International scientific journal: Security@future 3/2018, ISSN 2535-0668 стр . 123-126;

10. Dolchinkov N. Nuclear weapons in NATO, International scientific journal: Science. Business. Society 4/2018, ISSN 2367-8380 стр. 181-184;

11. www.extremecentrepoint.com/archives/5800

12. <https://www.vesti.bg/svati/>

13. <https://bg.wikipedia.org/wiki/>

14. www.exportcontrol.bg/docs/DNIAO

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 activeness 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 their 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 ever-deeper 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 infidels. Territories and countries are either “the House of Islam” or “the House of War”. Armed conflicts are either a “holy war” for the true faith or “internecine 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 lense 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. Canonic 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/or 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 ethnic-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. One 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 new Islamic culture in Bulgaria, or is this rather a question of a specific kind of religious modernization that retains the fundamental postulates of the faith while shifting them into a new social context and building a space of dialogue with the democratic values currently being established in Bulgarian society? (Bosakov 2010).

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 space 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 contemporary Bulgarian society cannot be looked upon only as coexistence or as attracting the smaller cultural communities into the majority’s behavior model. It is precisely in a country like Bulgaria, where Islam and Christianity have coexisted for centuries, that dialogue, now more than ever, is the only means for effective integration and consolidation of the national community. The demonstrative, socially desirable tolerance, registered in most sociological studies, actually bears within itself a set of restrictions and suppressed conflicts that inform toleration. In the field of meanings and symbols defined as tolerance and toleration, we find projected an important part of the transformation of attitudes towards Islam and towards religious otherness in general. The Bulgarian tradition permits approaching Islam in a way that corresponds to its syncretic character and to the Bulgarian history of neighborly relations. By its significant meanings and symbolic colouring, neighborhood, as direct contact and direct spatial proximity with others, defines everyday life. This is the micro social scale in which the real dimensions of individual achievement are situated and the conditions for success are estimated. The need to comprehensively study this question in terms of space stems from the understanding of identity as a quality that is invariably a result and a condition achieved in the course of relating to others and comparing with others (in this sense, identity is the result of a qualitative definition of the Other). Ethnoreligious distances reveal the parameters of a “contactless tolerance”: in cases when assertions are proposed that do not require direct contact with others, there is greater willingness to look for socially desirable answers. Any concrete attempt to introduce religious awareness of the “others” in a situation of immediate contact leads to decreased potential willingness to accept those different others. The gap between a consistent compliance with religious morality and norms on one hand and the idea of the orthopraxis of the other religious community on the other, generates mistrust, disregard and suspicion as to the motives of people of a different faith. These attitudes correspond to a latent ethno-religious conflict, which is liable to secondary mobilization by political and economic means. In other words, neighborhood, as a universal social network of everyday practices, is able to compensate for some of the tensions, but its influence remains confined within the framework of a contradiction in mass consciousness – the contradiction between a positive attitude to the neighbor who is of a certain religious confession and, at the same time, suspicion with regard to that religious community as a whole ((Bosakov 2006).

In looking for the means to overcome the feeling of offended religious identity among the minority, an identity that it often perceives as being under threat, a careful sociological scrutiny of the culture of neighborhood and of the importance of neighborhood identifies the following states and processes: (Bosakov 2000)

- Growing modernization in everyday life is severely trying for part of the meaning and symbolism of a religion. With respect to Islam in particular, this is one of the fundamental challenges of the new millennium: to devise a model of Islamic modernity in which the basic norms of Islam will preserve their importance, while the elements of the

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 ethno-religious 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 viewed as part of the risks involved in the modern European way of life and security (Wodak 2015). But the moral defect of the modern society is greed – a greed that allows market values to penetrate the lifeworld of people that has traditionally been guided by nonmarket norms. As a result of this expansion, social relationships come to be

shaped in the image of the market. The trends dictated by our times are manifest in a great variety of areas: in consumption, technological standards, mass popular culture, youth subcultures and counter-cultures, the media and advertising, and even in elite forms of art, science and philosophy. But they all have one thing in common: directly or indirectly, these trends stem from the advance of the all-powerful global market. In recent decades the financial levers and formalized vocabulary of the market have been imposed as a kind of social algebra in widely different areas of life: the neo-liberal mantras such as efficiency, accountability, strategic planning, the project principle, optimized use of resources, maximized profit, etc., have colonized spheres of life that are quite remote from the economy, including education, healthcare, creativity, innovation, knowledge, the art market, and have oriented these spheres to results that are "immediately measurable" in an economic and managerial perspective. But is this neo-liberal religion not turning democracy, the liberal ideals, the freedom of the individual, the arts, the quality of life, etc., from values in themselves, into conditions, "dependent variables", that are important only insofar as they influence economic development? The difference between market economy and market society is this: a market economy is a means – a valuable and important means – for organizing our productive capacity. The market society, to the contrary, is a way of life where market values permeate all aspects of human striving and effort. It is a place where social relations are molded in the image of the market. The only escape from this apocalyptic situation lies in the transformation of modern democracy by means of civic control, prevention and indictment, which might put a stop to the escalating loss of legitimacy of the procedures of representative democracy and of the figures of the politician, the scientist, the expert and the judge.

REFERENCES

- Bosakov, V. 2015. *Islam and Modernity. Mutual Challenges*. Sofia: Ivrai Pbls (in Bulgarian) [Islamy i modernost: vzaimni predizvikatelstva. Sofiya: IvRay]
- Bosakov, V. 2010. *The Integration of Muslims in Bulgaria*. Sofia: Ivrai Pbls (in Bulgarian) [Integratsiyata na myusyulmanite v Balgariya. Sofiya: IvRay]
- Bosakov, V. 2009. Value Orientations of Muslims in Bulgaria. In: Fotev, G. (ed.) 2009. *European Values in Present-day Bulgarian Society*. Sofia: University Publs St. Kliment Ohridski. pp. 197-217 (in Bulgarian) [Tsennostni orientatsii na myusyulmanite v Balgariya. V: Fotev, G. /sastavitel/ Evropeyskite tsennosti v dнешnoto balgarsko obshtestvo. Sofiya: UI „Sv.Kliment Ohridski”]
- 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 izsledvaniya]
- Bosakov, V. 2000. *The Bulgarian Turks between the Culture of Neighbourhood and Religious Identity*. Sofia: LiK Pbls (in Bulgarian) [Balgarskite turtsi mezhdu kulturata na sasedstvo i religioznata identichnost. Sofiya: LiK]
- Weber, M. 1968. *Soziologische Grundbegriffe: Gesammelte Aufsätze zur Wissenschaftslehre*. Tübingen: J.B.C Mohr
- Wodak, R. 2015. *The Politics of Fear: What Right-Wing Populist Discourses Mean*. London: Sage

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).

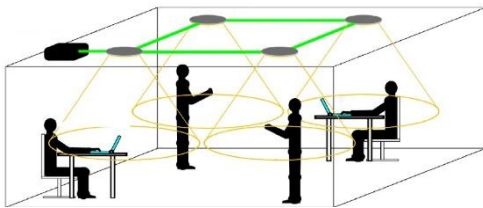


Fig. 1. The organization of communication systems using visible light

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].

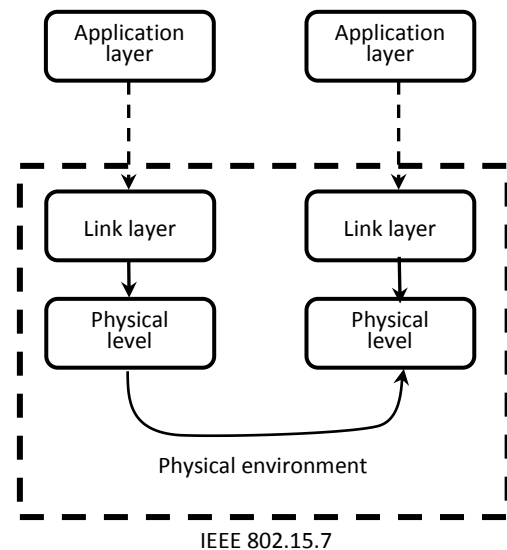


Fig. 2. Layered VLC architecture.

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.

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 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/)
2. Anurag Sarkar, Shalabh Agarwal, Asoke Nath, Li-Fi technology: data transmission through visible light, *Int. J. Adv. Res. Comput. Sci. Manag. Stud.* 3 (6) (2015).
3. Y. Wang, N. Chi, Y. Wang, L. Tao, J. Shi, Network architecture of a high-speed visible light communication local area network, *IEEE Photonics Technol. Lett.* 27 (2) (2015) 197–200p.
4. (<https://mentor.ieee.org/802.15/dcn/08/15-08-0171-00-0v1c-10mbps-visible-light-transmission-system.pdf>).
5. S. Schmid, G. Corbellini, S. Mangold, T.R. Gross, LED-to-LED visible light communication networks, in: *Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing*, 2013, pp.1–9.
6. C. Ley-Bosch, I. Alonso-González, D. Sánchez-Rodríguez, C. Ramírez-Casañas, Evaluation of the effects of hidden node problems in IEEE 802.15. 7 uplink performance, *Sensors* 16 (2) (2016).
7. IEEE, P802.15.7 – Standard for Short-Range Wireless Optical Communication, 2011.
8. Zukauskas, M.S. Shur, R. Gaska, *Introduction to Solid-state Lighting*, J. Wiley, United States, 2002.

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. Introduction¹

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 by the armed forces [4]. As a summary, see the figure below (Fig. 1.)

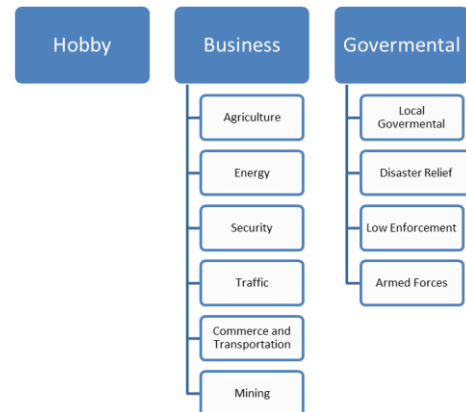


Fig. 1. The beneficial main- and subareas of drone employment²

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.).

¹ SUPPORTED BY THE ÚNKP-18-3-III-NKE-19 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY OF HUMAN CAPACITIES, HUNGARY

² Edited by the author based on references [2]-[4].

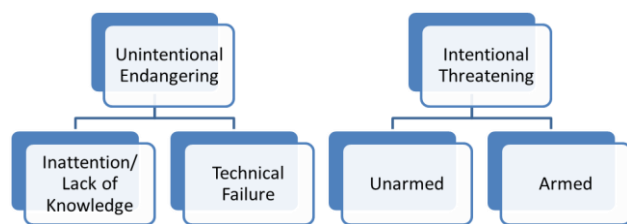


Fig. 2. The main- and subareas of risks and threats posed by drones³

3. Administrative Means for Drone Traffic Management

The author means administrative measures for drone traffic management which excludes active counter solutions, so by the former one he refers on traffic management systems, judicial regulation, production regulation, licencing, education, information and advertisement, etc.

One of the most comprehensive means of administrative measures is the so called Unmanned (Aircraft System) Traffic Management (UTM). In the interpretation of ICAO (International Civil Aviation Organization) UTM is “a concept that brings an automated ATM-like system to very low level airspace which will be occupied primarily by unmanned aircraft weighing less than 25 kgs (commonly referred to as drones). Development of this concept is underway in many States, at universities and by large aviation corporations and new start-up tech companies.” [15] At the FAA (Federal Aviation Administration, USA) UTM means an “ecosystem for uncontrolled operations that is separate from, but complementary to, the FAA’s Air Traffic Management (ATM) system. UTM development will ultimately identify services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled drone operations.” [16]

Two separate means or incorporated elements of the UTM are GeoFencing and GeoCaging. By GeoFencing an imaginary fence is raised around a given reference point (e.g. a centre of a building with a proper radius) and no drone (with the proper technology) can cross that line. [17] GeoCaging is the opposite, the drone is in an imaginary cage and cannot leave it. [18]

Informing drone users will be essential in the future about judicial regulations and changes; the ethical and responsible use of drones; and about possible drone piloting trainings. The necessity of possessing drone piloting licence is also an issue to be thoroughly discussed and examined. The standardization of drone production is also an important area to think about. In the formulating European Union rules there will be different equipment regulations regarding the drone classes also defined by the EU. The trustworthy tracing of drones is one of the essential bases of UTM and in general of reliable drone traffic management system, for example by small transponders or by other means. [19, p.114-116.] [20, p.274-277.]

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 synergic 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.).

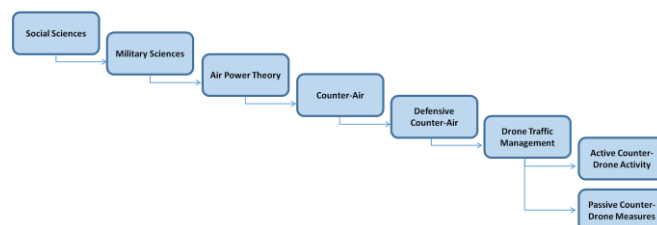


Fig. 3. Scientific categorisation of counter-drone activity

According to the fifth chapter of NATO AJP 3.3.1 B: “DCA operations are conducted primarily in reaction to adversary air and missile offensive initiatives. DCA includes active and passive measures to protect forces and vital interests from enemy air and missile attacks. DCA operations attempt interception of intruding enemy aircraft and missiles as early as possible and should be

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:

- First, the aerial target detection shall be performed and, in parallel, it need to be looking for the location of the control station by examining the signal output;
- The detected aerial target should be tracked, so with the help of a proper software to convert it from plot to tack. The tracking shall be continuous, and a predetermined trajectory prediction is also should be calculated by the actual flight properties;
- According to the available flight information or flight plan, the track needed to be identified and labelled with the sufficient identification category (i.e.: friend, x-ray, zombie, hostile, etc.);
- The intensive flow of information is also continuous, accordingly with the identification category and whether the drone is a threat or not;

- 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

- [1] Eurocontrol, European Drones Outlook Study – Unlocking the Value for Europe. 2016. [Online] Available: https://sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf (2019.01.31.)
- [2] Detektor Plusz, Rottler, V.: A drónok rendészeti alkalmazása (professional study) [Online] Available: <http://detektorplusz.hu/index.php?m=23684> (2019.02.15.)
- [3] Restás, Á.: A drónok közszolgálati alkalmazásának lehetőségei. In: Új Magyar Közigazgatás, 10/3. 2017. pp.49-63.
- [4] Varga, A. F.: A drónok mint a kockázatmentes hadviselés eszközei. In: Hadtudományi Szemle, 6/2. 2013. pp.44-58.
- [5] TechRepublic.com, Forrest, C.: 17 Drone Disasters that Show Why the FAA Hates Drones [Online] Available: <https://www.techrepublic.com/article/12-drone-disasters-that-show-why-the-faa-hates-drones/> (2019.02.26.)
- [6] The Guardian, Topham G., Perraudin, F.: Two Arrested as Gatwick Reopens Following Latest Drone Sighting [Online] Available: Letöltve: <https://www.theguardian.com/uk-news/2018/dec/21/gatwick-airport-reopens-limited-number-of-flights-drone-disruption> (2019.02.26.)
- [7] The Guardian, Rawlinson, K.: Heathrow: Police Investigate after Drone Sighting Disrupts Flights. [Online] Available: <https://www.theguardian.com/uk-news/2019/jan/08/heathrow-airport-departures-suspended-after-drone-sighting> (2019.02.26.)
- [8] Krajnc, Z.: Drónok, hibrid fenyegetés, terrorizmus a légtérből: a légi hadviselés privatizálása. In: Hadmérnök, XIII/4. 2018. pp.358-369.
- [9] The Middle East Media Research Institute, Stalinsky, S.; Sosnow, R.: A Decade of Jihadi Organizations' Use of Drones – From Early Experiments by Hizbullah, Hamas, And Al-Qaeda to Emerging National Security Crisis for the West as ISIS Launches First Attack Drones. 2017. [Online] Available: <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda#Hizbullah%20Anchor> (2019.03.01.)

- [10] Rassler, D.: The Islamic State and Drones – Supply Scale and Future Threats. West Point, Combating Terrorism Center, United States Military Academy, 2018. 24.p.
- [11] Defense One, Watson, B.: The Drones of ISIS, 2017. [Online] Available: <https://www.defenseone.com/technology/2017/01/drones-isis/134542/> (2019.03.01.)
- [12] SecurityMagazine.com, Ludwig, S.: Drones: A Security Tool, Threat and Challenge [Online] Available: <https://www.securitymagazine.com/articles/88803-drones-a-security-tool-threat-and-challenge> (2019.02.26.)
- [13] Sauvé, G.: The Menace of Drones in a Prison Environment. London, Countering Drones konferencia, 2018.12.11-12.
- [14] CNN, Ripley, W.: Drone with Radioactive Material Found on Japanese Prime Minister's Roof 2015 [Online] Available: <https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html> (2019.03.01.)
- [15] ICAO, Unmanned aerial system Traffic Management (UTM) [Online] Available: <https://www.icao.int/annual-report-2017/Pages/new-emerging-activities-unmanned-aerial-system-traffic-management.aspx> (2019.03.12.)
- [16] FAA, Unmanned Aircraft System Traffic Management (UTM) [Online] Available: https://www.faa.gov/uas/research_development/traffic_management/ (2019.03.12.)
- [17] Aerial Information Systems Corporation, What is Geofencing? [Online] Available: <https://www.aisc.aero/what-is-geofencing/> (2019.03.12.)
- [18] Single European Sky ATM Research – SESAR, SESAR project researches tracking of drones in the airspace [Online] Available: <https://www.sesarju.eu/news/sesar-project-researches-tracking-drones-airspace> (2019.03.12.)
- [19] Bódi, A.; Szabó, T.; Wühl, T.: Drónok követése közhiteles módon. In: Repüléstudományi Közlemények, XXVIII/2. 2017. pp.111-118.
- [20] Makkay, I.: ADS-B és a drónok. In: Repüléstudományi Közlemények, XXVII/2. 2015. pp.272-278.
- [21] Sathyamoorthy, D.: A Review of Security Threats of Unmanned Aerial Vehicles and Mitigation Steps. In: Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia, 2015. [Online] Available: https://www.researchgate.net/publication/282443666_A_Review_of_Security_Threats_of_Unmanned_Aerial_Vehicles_and_Mitigation_Steps (2019.03.20.)
- [22] Battelle, DroneDefender C-UAS Device [Online] Available: <https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS-technologies/dronedefender> (2019.03.22.)
- [23] Battelle, DroneDefender V2 Counter-UAS Device (video) [Online] Available: <https://www.youtube.com/watch?v=gXNxoHMUdgw> (2019.03.22.)
- [24] Shepard, D. P.; Humphreys Todd E.: Characterization of Receiver Response to Spoofing Attacks. Proceedings of ION GNSS, Portland, 2011. [Online] Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.869.1854&rep=rep1&type=pdf> (2019.03.22.)
- [25] Komjáthy, L. J., Csengeri, J.: A távirányított és pilóta nélküli repülőrendszerek alkalmazási lehetőségei a felkelők elleni műveletek során. In: Honvédségi Szemle, 145/6. 2017. pp.81-92.
- [26] Makkay, I.: Drónok harca. In: Repüléstudományi Közlemények, XXVII/1. 2015. pp.61-72.
- [27] Palmer, T. S.; Geis II, John P.: Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority. In: Air & Space Power Journal, 30/2. 2017. pp.102-118.
- [28] NATO AJP 3.3B Allied Joint Doctrine for Air and Space Operations. Brussels, NSO, 2016.
- [29] NATO AJP 3.3.1B Allied Joint Doctrine for Counter-Air. Brussels, NSA, 2010.

AGING OF THE ASC WHETLERITE TYPE GAS MASK CARBONS DURING STORAGE AND OPERATION – OVERVIEW

Assist. Prof. Dr. Eng. Liliya V. Manoilova¹,
Mag. -Eng. Athanasios P. Chatzis¹, Ass. Prof. Dr. Eng. Radostin N. Nickolov¹
University of Chemical Technology and Metallurgy 8 Kl. Ohridski, 1756, Sofia, Bulgaria
E-mail: lili_manoilova@abv; at.xatz@gmail.com; r_nickolov@uctm.edu

ABSTRACT: Based on the experience from the storage and operation of the gas masks canisters and filter canisters for collective protection, an overview has been made of one of the main disadvantages of the gas mask carbons used of type ASC Whetlerite, the declining of their protective properties as a result of the "aging" process. The "aging" factors of the gas mask carbons have been considered and mechanisms adopted for deactivation of their active phases. It has been demonstrated that the inclusion of TEDA and derivatives of pyridine in the active phase of the gas mask carbons of the type ASC Whetlerite, only partially solves the problem with the increase of the robustness against "aging" in the conditions of increased atmospheric humidity in operation and storage and for the overall solution, gas mask carbons need to be developed based on impregnation compositions other than of the ASC Whetlerite.

Keywords: ASC WHETLERITE TYPE CARBON, "AGING" OF ASC WHETLERITE TYPE CARBON, FACTORS AND MECHANISMS OF "AGING"

Up to that moment, the widest application in the modern-day gas mask filters, filters employed in collective protection applications (fixed installations, armored vehicles, naval vessels, etc.) due to the good ratio cost-efficiency, has been achieved by the gas mask carbon type ASC Whetlerite. ASC Whetlerite is an activated carbon impregnated with salts of copper, chromium and silver. This material is used by the military to provide protection against chemical warfare agents by either adsorption of the agent or by adsorption followed by chemical reaction with impregnants (primarily toxic agents with relatively low boiling points: hydrogen cyanide, cyanogen chloride, cyanogen) [1].

Regardless of the significant efficiency of the ASC Whetlerite carbons in terms of the toxic agents referred: hydrogen cyanide, cyanogen chloride, cyanogen, one of its main disadvantages is deemed to be the decrease of its protective properties mainly against cyanogen chloride as a result of some extreme conditions such as

higher humidity (including pre-adsorbed water), acidic environment, or by usage [2].

The most significant factor for quickly losing of effectiveness i.e. deactivation of gas mask (impregnated) carbon according to Nickolov [3] happens to be the so called "aging" as a result of the impact of the pre-adsorbed water.

This notion has not yet been given any summary and accurate formulation [3]. Unclear problems exist about the mechanism, as well as conditioning factors and consequences of that process. It is known [3] that it mainly affects the active supplements and in parallel, to a less extent, the basic carbon structure.

Assurance in this respect is given by the data [3] demonstrating the alteration of the protective properties against the vapors of cyanogen chloride, as a result of the "aging" (Table 1 and 2).

Table 1. Impact of the pre-adsorbed humidity by the gas mask carbon type K-5y on the protective properties of the breathing masks EO-14 after 90 days and nights in wet condition

Quantity of the pre-adsorbed humidity by the gas mask carbon type K-5y in the breathing masks EO-14, g	Sorption capacity of the gas mask carbon of the gas masks EO-14, by the vapors of cyanogen chloride, g	
	immediately after balanced wetting	after 90 days and nights storage in wet condition
about 3, corresponding to 50 % wetting	21	21
about 10, corresponding to 70% wetting	16	7
about 125 -130, corresponding to 90% balance wetting	4	0.3

Table 2. Alteration of the sorption capacity (g) by the vapors of cyanogen chloride on gas mask carbons as a result of the "aging" process

Carbon type	"Aging" type	"Aging" conditions	Sorption capacity by ClCN, mg/ml _{carbon}
Norit RG 1.5	non-aged (new)	new, received from the Drager company	8.0
Norit RG 1.5	naturally	Drager filter unit CH641 (1970) kept for 13 months under increased humidity (75 %)	4.4
Norit RG 1.5	accelerated	new, artificially "aged" for 10 days and nights under 72°C and relative humidity 90 %	0.6
Portion Type 26	non-aged (new)	Portion filter, new	12.3
Portion Type 26	naturally	Portion filter (1958) kept for 10 years under humidity 75 %	0.8
Pittsburg 12x30 ASC	non-aged (new)	kept as required	10.8
Pittsburg 12x30 ASC	naturally	Gas mask type A62 (1968) kept for 3 years under humidity 75 %	2.0
Pittsburg 12x30 ASC	accelerated	Storage as required, followed by aging for 10 days and nights under relative humidity 90 %	6.4

The tables present gas mask carbons of ASC Whetlerite type, manufactured by different companies however having minor differences by composition of the active phase. The common thing about all carbons considered is the significant decrease of their sorption capacity against the vapors of cyanogen chloride. The combination of the impact of pre-adsorbed water (as a result of the balanced wetting) with increased temperature (sample Norit RG 1.5) minimizes the impact of the storage duration and demonstrates 13 times decrease of the sorption capacity. The continuous storage in wet atmosphere (75 and more %), respectively resulting in the relevant balanced wetting, regardless of the normal ambient temperature, consequently decrease the sorption capacity against the vapors of cyanogen chloride between 2 and 10 times. The storage duration in the conditions of increased humidity can be indicated as an important factor of aging [3].

Significant number of studies have been run on the deactivation of the gas mask carbons, nonetheless, due to its exclusive complexity [4], the mechanism of irreversible decrease of the protective properties by cyanogen chloride as a result of the "aging" has not been clarified up yet. Further complication of the problem stems from the fact that some major supplements (for instance TEDA) can increase the robustness of ASC Whetlerite against the "aging" [5] as, accordingly, their role cannot be explained [2], and also because surface chemistry of the same impregnated carbons is quite complex due to the large number of compounds which can be found on the Cu-Cr impregnated carbon surface [6].

According to all researchers working on the ASC Whetlerite, the active components of the phase represent $\text{Cu}(2+)/\text{Cr}(6+)$ species. According to Pytlewski [7] several Cu-Cr NH_3 – containing species exist on the surface of Cu-Cr impregnated carbons among which, the most important effect for the removal of hydrogen cyanide, cyanogen chloride, cyanogen has $\text{CuOH.NH}_4.\text{CrO}_4$. Hammarstrom and Sacco [8] also accept that $\text{CuOH.NH}_4.\text{CrO}_4$ is the active substance at the impregnated carbon surface for the removal of toxic agents and they revealed that the deactivation under humid atmosphere is due to the conversion of $\text{CuOH.NH}_4.\text{CrO}_4$ into amorphous brochantite chromate, $\text{Cu}_4(\text{OH})_6.\text{CrO}_4$, which thereafter decomposes to CuO ,

$\text{Cu}_2\text{Cr}_2\text{O}_4$ and Cr_2O_3 [6]. This mechanism is shown in Figure 1.

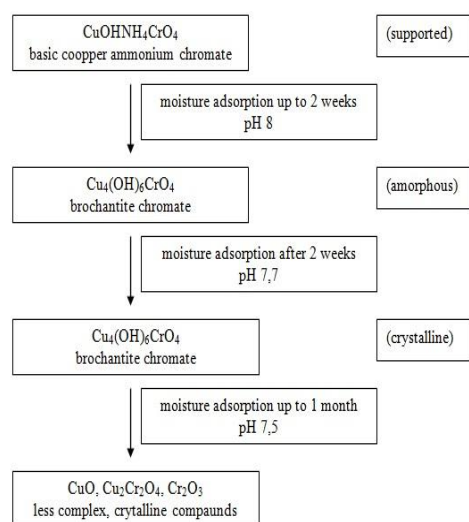


Fig.1. Moisture deactivation (ageing) mechanism according to Hammarstrom and Sacco, Jr [8]

The X-ray photoelectron spectroscopy method used by the researchers represents non-alternatively, as a main reason for the deactivation of the ASC Whetlerite type gas mask carbons, the reduction (to various extend) of $\text{Cr}^{6+} \rightarrow \text{Cr}^{3+}$ and of $\text{Cu}^{2+} \rightarrow \text{Cu}^{1+}$ surface species.

Brown et al. [9] claimed that the humid environment did not alter the oxidation state of copper, but it leads to reduction of a part of Cr^{6+} (the active species of Cu-Cr impregnated carbon surface) to Cr^{3+} .

In turn, Ehrburger et.al. [6] considered deactivation of Cu-Cr impregnated carbons as two step redox-type reaction. In a first step, chromium species are reduced from oxidation state Cr^{6+} to Cr^{3+} and copper species from Cu^{2+} to Cu^{1+} . Thereafter, monovalent copper compounds are reduced to metallic copper. The latter is observed at elevated temperature. In both cases, the reducing agent is the carbon support itself.

It should be noted, that Cr^{6+} was partially reduced by the carbon support even during the impregnation and/or the drying steps of preparation [6]. Hence the supported chromium species are generally present in the oxidation states +6 and +3 (a minor amount in the general case), as also found by X-ray photoelectron spectroscopy [10].

All studies run in terms of the deactivation of ASC Whetlerite type gas mask carbons prove the importance of the carrier, active carbon in the process referred. According to Deitz et al. [11] carbon is not an inert support. Similarly, Ehrburger et al. [12] assume that the carbon support appears to be the reducing agent of Cu^{2+} into Cu^{1+} and since the rate of aging is strongly increased in presence of water it can be assumed that the reduction of Cu^{2+} (respectively Cr^{6+}) occurs via adsorbed water in micropores of the carbon support.

In the thirties of the twentieth century Dubinin and Zaverina have proven that the active carbons gradually change their properties during storage which, according to [13] is due to the atmospheric humidity and oxygen. The limiting impact of the humidity is emphasized in [3].

All researchers of the problem relate the aging of the active carbons to the formation of surface oxygen groups (SOG). In accordance with the mechanism adopted by Dubinin [14,15] the sorption capability by water vapors of the active carbons is determined by the hemisorbed oxygen, i.e. by their Surface Oxygen Groups. Hence, the surface oxides are primary adsorption centers for the water molecules. The latter, in parallel with the connection with these centers or amongst them, interact with the carbon surface which results in the increase of its adsorption capability in terms of the atmospheric humidity. Thus, the aging cycle is closed through the increase of the content of surface oxides, respectively to the quantity of sorbed water. According to Tomassi and Neffe [16] the process considered, in a medium of increased humidity content, runs relatively fast.

According to Nickolov [3], the mechanism considered for aging of the active carbons also applies to the gas mask carbons of ASC Whetlerite type, as the active supplements in the latter further assist for the formation of primary sorption centers for water, respectively for the increase of the quantity of water sorbed by the carbons and hence for the aging of the gas mask carbons themselves.

In our opinion, the most exhaustive explanation of the "aging" of the gas mask carbons is given by Saciuk et al.[17]. According to them, the presence of pre-adsorbed water with low alkaline reaction, due to residual ammonia, engenders the dissolving of the active Cu-Cr supplements. Temperature increase (for instance in artificial "aging") accelerates the reduction of $\text{Cr}^{6+} \rightarrow \text{Cr}^{3+}$, whereat a reductor is probably the basic carbon itself. The evaporation of the pre-adsorbed water is

the onset of the recrystallization of the dissolved compounds. This does not affect the total volume of the micropores of the gas mask carbons, however depending on the type and sizes of resultant crystals can lead to its known redistribution at the account of the supermicropores.

The results from the studies of Hjermsted and Berg [18] confirm Saciuk et al. considering also the fact that dissolving and recrystallizing of active substances of ASC Whetlerite carbons in the capillary-condensed water and the surface –adsorbed water, made the microcrystals grow on the carbon surface, so the contacting area between adsorbate and active substances decreased.

Nickolov, on the basis of unpublished research results claims that in the case of the ASC Whetlerite type carbons obtained in the heat treatment at temperature higher with 20-25⁰ than the technologically accepted, the reduction $\text{Cr}^{6+} \rightarrow \text{Cr}^{3+}$, under the impact of the pre-adsorbed humidity, runs significantly faster compared to the gas mask carbons obtained while observing the technological conditions.

No effective solutions exist for fighting the aging in conditions of increased atmospheric humidity during operation and storage of ASC Whetlerite type gas mask carbons. Currently to that end, the impregnation ingredients are added up mainly by TEDA [19] (a strong basic compound [2]). To the same end, the Soviet army used pyridine [20], and the American army, besides pyridine, also used picoline [21]. Nowadays, systematic researches of the use of pyridine carboxylic acid as a supplement for the delay of aging of ASC Whetlerite type gas mask carbons are run by J. Lahaye et al. [22]. According to Baker and Poziomek [23], it has been observed that the inclusion of pyridine in the impregnation solutions for obtaining ASC Whetlerite type gas mask carbons results in the reduction of Cr^{6+} to Cr^{3+} , which lowered the interest in the use of pyridine and its derivatives.

As of that moment, regardless of the presence of a series of patents, no effective components exist in the impregnation contents for obtaining ASC Whetlerite type gas mask carbons providing adequately high robustness in terms of aging in the conditions of increased atmospheric humidity during operation and storage.

This, regardless of the good ratio cost-efficiency in ASC Whetlerite type gas mask carbons, necessitates the development of gas mask carbons based on impregnation compositions other than the ASC Whetlarite's, not including Cr^{6+} or its content minimized (>0.6 %) [24].

Conclusion

The widest use in the modern-day gas mask filters and filters employed in collective protection applications are the gas mask carbons of the type ASC Whetlerite. Regardless of the significant efficiency of the ASC Whetlerite carbons in terms of toxic agents such as hydrogen cyanide, cyanogen chloride, cyanogen, one of its main disadvantages is deemed to be the decrease of its protective properties mainly against cyanogen chloride as a result of some extreme conditions such as higher humidity (including pre-adsorbed water), acidic environment, or by usage. The most significant factor for quickly losing of effectiveness i.e. deactivation of gas mask (impregnated) carbon happens to be the so called "aging" as a result of the impact of the pre-adsorbed water. This process mainly affects the active supplements (mainly through the reduction $\text{Cr}^{6+} \rightarrow \text{Cr}^{3+}$ and much less $\text{Cu}^{2+} \rightarrow \text{Cu}^{1+}$) and in parallel, to less extend, the basic carbon structure. As of that moment, no effective components exist in the impregnation compositions for obtaining ASC Whetlerite type gas mask carbons providing adequately high robustness in terms of aging in the conditions of increased atmospheric humidity during operation and storage. This necessitates the development of gas mask carbons based on impregnation compositions other

than the ASC Whetlarite's not including Cr^{6+} or its contents minimized.

Acknowledgements

The publication has been developed under the National program „Young Scientists and Post-doctoral students” of the MES /Ministry of Education and Science/, Bulgaria.

References

- Rossin J., E. Petersen, D. Tevault, R. Lamontagne, L. Isaacson, Effects of environmental weathering on the properties of ASC Whetlerite, Carbon 29(2), 1991, 197-205
- Zhiqiang L., Z. Mingrong, C. Kuixue, The investigation for the deactivation mechanism of Cu-Cr impregnated carbon by XPS, Carbon 31(7), 1993, 1179-1184
- Nickolov R., PhD thesis, MTSRI, Sofia, 1988, and references therein
- Hammarstrom J.L., A. Sacco, Jr., Investigation of Hydrogen reactivity and its use as surface probe on high surface area Copper-Chromium-Silver impregnated charcoal, J. Catal. 100, 1986, 293-304
- Joseph A.R., X-ray Photoelectron Spectroscopy Surface Studies of Activated Carbon, CRCEC-TR-068, AD-A209 393 (1989); Kim Y.S., The 20th DOE/NRC Nuclear Air Cleaning Conference (1988)
- Ehrburger P., J. Lahaye, P. Dziedzic, R. Fangeat, Effect of aging on the behavior of copper-chromium compounds supported on activated carbon, Carbon 29, 1991, 297-303
- Pytlewski L.L., Studies of ASC Whetlerite Reactivity, Edgewood Arsenal Contract Report, EC-CR-73010, AD774835 (1974)
- Hammarstrom J.L., A. Sacco, Jr., Investigation of deactivation mechanisms of ASC Whetlerite Charcoal, J. Catal. 112, 1988, 267-281
- Brown P.N., G.G. Jayson, G. Thompson, M.C. Wilkinson, Effect of ageing and moisture on the retention of hydrogen cyanide by impregnated activated charcoals, Carbon 27, 1989, 821-833
- Ross M.M., R.J. Colton, V.R. Deitz, The study of whetlerite surfaces by X-ray photoelectron spectroscopy, Carbon 27, 1989, 492-494
- Deitz V.R., J.N. Robinson, E.J. Poziomek, Electron transmission microscopy of charcoals impregnated with ammonium salts of Cu(II) and Cr(VI), Carbon 13, 1975, 181-187
- Ehrburger P., J.M. Henlin, J. Lahaye, Aging of cupric oxide supported on activated carbon, J. Catal. 100, 1986, 429-436
- Jankowska H., J. Choma, Aktualni stan wiedzy na temat wpływu procesu starzenia i innych czynników na własności sorbentów węglowych, Biuletyn Informacyjny WChIR 2(4), 1979, 56
- Dubin M.M. Surface Oxidation and Adsorption Properties of the Active Supplements, in book: Surface chemical compounds and their role in the adsorption phenomenon, M.PUBLISHING HOUSE MU, 1957, 5-11
- Дубинин М.М., Изв. АН СССР. Сер. хим. 1981, 9-12, in Russian
- Tomassi W., S. Neffe, Biul. WAT 22, 1973, 256
- Saciuk M., M. Pietrzykowski, B. Piekarska, A. Saratowicz, Wpływ przyspieszonego starzenia na zmianę parametrów struktury kapilarnej sorbentu chromowo-miechdzioowego, Biuletyn Informacyjny WChIR 2(4), 1979, 65-77
- Hjermsted H.P., R. Berg, Am. Ind. Hyg. Ass. J. 38, 1984, 211-216
- Suzin Y., L.C. Buettner, C.A. LeDuc, Behavior of impregnated activated carbons heated to the point of oxidation, Carbon 36, 1998, 1557-1566
- M.M. Dubinin (Ed.), Basis of Protection Technique Against Chemical Warfare Agents, vol.1, VAKhZ "K.E. Voroshilov". Moscow, 1949, in Russian
- Grabenstetter R.J., E.F. Blacet, in: Military Problems with Aerosols and Nonpersistent Gases, vol. 1, 1946, ch.4, p.46
- Lahaye J., P. Ehrburger, R. Fangeat, Destruction of cyanogen chloride with 4 pyridine carboxylic acid impregnated activated carbon – I. The physical-chemistry of interaction, Carbon 25, 1987, 227-231
- Baker J.A., E.J. Poziomek, Effect of amine treatments on the chemical reactivity of Copper/Silver/Chromium Impregnated Charcoals, Carbon 13, 1975, 347-348
- Manoilova L., A. Hatzis, Iv. Spassova, R. Nickolov, Concept for the development of a new type carbon catalyst designed for protection against vapours of highly toxic substances, Machines Technologies Materials, IX(5), 2015, 27-30