

# SCIENCE & MILITARY

No 1 | Volume 12 | 2017



*Dear readers,*

Our journal Science & Military is in the twelfth year of its existence. The Armed Forces Academy of General M. R. Štefánik issues the journal Science & Military also to provide the space for presentation of scientific research results. It is undoubtedly true that science and research enhance the quality of educational process, make the career and professional development possible and create the basis on which the future of the society can be built.

The Science & Military is one of the few journals in Slovakia in which university teachers, scientists and doctoral students can regularly publish their scientific papers focused on basic and applied research in the fields of national and international security, economy and management of defence and human resources, armament, technologies, communication and information systems, military logistics as well as other areas related to military science.

We would like to continue improving our journal Science & Military in the future. We will do our best to ensure that it will contain high-quality scientific articles based on responsible and thorough literature search, working with original sources, searching as well as getting familiar with the related research conducted in Slovakia and abroad. We want the articles in the journal Science & Military to be suitable for an international scientific discussion.

Dear readers, let me briefly inform you about the contents of the latest edition.

The first article, written by Juliusz Piwowarski and Andrzej Wawrzusiszyn titled „Towards More Secure EU Borders European Border and Coast Guard“, highlighted the importance of the humanitarian, social, socio-cultural, economic, political and trans-border security importance of the refugee influx in Europe. Effective border management must be based on shared responsibility, because the crisis has shown clear shortcomings and gaps in existing mechanisms of EU standards.

The next article is titled „Low Level Profile Security Analysis in Wireless Environment“ and it was written by Martin Obert and Marcel Harakal. The authors try to predict mobile data traffic tender by extending the CAGR forecasting method (Compound Annual Growth Rate) released from Cisco. The most significant result presented in the paper is a detailed analysis of vulnerabilities of WEP and WPA wireless security protocol.

In his article, titled "Challenges and Threats for the International Security as the Consequence of the Russian Federation's Hybrid War", Miroslav Banasik presents a brief but exhaustive outline of the hybrid war, especially in terms of its definition, meaning and practical use.

The following paper „Optimal Sensor Dislocation for Target Localization in 2D and 3D Area“ by Peter Rindzák describes the possibilities of

UAV (Unmanned Aerial Vehicles) employment where the radar sensors are part of it in the area of NEC (Network Enabled Capability) in armed forces domain.

In the article titled „Ukraine in Dire Straits: The Conundrum of Ensuring its Military Security“, written by Oleg Poshedin and Maryna Chulaievskaya, the authors identified very well those international security institutions, which could be helpful in addressing the conflict in Donbas effectively. The article also describes the tools at disposal of these organizations, which might be used efficiently in the case of Russian Aggression against Ukraine.

The article titled „The Gender Issue in the Polish Armed Forces on the Example of Peace and Stabilization Operations“, written by Dariusz Kozerański, presents the engagement of Polish Military Contingents in international activities as stabilization and peace missions carried out in Afghanistan and Iraq. This paper also brings closer the question of the crisis situations causes and the relations between their participants – stressing the attention on women – soldiers – based on unique fields research provided by the author in the Republic of Iraq, Kosovo, Bosnia and Afghanistan. The article presents statistical data on the number of women in various positions and also outlines the possibility of their further deployment in peacekeeping activities.

Mariusz Rozwadowski in the article titled „Swot Analysis Tool For Restructuring of Selected Organizations Security and Public Order“ presents definitions, determinants and models of safety management as well as the positive and negative phenomena associated with the method of Swot in the selected units of the police.

The final article, which was written by Samuel Filípk and Peter Droppa and titled „Possibilities in Development of Thermal Camouflaging“, discusses the possible approaches in development of thermal camouflaging systems for the mobile military technologies.

Dear readers, let me thank you for your interest and support. I strongly believe that this edition will provide you with interesting information and ideas that will enrich your knowledge in a particular field you are interested in.

I would like to thank all the reviewers who evaluated the copies sent to the editorial board.

I hope the journal Science & Military will continue presenting high-quality articles that will help us achieve our goal, which is indexing in the SCOPUS international database.

*Col. (ret.). Assoc. Prof. Eng. Marcel HARAKAL, PhD.  
Chairman of the editorial board*

## Reviewers

Eng. Juraj <b>BESKID</b> , PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Pavel <b>BUČKA</b> , CSc.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
PhDr. Pavel <b>CZIRÁK</b> , PhD.	Ministry of Defence of the Slovak Republic, Bratislava (SK)
Assoc. Prof. RNDr. Ľubomír <b>DEDERA</b> , PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Assoc. Prof. Eng. Jaroslav <b>DOČKAL</b> , CSc.	Karel English College, a. s., Brno (CZ)
PhDr. Libor <b>FRANK</b> , Ph.D.	University of Defence, Brno (CZ)
Col. Prof. Klára Sipos <b>KECSKEMÉTHY</b> , PhD.	National University of Public Service, Budapest (HU)
Eng. Ivan <b>KOPECKÝ</b> , PhD.	Alexander Dubček University of Trenčín (SK)
Col. (GS) Tibor <b>KRÁLIK</b> , M.Sc.	Ministry of Defence of the Slovak Republic, Bratislava (SK)
PhDr. Mária <b>MARTINSKÁ</b> , PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš (SK)
Prof. Eng. Pavel <b>NEČAS</b> , PhD., MBA	The University of Security Management in Košice (SK)
Assoc. Prof. Eng. Pavel <b>PAČES</b> , Ph.D.	Czech Technical University in Prague (CZ)
Prof. Eng. Josef <b>REITŠPÍS</b> , CSc.	The University of Security Management in Košice (SK)
Eng. Karol <b>SEMRÁD</b> , PhD.	Technical University of Košice (SK)
Eng. Eva <b>ŠTEPÁNKOVÁ</b> , Ph.D.	University of Defence, Brno (CZ)
Assoc. Prof. Mgr. Jaroslav <b>UŠIAK</b> , PhD.	Matej Bel University in Banská Bystrica (SK)

## TOWARDS MORE SECURE EU BORDERS EUROPEAN BORDER AND COAST GUARD

Juliusz PIWOWARSKI, Andrzej WAWRZUSISZYN

**Abstract:** According to the current migration crisis, implementation of European integrated border management system at national and EU levels becomes contemporary priority of the European Union. It is aimed at effective management of processes directly related to organization of EU external borders crossing and facing challenges of large scale migration and countering potential threats at these borders. The same, its idea is to contribute to improvement of effectiveness in preventing and combating the phenomena of a cross-border crime and to ensure a high level of internal security in the European Union. To ensure effectiveness of implementation of these objectives, a new formation has been established at the present time – the European Border and Coast Guard. In this article authors analyse system of integrated management of external borders of the European Union and characterize its purpose, organization, structure and powers of this new EU agency - European Border and Coast Guard.

**Keywords:** Cross-border security, refugee crisis, the Schengen area, border protection, border management, immigration policy.

### 1 INTRODUCTION

In the last several years border management policy of the European Union has developed significantly: there has been created such instruments and agencies as Schengen information system, visa information system or borders agency Frontex. After short period of consolidation, came a period of new actions in response to challenges associated with the influx of immigrants and greater security concerns. It has a stronger focus on more direct operational support and the 'Europeanisation' of border management policy.

Current migration crisis poses serious problems of humanitarian, social, socio-cultural, economic, political nature, and trans-border security (and the internal security of the European Union) that never before have been witnessed by the EU. Not only the existence of the Schengen area is threatened but if this trend continues, it may seriously erode European integration. If the European Union wants to survive and be able to develop, it must recover full ability to decide who, where, when and in what purpose crosses borders and decide what requirements must be put on persons who would like to ask for permission to settle somewhere in the territory of the Community.

Therefore, the priority is to restore real, based on hard realities immigration policy, which for Europe is associated with urgent recovery of security of her own external borders. Homogenous area that was deliberately left without controls at internal borders - specified as the Schengen area – currently requires redefining common policy of external borders management. The European Union therefore works at identifying common standards of control at external borders and gradual implementation of an integrated system for management of these borders. An important issue is the establishment of the European Border and Coast Guard.

### 2 EVOLUTION OF SECURITY CONCEPT OF EXTERNAL BORDERS OF THE EUROPEAN UNION

The first step towards common European external border management was made on 14 June 1985, when five of ten of the European Economic Community Member States have signed the Schengen Agreement<sup>1</sup>, which five years later has been supplemented by the Convention implementing the Schengen Agreement.<sup>2</sup> The foundation of cooperation was to be mutual trust between States allowing the efficient use of instruments such as implementation of the law on border control and border management standards.

In the initiative of creation of joint border services a number of advantages were pointed out. In particular, among these advantages, we have to mention the increase of security of the European Union territory, and the increase in awareness of nation states' citizens creating the body of the Union, as to their belonging to one cultural and socio-political area<sup>3</sup>. In addition, costs related to the

<sup>1</sup> Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, signed in Schengen 14 June 1985. Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders signed in Schengen 19 June 1990.

<sup>2</sup> Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders signed in Schengen 19 June 1990.

<sup>3</sup> Comp. PIWOWARSKI, J.: *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*. Słupsk : Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, 2016.

management of borders would be distributed among all Member States<sup>4</sup>.

The foundation of the system has become the principle that better control management of external borders of the Union will help to fight against terrorism, illegal immigration organisations, human trafficking. The same, it will positively impact on the level of security of Member States and their citizens. In the prepared plan of actions it was stated that at the legislative level common solutions should be adopted, and at the operational level – realisation of joint operations of national services responsible for control and protection of external borders.

Plan of the Member States' of the European Union external borders management was agreed by the Council in 2002. This plan in its assumptions confirmed the need for establishment of a common experts unit in the field of borders competence, as a mean to establish integrated management system of external borders of the EU.

In 2004 were adopted conclusions on the structure, functional requirements, and biometric identifiers that should be included in the future European visa system. A year later, the European Council set targets in the field of area of security and justice development for the next five years, representing a new stage on the road for creation European policy of external borders of the Union management.

System of integrated external borders management of the European Union is based on specific terms of proceedings:

- firstly, the spine of management of external borders is the Schengen borders code, which includes provisions for border crossing points at external borders and conditions for temporary reintroduction of controls at internal borders<sup>5</sup>,
- secondly, as not all the Member States have external borders, that have to be controlled, and are not affected in the same way by cross-border movement, the European Union uses its funds to offset some of the costs incurred by the Member States with external borders. In 2007-2013 the financial burden-sharing mechanism was carried out by the External Borders Fund<sup>6</sup>; in 2014-2020

it has been replaced by the Internal Security Fund: borders and visas<sup>7</sup>,

- the third category includes measures related to the creation of centralized databases for migration and borders management: the Schengen Information System (SIS)<sup>8</sup>, the Visa Information System (VIS)<sup>9</sup> and fingerprinting system Programme 'Solidarity and Management of Migration Flows'. Eurodac<sup>10</sup>, allowing the identification of asylum seekers and illegal immigrants,

<sup>7</sup> Regulation (EU) No 514/2014 of the European Parliament and of the Council of 16 April 2014 laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, preventing and combating crime, and crisis management.

<sup>8</sup> According to art. 93 of the Convention implementing the Schengen Agreement, the purpose of the Schengen Information System shall be in accordance with this Convention to maintain public policy and public security, including national security, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system. This is the first in Europe police system of information flow that allows automatic transmission of data. When you enter specific information about the person (for example, queried, or observed by the Police) or a particular event to the national system, it is immediately available in the computer terminals of other countries. We have to mention the Schengen Information System of second generation (SIS II), more functional, modernized version of the system. Legal basis of SIS II gives two acts based on Title VI EU Treaty, which is Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Source: Wawrzusiszyn, A. *Wybrane problemy transgranicznego bezpieczeństwa Polski*. Warszawa : Wydawnictwo Naukowe DIFIN, 2012. p. 107-116.

<sup>9</sup> The Visa Information System (VIS) allows to improve cooperation between the Member States of the European Union i.a. in the field of common visa policy within the framework of the European Union and preventing visa trade. In the VIS are collected data of the applicant and information of visa application, as well as the same visa (if it was released, cancelled, revoked or renewed, or denied its prolongation). The system includes biometric data, photographs and fingerprints of a person making application for visa. Thanks to the system, border services officers during passport controls have the ability to verify the identity of people crossing borders of the Schengen area. Source: Wawrzusiszyn, A. *Wybrane problemy transgranicznego bezpieczeństwa Polski*, op. cit., p. 107-116.

<sup>10</sup> Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

<sup>4</sup> More: BURSKI, L.: *Frontex jako kluczowy element współpracy w ochronie granic zewnętrznych Unii Europejskiej*. Studia i Komentarze Instytutu Europy Środkowo-Wschodniej, nr 17, 1/2011, Lublin 2011.

<sup>5</sup> Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).

<sup>6</sup> Decision No 575/2007/EC of the European Parliament and of the Council of 23 May 2007 establishing the European Return Fund for the period 2008 to 2013 as part of the General Programme 'Solidarity and Management of Migration Flows'.

- fourthly, there is a set of measures (the so-called package of means relating to intermediaries)<sup>11</sup>, whose purpose is to prevent unauthorized entry, transit and stay and punishment for those acts,
- fifthly, implementation of simplified rules for local border traffic<sup>12</sup>,
- the last category are the means concerning operational cooperation on border management, which focus around the European Agency for the Management of Operational Cooperation at the External Borders (Frontex)<sup>13</sup>.

In many ways, the influx of immigrants led to the Europeanisation of border management. The Treaty of Lisbon<sup>14</sup> provided joint border management policy. The Program of Stockholm<sup>15</sup> included a call for assessing the possibilities of creation of an European system of border guards; this appeal was only repeated five years later in the conclusions of the European Council<sup>16</sup> of June 2014. Once again,

a stimulant for action of the European Commission<sup>17</sup> has become the migration crisis and constant criticism from Member States that the European Union does not control her external borders.

In September 2015 the European Council called for the tightening of controls at these borders, as well as to increase resources for Frontex, EASO<sup>18</sup> and Europol<sup>19</sup>. The idea was to strengthen the mandate of Frontex, in particular by allowing the direct purchase of equipment, a significant increase in its human and financial resources and to increase its role in *return operations*<sup>20</sup>.

The aim of current policy of the Union in the field of external borders management is the development and implementation of the European integrated border management at national and EU levels, which is an inevitable consequence of free movement of people within the Union and an essential element of area of freedom, security and justice.

European integrated border management system is today essential to improve the management of the migratory phenomena, having unknown level of dynamics. Integrated border management system is based on a four-level access control model, includes measures in third countries, for example in the framework of the common visa policy, measures in neighbouring third countries, measures of border control at external borders, risk analysis and

<sup>11</sup> See Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence (2002/946/WSiSW).

<sup>12</sup> Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 december 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.

<sup>13</sup> Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Dz. U. L 349, 25.11.2004); Council Decision of 26 April 2005 designating the seat of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (2005/358/EC) (Dz. U. L 114, 4.5.2005).

<sup>14</sup> Treaty of Lisbon – official name of this act is Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. The Treaty is also unofficially named as reforming treaty, it is an international treaty i.a. reforming institutions of the European Union.

<sup>15</sup> The Program of Stockholm – set out of priorities of the European Union, which have been adopted in the area of justice, freedom and security for the period 2010-2014.

<sup>16</sup> The European Council consists of heads of States or heads of Government of the Member States within the European Union. Most nation states are currently represented by Prime Ministers, with the exception of Cyprus, France, Lithuania and Romania, which are represented by Presidents, and its President (elected by the European Council on 2,5-years tenure) and President of the European Commission. In its work it takes also part the High Representative of the Union for Foreign Affairs and Security Policy. However, it should not be mistaken with the Council of Europe. The Treaty of Lisbon has confirmed status of the European Council as an institution of the European Union.

<sup>17</sup> The European Commission is the executive body of the European Union and represents interests of the Union as a whole (and not the interests of particular countries). It is the executive body of the European Union, which is responsible for providing current European Union policies and oversees work of all its agencies and manages its funds. The European Commission has an exclusive legislative initiative in the field of EU law and is entitled to issue implementing regulations (Commission Regulation). Its headquarters is the capital of Belgium, Brussels. The Commissioners are similar to Ministers in of Governments of particular countries. For each Member State of the European Union there is one Commissioner, however, each of them should represent interests of the whole European Union.

<sup>18</sup> The European Asylum Support Office (EASO) is a European Union (EU) agency. Its function is to: boost the cooperation of Member States on asylum matters, support the Member States whose asylum and reception systems are under particular pressure, improve the implementation of the Common European Asylum System (CEAS).

<sup>19</sup> The European Police Office (Europol) is the EU's law enforcement agency, whose remit is to help make Europe safer by assisting law enforcement authorities in EU member countries.

<sup>20</sup> *Return operation* means an operation that is coordinated by the European Border and Coast Guard Agency and involves technical and operational reinforcement being provided by one or more Member States under which returnees from one or more Member States are returned either on a forced or voluntary basis.

measures within the Schengen area and the returns. The full implementation of the above assumptions will ensure consistency with other policy objectives.<sup>15</sup> December 2015, the European Commission adopted measures in force for integrated management of the external borders of the European Union and the protection of the Schengen area without internal borders, to help to manage migration more effectively, improve internal security of the European Union and ensure compliance with the principle of free movement of persons. The Commission has proposed, *inter alia*, to create the European Border and Coast Guard.

### 3 EUROPEAN BORDER AND COAST GUARD

6 October 2016, at Captain Andreevo Bulgarian-Turkish border crossing, the start of operation of the Agency European Border and Coast Guard<sup>21</sup> (European Border and Coast Guard-EBCG) was inaugurated, which replaced the European Agency for the Management of Operational Cooperation at the External Borders (Frontex). The new agency retained the shortcode Frontex, however, its mandate has been greatly extended.

The European Border and Coast Guard was created by the European Agency of Border and Coast Guard and the national authorities of the Member States responsible for border management, including coastal guards in the field of carried out border control tasks.

Main purpose of the European Border and Coast Guard is to ensure the effective functioning of an integrated system for management of external borders of the European Union. It will take care of effective management of migration flows and a high level of security in the Union, in full respect of fundamental rights.

Although that still on the Member States lies the primary responsibility for management of their external borders, in own and of all Member States interest, new formation will support the use of EU measures relating to the management of external borders by strengthening, evaluation and coordination of activities of the Member States in implementation of these measures and the returns.

A particular challenge will become the activities related to migration and prevention of potential threats at external borders and thus to contribute to the fight against serious cross-border crime. The European Border and Coast Guard was equipped with the necessary financial resources, human resources and hardware.

### 4 ORGANIZATION AND STRUCTURE OF THE EUROPEAN BORDER AND COAST GUARD

The Agency is a body of the European Union and has legal personality. May acquire or dispose movable and immovable property and be a party of legal proceedings<sup>22</sup>. It is independent in performance of its mandate and operating. It is represented by the Executive Director, and its administrative seat is the Polish capital, Warsaw.

Administrative and management structure of the Agency shall comprise:

- the Management Board,
- the Executive Director,
- the Consultative Forum,
- the Official for Basic Rights.

The Management Board is responsible for taking strategic decisions by the Agency, as well as, *inter alia*, appoints the Executive Director and his Deputy, shall adopt decisions on establishment of the common integrated risk analysis model, the nature and conditions of sending liaison officers to the Member States, adopts technical and operational strategy, adopts annual report on activities of the Agency, determines organisational structure of the Agency and personnel policy, approves working arrangements with third countries. The Management Board shall each year send the European Parliament and the Council any information relevant to the outcome of evaluation procedures to be carried out by the Agency.

The Management Board is composed of one representative of each Member State and two representatives of the Commission. Therefore, each Member State shall designate a member of the Management Board and an alternate who will represent the Member in his absence. The Commission shall appoint two members and their alternates. The term of the Management Board members takes four years and can be extended. The Management Board shall hold at least two ordinary meetings a year; in addition, it shall meet on initiative of the President, at request of the Commission or at request of at least one-third of its members.

The Executive Director shall be a legal representative of the Agency, manages it and is completely independent in the performance of their duties. He speaks at the European Parliament at the latter's request and regularly reports to it. Primarily he is responsible for the preparation and implementation of the strategic decisions taken by the Management Board, as well as for decision-making related to its operational activities. The Executive Director is responsible for its activities to the Management Board.

---

<sup>21</sup> More: Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.

---

<sup>22</sup> Ibidem.



The Agency shall establish the Consultative Forum in support of the Executive Director and the Management Board with independent advice on matters relating to fundamental rights. Therefore, to participate in the consultation forum shall be invited representatives of the European Union Agency for Fundamental Rights, EASO, United Nations High Commissioner for Refugees<sup>23</sup> and other organizations. Methods and work programmes are prepared with their support. The Board also appoints the Official for Basic Rights, whose task is to participate in the work on the strategy of the Agency on fundamental rights, as well as to monitor and promote the observance of those rights by the Agency. The Official is independent in performance of his duties. He shall report directly to the Executive Board and cooperates with the Consultation Forum.

The Agency has its own financial resources. Budget consists of: the European Union grants, fees for services rendered, voluntary contributions of the Member States. However, any expenditure incurred administrative costs, infrastructure, operational and staff.

## 5 COMPETENCE OF THE EUROPEAN BORDER AND COAST GUARD

The Agency pursues its competence without interfering the responsibility of the Member States with regard to maintenance of public order and protection of internal security<sup>24</sup>. Through its actions contribute to combat cross-border crime, such as smuggling of migrants, trafficking in persons and terrorism, as well as to detect them, if there are appropriate circumstances to take such action. Cooperates and coordinates its activities with Europol and Eurojust<sup>25</sup> – agencies responsible for promoting and enhancing the effectiveness of activities of the Member States in preventing and combating serious crime affecting at least two Member States.

For implementation of assigned competence the Agency has the intervention reserve of border guards and equipment. The group counted 1,5 thousand experts, which, if necessary, will be deployed in three days. It is important that the Agency can acquire the equipment and use of technical equipment provided by the Member States. It is also assumed that the human resources by 2020 will reach the level of 1000 people employed on a permanent basis, including officers working in the field.

An extremely important role of the Agency is monitoring and supervision. Monitoring and risk analysis centre will oversee migration flows into and within the European Union and will carry out risk analysis and mandatory assessments of vulnerability in order to identify and eliminate weak points. Risk analysis will be drawn up on the basis of information of the Member States on the situation, trends and potential threats at external borders and on the returns. They shall include, inter alia, statistics and operational information collected in relation to the implementation of the Schengen acquis and the information obtained from the analytical layer national security system. Results of the common integrated risk analysis model will be included in the development of common training programmes of border guards and personnel performing tasks in the field of returns.

Through their liaison officers, the Agency provides regular monitoring of the management of external borders. Their role is to promote cooperation and dialogue between the Agency and national authorities responsible for border management and the returns, including coastguards in the field carried out border control tasks. Report of the liaison officer is a part of the exposure assessment: assessing the ability and readiness of Member States to face the upcoming challenges at external borders, determination of possible effects and the resulting impact on functioning of the Schengen area, as well as their ability to participate in a rapid reaction reserve.

The Agency evaluates operational capacity, technical equipment and resources available to the Member States to combat the challenges at external borders, and, in the case of shortcomings, obliges the Member States to improve the situation within a specified period.

A very important competence, from the activities of the Agency, is the right to intervene. In the face of specific and extremely difficult challenges, in the event of a mass influx to points at external borders of third-country citizens trying to enter illegally the territory of a Member State, Member States may apply for joint operations and quick interventions at the borders. The objectives of these activities are achieved usually by the so-called multifunctional operations (combating migrant smuggling or trafficking, migration management, including

<sup>23</sup> United Nations High Commissioner for Refugees is UN body authorized to lead and coordinate international action to protect refugees and resolve their problems around the world. The main task of the Office is to ensure rights of refugees and asylum assistance or repatriation.

<sup>24</sup> More: Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.

<sup>25</sup> The European Union's Judicial Cooperation Unit – the European Union agency of prosecutor character, aimed at supporting and strengthening coordination and cooperation between national investigating and prosecuting authorities in relation to fighting trans-border organized crime in the EU. Coordination concerns the investigative proceedings and settlement proposals in respect of legal aid.

identification, registration, chatting, returns, etc.). To carry out these operations detailed plans are prepared, specifying organizational and procedural aspects of joint action. However, in the situation of migratory pressures in the area of external borders hotspot<sup>26</sup>, with a large influx of mixed migratory movements, a Member State may ask for technical and operational strengthening by the European border and coast guard units<sup>27</sup>. The scope of the above actions could include:

- assistance in checking the third-country citizens arriving on external borders, fingerprinting and provide information on the purpose of these procedures,
- provision of information to people who intend to apply for international protection, targeting those persons to competent authorities of the Member State or to EASO,
- technical and operational assistance in the field of the return – preparation and organization of return operations.

Teams supporting migration management include, if necessary, experts in the field of protection of children, fight against human trafficking, protection from gender-related persecution or in the field of fundamental rights.

Noteworthy is the fact that, in the case where a Member State fails to take the measures proposed by the Agency or, when migratory pressure poses a threat to the functioning of border services in accordance with the Schengen rules, the European Commission may submit to the Council a plan of action. The Council shall decide then whether sending a rapid response team is necessary. This plan of action should be agreed by the Member State and the Agency before it comes to the deployment of border guards. If a Member State opposes the decision of the Council, the other Member States of the European Union will be able to start a temporary border controls with that State.

The Agency plays a special role in the field of returns, and most of all:

- coordinates technical and operational-level returns-related activities of Member States,

- provides technical and operational assistance to Member States which face particular challenges to their returns systems,
- coordinates the use of appropriate information systems and provides support to the Member States in the field of consular cooperation for establishing the identity of third-country citizens and obtaining travel documents,
- organizes and coordinates the returns operations and provides support for voluntary departures in cooperation with the Member States,
- organizes, supports and coordinates activities for exchange of information and identification and collection of best practices in the field of returns between the Member States,
- finances or co-finances actions, interventions and actions in accordance with the financial regulations.

In created the European Office for Returns, in the framework of the Agency, shall function European intervention teams for returns consisting of experts in the field of removal, monitoring and returns. They will be responsible for the effective return of illegally staying third-country citizens. EU standard travel document for return purpose will ensure wider acceptance of returnees by third countries.

A new competence of the Agency is supervising the coastal guards. The national coast guard became part of the European Border and Coast Guard as it performs tasks of border control. The mandates of the a Community Fisheries Control Agency<sup>28</sup> and the European Maritime Safety Agency<sup>29</sup> have been adapted to the tasks of the new European Border and Coast Guard. These three agencies can now take joint actions in the field of supervision, for example, jointly using drones in the Mediterranean. Specific forms of cooperation in the field of coast guard functions are specified in the working agreement in accordance with the mandates assigned to them and the financial rules applicable to these agencies.

The Agency facilitates and supports the technical and operational cooperation between Member States and third countries in the framework of external relations policy of the European Union. It also works in the framework of working agreements specifying the scope, nature and purpose of the cooperation, even operational.

Significant attention is paid to Agency training activities and scientific research. It provides training and seminars for officers of competent national

---

<sup>26</sup> The hotspot area means an area on which the host Member State, the Commission, competent agencies of the Union and Member States cooperate in order to manage an existing or potential extremely difficult challenge of migration, which is characterized by a significant increase in the number of migrants arriving at external borders.

<sup>27</sup> European Border and Coast Guard teams means teams of border guards and other members of staff of the participating Member States sent as national experts to the European Agency for Border and Coast Guard, deployed during the joint operations and rapid border intervention teams and supporting management of migration.

---

<sup>28</sup> Regulation (EU) 2016/1626 of the European Parliament and of the Council of 14 September 2016 amending Council Regulation (EC) No 768/2005 establishing a Community Fisheries Control Agency.

<sup>29</sup> Regulation (EU) 2016/1625 of the European Parliament and of the Council of 14 September 2016 amending Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency.

authorities in the field of the Union law and international law and fundamental rights, and for members of the European Border and Coast Guard teams advanced training appropriate to type of performed activities and granted permission. It is also entitled to organising, in cooperation with the Member States and third countries, training activities in their territories. In addition, the Agency is actively monitoring research and innovation relevant to the European integrated border management, including the use of advanced surveillance technology, and participates in it.

For effective operation, the Agency shall take all necessary measures in order to facilitate the exchange of information relevant for its tasks with the Commission and the Member States and, where appropriate, with competent agencies of the Union. Developed information system enables the exchange of classified information with those entities, and the exchange of personal data.

In order to carry out their powers, the Agency shall cooperate with the Commission, other bodies, offices and agencies, the European External Action Service, EASO, Europol, the European Union Agency for Fundamental Rights, Eurojust, the European Union Satellite Centre, the European Maritime Safety Agency and the European Fisheries Control Agency. It focuses on migration and prevention and detection of cross-border crime, such as smuggling of migrants, trafficking persons and terrorism; it can work also with international organisations and third countries. Such cooperation takes place within the framework of working arrangements concluded with relevant authorities.

## 6 CONCLUSION

Security and border management are now becoming key issues in European discussions, because effects of neglect in this area Europe can feel very painfully. The crisis triggered by a *de facto* uncontrolled influx of refugees made Brussels began to consider changes in the approach to external borders. Effective border management must be based on shared responsibility, because the crisis has shown clear shortcomings and gaps in existing mechanisms of EU standards.

The European Border and Coast Guard should ensure a true joint border management in accordance with the principle that all the countries of the European Union should share responsibility for security of external borders. This decision is one of the most important points of the strategy for resolving the refugee crisis, which threatens to overwhelm the Schengen system. Establishing the formation analysed in this article is not a panacea for today's problem of mass exodus. The new entity is not an antidote that can resolve the crisis, or immediately restore correct functioning of the great achievement of Europe, which is the Schengen area.

However, this is the first decisive step, without which all the rest of legislative proposals to resolve the refugee crisis and save the Schengen, would remain only an expensive, but ineffective effort.

## References

- [1] ADAMSON, F. B.: Crossing Borders: International Migration and National security. In *International Security*, 31/1.
- [2] BURSKI, Ł.: *Frontex jako kluczowy element współpracy w ochronie granic zewnętrznych Unii Europejskiej*. Studia i Komentarze Instytutu Europy Środkowo-Wschodniej, nr 17, 1/2011, Lublin 2011.
- [3] CASTLES, S., MILLER, M. J.: *The Age of Migration. International Population Movements in the Modern World*, 4<sup>th</sup> ed., Palgrave Mcmillan 2009.
- [4] JORRY, H.: *Construction of a European Institutional Model for Managing Operational Cooperation at the EU's External Borders: Is the FRONTEX Agency a decisive step forward?* Challenge Liberty and Security, "Research Paper", March 2007, No 6.
- [5] PIWOWARSKI, J.: *Transdyscyplinarna istota kultury bezpieczeństwa narodowego*. Słupsk : Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, 2016.
- [6] WAWRZUSISZYN, A.: Idea Schengen w obliczu kryzysu migracyjnego. In *Zeszyty Naukowe SGSP*, Nr 57 (1) 2016.
- [7] WAWRZUSISZYN, A.: Transgraniczny charakter współczesnych zagrożeń. In *Międzynarodowe konteksty bezpieczeństwa wewnętrznego państwa*. Piwowarski, J., Bogdalski, P. (ed.). Kraków : Wydawnictwo WSBP i „Apeiron”, 2014.
- [8] WAWRZUSISZYN, A.: Współczesne tendencje i kierunki rozwoju nielegalnej migracji. In *Status cudzoziemca w prawie międzynarodowym. Implikacje w prawie Unii Europejskiej i polskim porządku prawnym*. Łachacz, O., Galster, J. (ed.). Olsztyn : Wydawnictwo UWM w Olsztynie, 2013.
- [9] WAWRZUSISZYN, A.: *Wybrane problemy transgranicznego bezpieczeństwa Polski*. Warszawa : Wydawnictwo Naukowe DIFIN, 2012.

## Legal acts

- [1] Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, signed in Schengen 14 June 1985.

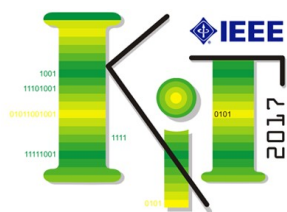
- [2] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders signed in Schengen 19 June 1990.
- [3] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders signed in Schengen 19 June 1990.
- [4] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).
- [5] Council Decision of 26 April 2005 designating the seat of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (2005/358/EC) (Dz. U. 114, 4.5.2005).
- [6] Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence (2002/946/WSiSW).
- [7] Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Dz. U. L 349, 25.11.2004).
- [8] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.
- [9] Decision No 575/2007/EC of the European Parliament and of the Council of 23 May 2007 establishing the European Return Fund for the period 2008 to 2013 as part of the General Programme 'Solidarity and Management of Migration Flows'.
- [10] Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.
- [11] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II).
- [12] Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).
- [13] Regulation (EU) 2016/1625 of the European Parliament and of the Council of 14 September 2016 amending Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency.
- [14] Regulation (EU) 2016/1626 of the European Parliament and of the Council of 14 September 2016 amending Council Regulation (EC) No 768/2005 establishing a Community Fisheries Control Agency.
- [15] Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.
- [16] Regulation (EU) No 514/2014 of the European Parliament and of the Council of 16 April 2014 laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, preventing and combating crime, and crisis management.
- [17] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.

Assoc. Prof. Juliusz PIWOWARSKI, Ph.D.  
University of Public and Individual Security "Apeiron"  
in Krakow  
Faculty of Security and Socio-Legal Studies  
Krupnicza 3/1 st.  
31-123 Krakow  
Poland  
E-mail: science2@apeiron.edu.pl

Andrzej WAWRZUSISZYN, Ph.D.  
University of Warmia and Mazury in Olsztyn  
Faculty of Law and Administration  
ul. M. Oczapowskiego 2  
10-702 Olsztyn  
Poland  
E-mail: andrzej.wawrzusiszyn@uwm.edu

**Assoc. Prof. Juliusz Piwowarski, Ph.D.** - currently (since 2010) serves as the Rector of the University of Public and Individual Security "Apeiron" in Krakow. The founder of Cracow Research Institute for Security & Defence Skills APEIRON (2012) at the University of Public and Individual Security "Apeiron" in Cracow. So far Juliusz Piwowarski is the author of two monographs published abroad, eleven monographs published at Polish publishers and nearly a hundred scientific articles published at Polish and foreign scientific magazines.

**Ph.D. Andrzej Wawrzusiszyn** - Adjunct of the Chair of Security and Public Order of Faculty of Law and Administration at the University of Warmia and Mazury in Olsztyn. Graduated of Higher Officer School of Mechanized Military Forces, University of Maria Curie-Skłodowska and the National Defense University, for many years Polish Army and Border Guard officer on the management and didactic positions. Within the framework of scientific activities specializes in issues of national security, security management, education for security. Member of the Polish Association of Political Science, Defense Knowledge Society and European Association for Security.



## Communication and Information technologies

### 9<sup>th</sup> International Scientific Conference

Hotel GRANIT - Tatranské Zruby

**October 4, 2017 – October 6, 2017**

Presentation of new sophisticated technologies and results of both theoretical as well as applied research in the area of communication and information technologies. The aims of the Conference are professional discussions and plenaries on communication and information technologies and their use in research, training and education, with focus on military applications. Conference Proceedings will be published in the *IEEE Xplore*® Digital Library and indexed in *Scopus*.

Conference Contact:

Address: Armed Forces Academy of General M. R. Štefánik, Department of Informatics,  
Demänová 393, 031 06 Liptovský Mikuláš, Slovak Republic  
Phone: +421 960 423019  
Fax: +421 44 5525639  
E-mail: [kit2017@aos.sk](mailto:kit2017@aos.sk)  
Web: <http://kit2017.aos.sk>

# LOW LEVEL PROFILE SECURITY ANALYSIS IN WIRELESS ENVIRONMENT

Martin OBERT, Marcel HARAKAL

**Abstract:** In relation to Contemporary cybernetic threat analysis [1, 14] we try to predict mobile data traffic tender by extending the CAGR forecasting method (Compound Annual Growth Rate) released from Cisco [2]. By extending the forecasting, we identified equilibrium between infrastructural data and mobile data volume occurs in the year 2026. The conclusion gives us a good reason to concentrate our effort on analysis mobile security with focusing on WIFI (Wireless Fidelity) infrastructure networks protection. Our intent is to provide a detailed elaboration of the widely used WIFI security principles emphasizing their partial weakness based on core algorithms. As the goal of this paperwork, we also provide a limited elaboration of differences among them in order to theoretically figure out the level of their safety.

**Keywords:** mobile data, fixed internet data, access point, wireless security, wireless fidelity, pass phrase, seed, key stream, encryption, decryption, cipher text, pre-shared key, pair-wise transient key, open key authentication, shared key authentication.

## 1 CURRENT SITUATION AND DEVELOPING PREDICTION

In the year 2015, we provided comprehensive research of different kinds of cybernetic threats during the year 2013 [1]. The research has shown us only rare intent to penetrate into wireless security (only 3 attempts have been recognized during the year 2013). The reason of such low incidence should lie in these three aspects:

1. A certified WIFI security is greatly protected system and traffic is so strongly encrypted that it is almost impossible to penetrate it.
2. In time of analysis, plenty of WIFI access points (WIFI - AP) were opened and unsecured so in such case there was no system sensitivity that somebody is using them without authorization.
3. Improper attack identification. An identified attack should not be considered with wireless environment due to multi-classification (for instance Network Injection might be targeted

against fixed infrastructure networks as well as against wireless environment).

In the first two cases we were unable to assess a presence of malicious attempt. The third aspect arose due to attack typology generalization. Hence there is significant assumption of globally unified certified WIFI security in order to avoid of abuse WIFI – APs to execute attacks over them. This is achieved by improving user interfaces of the devices to be simpler in providing secure connection (security connection can be established by simple pressing a respective button on a WIFI-AP).

Our main goal in this article is to evaluate contemporary situation of cyber threats within wireless environment with forecasting vision to the future. Secondly, we will analyze different methods of WIFI securing particularly based on detail analysis of protocol-based theoretical principles. Finally, we conclude with consideration of distinguishes between different securing methods used in the WIFI environment.

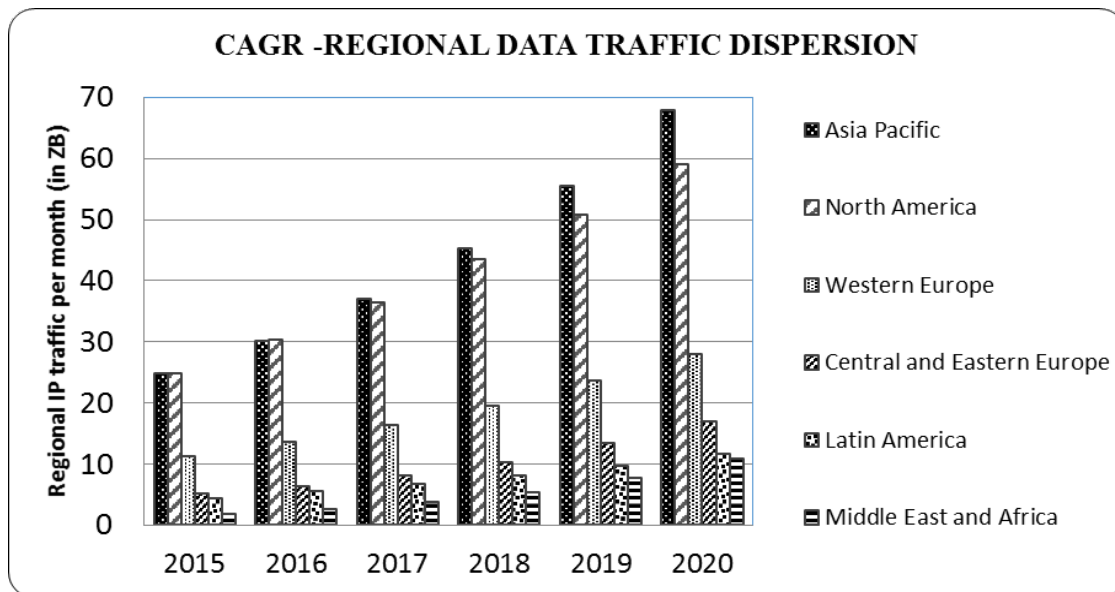
**Table 1** Global IP traffic 2015-2020

IP Traffic, 2015-2020							
	2015	2016	2017	2018	2019	2020	CAGR 2015-2020
<b>By Type (PB per Month)</b>							
Fixed Internet	49,494	60,160	73,300	89,012	108,102	130,758	21 %
Managed IP	19,342	22,378	25,303	28,155	30,750	33,052	11 %
Mobile data	3685	6180	9931	14,934	21,708	30,564	53 %
<b>By Segment (PB per Month)</b>							
Consumer	58,539	72,320	89,306	109,371	133,521	162,209	23 %
Business	13,962	16,399	19,227	22,729	27,040	32,165	18 %
<b>By Geography (PB per Month)</b>							
Asia Pacific	24,827	30,147	36,957	45,357	55,523	67,850	22 %
North America	24,759	30,317	36,526	43,482	50,838	59,088	19 %
Western Europe	11,299	13,631	16,408	19,535	23,536	27,960	20 %
Central and Eastern Europe	5205	6434	8116	10,298	13,375	17,020	27 %
Latin America	4500	5491	6705	8050	9625	11,591	21 %
Middle East and Africa	1930	2698	3822	5380	7663	10,865	41 %
<b>Total (PB per Month)</b>							
Total IP traffic	72,521	88,719	108,533	132,101	160,561	194,374	22 %

Source: [2].

John N. Stewart (Senior Vice President of Cisco security and Trust Organization) reported analyzing for security issues about 3 petabytes of data every

single day [2]. From this amount is more than 100 terabytes of threats. Complete forecasting of data is shown in Table 1.



**Fig. 1** CAGR - Regional data traffic volume forecasting from Table 1 in graphic representation

In the Figure 1 there is graphically shown the global IP traffic spread within regions. As we can see, even in 2015 Asia region and North America were the biggest consumers of the global IP traffic. CAGR forecasts us to continue in that tender within the next couple of the years.

At the present, there is still prevailing of Fixed internet traffic against to Mobile data traffic, as we can see from the table. Therefore, we have used CAGR (CAGR – Compound Annual Growth Rate) from the table to forecast developing in following years bounded by the year 2030. For better imagination, we present the figures graphically (Figure 2) and we can see year 2026 as the year of intersection when mobile traffic will overtake fixed traffic volume and hence we can also estimate respective overtaking in the cyber threats area. Obviously, the tendency is mainly related with rapid growing in the industry. Nowadays, the Industry of 4<sup>th</sup> generation has been introduced and its enormous complexity and high level of mobility necessarily requires robust wireless communication environment. To emphasize that enhancing industry, as core reason of growing demands for wireless communication, could be Tesla factory. Elon Musk, CEO of Tesla factory founded his first factory for pure electric cars producing in Fremont, California. The factory is based on Industry 3<sup>rd</sup> generation in spite of its particular interlacing to industry 4<sup>th</sup> generation. All distributed control system communicates over wired environment.

In such design only paint shop (part of the factory for painting the cars and baking the color) consists of 72 control cabinets where is terminated more than 9000 wires. In order to control technological processes, these cabinets are interconnected by network which is placed in next six network cabinets. When you consider that some of the cables are more than 100 meters long, you can figure out how inefficient such solution is.

Limited by space and distance it was a logical step to introduce wireless communication among industrial processes primary presented in Tesla Gigafactory 1 [13]. The second desirable reason was deploying AIVs (Autonomous Indoor Vehicles) to achieve fully qualified Industry 4<sup>th</sup> standard. The AIVs can autonomously maintain complex logistic issues. However, they need to move so there is necessarily robust wireless data exchanging required.

As we can see, not only forecasting gives us clear evidence of increasing importance of the mobile data communication. As we can also see at the present time, we are unable to extend in critical areas without currently wireless communication introducing.

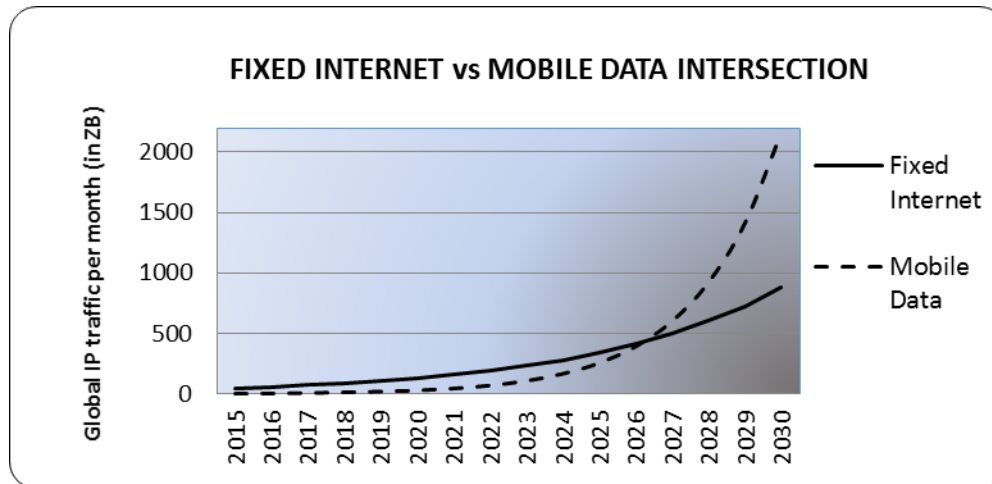


Fig. 2 Global IP traffic intersection forecasting in reference [2]

## 2 WIFI STANDARDS OVERVIEW

In spite of many wireless standards using in different areas, we will focus on WIFI (Wireless Fidelity) standard as the most developed standard which forms security perspective today. Before we start deeper elaboration within WIFI security, we will summarize WIFI standards:

- **802.11:** Very first wireless communication standard adopted in 1997 with raw bandwidth<sup>30</sup> up to 2Mb/s. Uses only WEP (Wired Equivalent Privacy) security implementation.
- **802.11b:** Extends raw bandwidth up to 11Mb/s. Some devices can support WPA/WPA2 after firmware upgrade.
- **802.11a:** Carrier frequency is multiply to 5GHz to avoid interferences with other devices using 2,4 GHz and raw bandwidth is extended to 54Mb/s. WPA/WPA2 is supported after firmware upgrade.
- **802.11g:** Based on carrier frequency 2,4 GHz. Raw bandwidth is up to 54Mb/s. Known as Wi-Fi standard. The standard has been developing at the same time like 802.11i, hence all devices have implemented WPA/WPA2 security in itself.
- **802.11n:** Wireless standard with two independent antennas known as MIMO Wi-Fi (Multiple input Multiple output). Raw bandwidth is up to 600 Mb/s. WPA/WPA2 is obligatorily implemented.
- **802.11ac:** Wireless standard with up to eight independent antennas. Raw bandwidth is 867 Mb/s per antenna and 6,77Gb/s is aggregate capacity by using eight antennas. WPA/WPA2 is obligatorily implemented.
- **802.11i:** Security implementation which supersedes previous WEP (Wireless Equivalent Protection) by WPA/WPA2 (Wi-Fi Protected

Access). Uses 4-way handshake for authentication. Its implementation is available since 2004.

- **802.11k:** It is roaming upgrade implemented in 2007. It provides information to discover the best available AP (Access Point) in wireless environment.
- **802.11r:** It is roaming upgrade implemented in 2008. It is faster than its predecessor by reducing control traffic during transition.
- **802.11v:** The standard giving information about topology and changes within it. It has become as an independent standard in 2011 but it has been implemented from very first wireless networks.
- **802.11e:** Implements set of QoS (Quality of Service). The standard was introduced in 2005. The purpose is to support delay sensitive applications like VoIP (Voice over IP).

As we can see from summarization, 802.11x wireless protocol family consists of many standards to control traffic over wireless environment. In our further elaboration, we are focusing primarily on two auxiliary control mechanisms, WEP and 802.11i (WPA/WPA2) security standard.

## 3 METHODS OF ATTACKS IN WIFI ENVIRONMENT OVERVIEW

In infrastructure wireless environment we recognize two philosophical concerns of an attacker:

1. Penetration into network during authentication and authorization process when special control frames and valuable messages are exchanged over network.
2. Data communication interception in order to recognize ciphering key from certain pattern. For example, when stream substitute cipher is used and you know original language of the message, you can just search for entropy of different letters or words (i.e. entropy of "the" occurrences is

<sup>30</sup> Raw bandwidth means all traffic proceeded over the channel.



close to 0,1 in spite of entropy of “quality” occurrences is close to 0,0001 in English text [3]). Hence, when you identify “pda” string with similar entropy equal to 0,1 you can just shift +4 alphabetic symbols and will get backtrack substitution p->t, d->h and a->e, the original text “the”.

In Ad-hoc networks, security issue is very important because there are fully or particularly distributed network control principles. On the other hand, there is typically missing centralized point for administration and policy propagation. Most of the Ad-hoc commercial networks are P2P (Peer to Peer) networks based on reputation policy hence there is different nature of attacks. An attacker mostly pretends a host with good reputation or tries to decimate the reputation of the others to gain enhance privileges [4].

Following is the summary of diverse security threats over wireless environment:

- **Data interception.** This threat is based on communication eavesdropping by an intruder on the same channel.
- **DoS (Denial of Service).** This kind of threat is coming from nature of wireless communication over common air medium. It gives an easy opportunity to get access to anybody to physical medium from data transmitting. In many cases the threat can be assessed as accidental but not intentional.
- **Rogue AP.** Is based on intentional or unintentional additive connection of a new AP into corporate wired network [5]. By its attaching to the network it creates unpredictable avenue of approach for potential intruders. In purely wired networks are usually not implemented wireless IPS (Intrusion Prevention Systems) hence such rogue AP can be very effective and harmful.
- **Misconfigured APs.** This can be a serious security issue especially when there is no central management implemented within a corporation. There is praxis for a longer time of using central security management policies like TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) which provide additive security value by its complexity known as “triple A” (AAA – Authentication, Authorization, Accounting).
- **Evil Twin APs.** It is very effective attack based on SSID (Service Set Identifier) knowledge. If attacker discovers SSID he can configure so-called Evil Twin AP (ET-AP), advertise its SSID and wait for a victim. Once, someone is connected to the ET-AP, a Man in the Middle attack can be launch in very efficient manner. Score of this kind of attack is very high and it is depended on proper original AP’s configuration as well as on a set up authentication method.
- **Misbehaving Clients.** This security issue is very closely related to correct hardware configurations and setting up group policies. Especially authorization from AAA policies can grant to a user some rights beyond his consciousness. Second aspect is social dimension, a user could have intent to penetrate into corporate network and hence healthy configured HW should detect such attempt over IPS or IDS (Intrusion Detection System).
- **Endpoint attacks.** Philosophy of the attack is based on exploitation of a user’s device usually by slipping some code consists of Trojan Horse. After installation into computer it will hand over some resources by suitable modifying privileges. Success of this kind of threat is also closely related to user’s authorization to control mainly local resources.
- **Ad Hoc and Software APs.** As is mentioned before, we recognize two cardinal types of wireless network. One is infrastructural network and opposite is challenging Ad-hoc network. Main reason of using infrastructural networks is centralized management which is an vital element for each enterprise corporation to keep it within controllable boundaries. Once, there is possibility to integrate Ad-hoc connection into infrastructural corporate network any security policy is becoming inefficient. In the past, when Ad-hoc access could be implemented only by adding or reconfiguring physical devices, the risk had not been so serious. But since Ad-hoc nodes can be emulated by software (integrally implemented since MS Windows 7) security risk has been dramatically increased.

In some sources there are mentioned other attacks (i.e. wireless phishing) what we do not suppose to be related with wireless environment. These attacks are generally derived from common principles and they are not related with wireless platforms.

#### 4 SUBSTANTIAL WEP AND WPA PRINCIPLES USING IN ATTACK

In the chapter we will present some theoretical principles of securing the wireless environment. To do this we have two direct outlooks (local wireless security and centralized wireless security) and we can also consider indirect security by defining rules and policies at application level (it means that user can connect to the network but his resources are limited in accordance with group policies).

On the matter of this article, we will analyze only direct local wireless security based on WEP, WPA and WPA2 elementary security principles.

WEP (Wired Equivalent Privacy) is the very first encryption method which was introduced as a part of 802.11 in 1997. As from the abbreviation implies, the aim was to provide same security level like used

to be in wired infrastructural networks in that time. The method uses symmetrical RC4 stream cipher with fixed key (k) and variable initialization vector (IV), what is denoted like RC4(k, IV) and represented by key stream (KS). IV has fixed size 24 bits and is occupying first 24 bits of the key stream. If key stream is 64 bits, 40 bits are dedicated to the fix key in case of 128-key stream there is place for 104 bits of the key following by IV. What is very important to know, that for each new packet there is generated new pseudorandom IV. Once, there is KS generated we use “exclusive or” (XOR) operation between KS and plain text as is shown in Figure 3. As we can see from the figure, transmitted message consists from open IV and ciphered text including CRC-32 generated for plain text before cipher is proceeded. At the receiver side, there is reverse procedure to decode the message back to the plain text. As is shown in Figure 4, cipher message is involved to XOR operation with the same key stream in order to get back plain text and CRC-32 which is denoted like ICV (integrity check value). When a plain text is obtained, new ICV is calculated from it and compare with ICV calculated by transmitter itself. This ICV comparison ensures integrity of the original plain text with decrypted one. Once there is no match, all frames are discarded.

General WEP vulnerabilities are:

1. Symmetric encryption. This causes transmitting secure key footprint to recipient over the network. As well as the information is at the transmitting point encrypted it is decrypted at the receiving point by the same key. No other private key is used during the transmission.
2. Massive key sharing. All nodes in one WEP-secured domain use and operate with the same 4 keys once derivate from the password phrase. This offers a huge amount of traffic for frequency analysis and gives high probability of its success.
3. Ciphered text is concealed only due to IV partition changing in each new packet. But IV length offers only  $2^{24}$  iterations so statistical repetition is achieved in approx. 5-7 hours on a busy network [8]. The second disadvantage of IV is its regular repetition over all values. Some of the values are so-called weak values (the value which has only a minor influence to final cipher text modification) and allow highlighting “footprints” of the original key in the ciphered text.
4. All the security is ensured by only one cipher engine (PRNG – Pseudo Random Number Generator algorithm, its generalized form is known as LCG – Linear Congruential Generator). LCG is very liable on frequency analysis, because of remapping entropy in produced stream cipher due to lack of iterating.
5. If there is not enough traffic for frequency analysis, we can focus on authentication procedure. However, the keys can be only manually distributed there is very limited space for success. The success is depended on concrete WEP implementation by a vendor of the device. In principle it is based on open key authentication (see Figure 7), when attacker is able to connect to a device even without key knowledge in order to try to force re-initialization of device (i.e. access point). Once the device is rebooted, depending on concrete WEP HW implementation, it is possible that the key values can be directly sent as a hex data [9].

Most of the WEP hacking techniques are based on:

1. **Passive attacks.** Is based on silent listening of the encrypted traffic and statistical analysis.
2. **Rogue AP attack.** In principle is similar to passive attacks, but it provides us more powerful resource to monitor network traffic. It can also easily turn to Active injection attack mode.
3. **Active injection attack.** Intruder tries to inject deceitful traffic in order to receive certain reaction of AP which can directly or indirectly reveal certain information.
4. **Dictionary building attack [8].** This attack is based on listening of the traffic and capturing certain information valuable for creating dictionary base for future active attacks. It is rarely used in WEP penetration and it is more suitable for asymmetric encryption methods where only systematic guessing could give us a positive result.

That was brief theory preparation and now we can focus on detail execution of typical attacks:

Brute force attack developed by Tim Newsham known as Newsham 21 bit WEP attack [8]. The attack is based on knowledge of vulnerability of certain wireless products (Linksys, Netgear, Belkin, D-Link) where efficiency of the secret key is decreased from original 40 bits to 21 bits. The principle of the reduction is based on several things:

1. Input password is a string. To produce a seed for PRNG we need to convert this string into numbers by using ASCII mapping. But ASCII mapping is mapping only double word value at one time, it means only four characters from original string. We need to know, that final seed must keep exact length to be valid as a seed for PRNG. The length is depended on concrete LCG, but in case of PRNG it is typically double word again (4 bytes) because of we are able to execute one output generation per one cycle with this size. If we put just first four characters from the string into PRNG, the remaining characters of the password would be just a rubbish. Hence,

we need somehow to scramble input password string into 4-bytes seed. We do it by using XOR operation between mapped double words like is shown in figure 5. As we can observe, we put only 4 bytes seed into PRNG created from original password phrase. Hence, the theoretical iteration cycle is  $2^{32}$  but this can be even reduced. The second issue what we can observe is own mapping to ASCII bytes. As we know ASCII consists only from 127 characters so we can surely predict that the highest bit of each

byte will be still zero. But we can observe also other important thing, we lost the original password string after XOR operation proceeding. In such situation we assume applying XOR operation as a one-way function, so we could never find out original password string from the seed or ciphered text itself. Moreover, the following process through PRNG will also scramble all bits over all positions, hence there is no more reliable rule of high zero-bits.

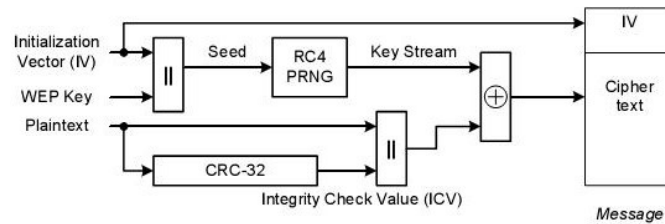


Fig. 3 WEP encryption process – Block diagram

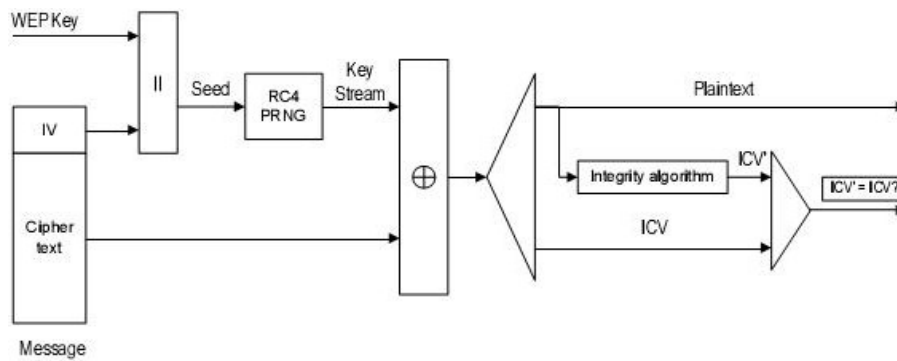


Fig. 4 WEP decryption process – Block diagram

T e s t i t																															
32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
2 <sup>31</sup>	2 <sup>30</sup>	2 <sup>29</sup>	2 <sup>28</sup>	2 <sup>27</sup>	2 <sup>26</sup>	2 <sup>25</sup>	2 <sup>24</sup>	2 <sup>23</sup>	2 <sup>22</sup>	2 <sup>21</sup>	2 <sup>20</sup>	2 <sup>19</sup>	2 <sup>18</sup>	2 <sup>17</sup>	2 <sup>16</sup>	2 <sup>15</sup>	2 <sup>14</sup>	2 <sup>13</sup>	2 <sup>12</sup>	2 <sup>11</sup>	2 <sup>10</sup>	2 <sup>9</sup>	2 <sup>8</sup>	2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	2 <sup>4</sup>	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
XOR	0	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	0	1	0	0	0
	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0
SEED	0	1	0	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1	0	0	0
SEED	1410074484 <sub>Dec</sub>																														

Fig. 5 Seed generation process from password “Test it”

- Once, we have had seed we need to understand own PRNG. PRNG is based on general LCG so for better understanding we use general LCG with simplified seed as well as other simplifications on behalf of better imagination. The LCG generator is defined by the recurrence relation:

$$I_{n+1} = (a * I_n + c) \bmod m$$

$I_{n+1}$  - Next iteration (output)

$I_n$  - Last iteration

$I_0$  - Seed (starting value)

$c$  - Incremental constant

$a$  - Multiplication

$m$  - Base for modulus

We can observe, that equation outputs are limited by “modulo m” It means that cycle period is less

than or equal to  $m$ . For a better understanding, we consider only twelve possible values from 1 to 12. We set up following initial values:  $m = 12$ ,  $c = 0$ ,  $a = 2$ ,  $I_0 = 4$ .

Modulus 12 limits our outputs to have maximum twelve different values. We can see decimal representation of the values on Figure 6. We start at number 4, because of  $I_0$ . To generate next number by using above mentioned principle, we will get number 8  $((2*4+0) \bmod 12)$ . When we continue with next number we will get 4 again  $((2*8+0) \bmod 12)$ . And all generation is repeated again and again. Hence, we can see very limited liability of the generator for randomness purposes. In spite of  $a$ ,  $c$  is firmly defined by vendor, we could not be sure that computed seed will not be much shorter like supposed period. Such seed (respectively password) is called "weak seed".

Therefore, the PRNG parameters must be somewhat improved to decrease probability of "weak seed" occurrence.

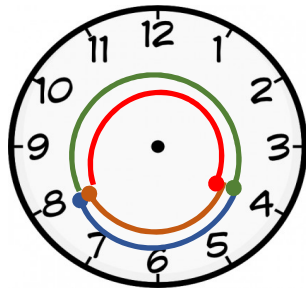


Fig. 6 LCG process principle

PRNG used in WEP RC4 has following parameters:  $a = 0x343FFD_H$ ,  $c = 0x269EC3_H$ ,  $m = 2^{32}$ .

As is shown on Figure 5, the generator works with double word (32 bits) seed, hence also modulo should be logically  $2^{32}$ .

Keeping LCG principle, PRNG can be denoted like:

$$I_{n+1} = (I_n * 0x343FFD_H + 0x269EC3_H) \bmod 2^{32}$$

This will generate 32 bits outputs of pseudo-random numbers with overall cycle period  $2^{32}$ . WEP 64 uses 24 bits for IV and 40 bits for own secret shared key. But it has four different keys. To make things more complicated, generated values don't represent the keys directly. The keys are composed from every third byte of generated double word. PRNG generates 40 iterations together and to compose one key we need 5 bytes (40 bits). It means we need  $5*4 = 20$  bytes to generate 4 keys. We can observe that by selecting 3<sup>rd</sup> byte from four, we reduce cycle period from  $2^{32}$  to  $2^{24}$ . Mr. Newsham denotes [9] the next reduction is caused by zero bits occurrence at the highest position of each byte of the composed keys. But this is only true up to the initial

seed is generated. Once we start pseudo-random generation, output bits at each position are just results of mathematical operation  $*$ ,  $+$  and modulus. Moreover, if we transcript " $a$ " and " $c$ " into binary form we can directly observe "ones" at high position of certain bytes.

$$\begin{aligned} a &= 0x343FFD_H \\ &= (00000000 \ 00110100 \ 00111111 \ 11111101)_B \\ c &= 0x269EC3_H \\ &= (00000000 \ 00100110 \ 10011110 \ 11000011)_B \end{aligned}$$

Therefore, we cannot agree with this reduction from 23 valid bits to 21 valid bits because of the highest bit zeros occurrence is only up to randomness.

For the sake of clarity, we need to understand some more details about key handling and RC4 using. Very first is authentication itself. To connect to network, we recognize two ways:

1. Open key authentication. In that case, potential client (STA) sends "Authentication Request" to AP. AP sends "Authentication Response" following by the same procedure for association device with AP as you can see in Figure 7. STA doesn't know correct password because it is not challenging during authentication process.
2. In spite of Shared key authentication, where after authentication request from STA AP sends clear challenge text back to the STA to be encrypted by known password (as shown by Figure 8). STA encrypts the text and sends it back to the AP in order to prove its authorization. The main weakness in this point is installing a rouge AP against legal STA. Rouge AP doesn't know password or keys, but it knows authentication procedure as well as open challenging text sent to STA for encrypting. Once it receives encrypted text it can get key stream by applying XOR operation between these two messages.
3. Shared key authentication.

One of the famous WEP breaking is Fluhrer, Mantin and Shamir (FMS) attack. The attack uses weaknesses in key scheduling algorithm (KSA) and Pseudo-random generator algorithm (PRGA).

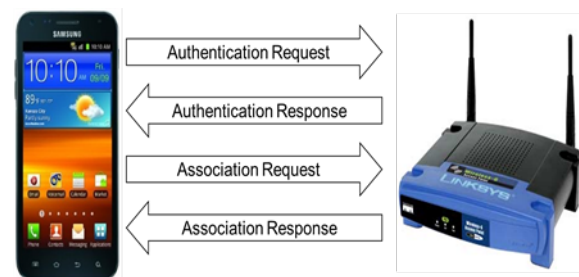


Fig. 7 WEP – Open key authentication

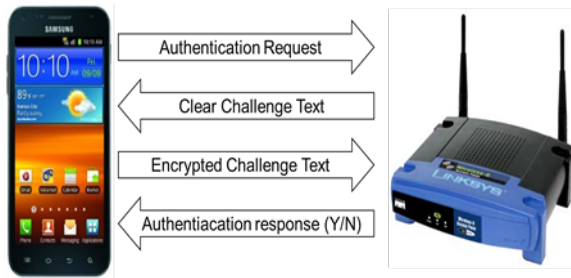


Fig. 8 WEP – Shared key authentication

Key Scheduling Algorithm:

Initialization:

For  $i = 0 \dots N - 1$   
 $S[i] = i \cdot j = 0$

Scrambling:

For  $i = 0 \dots N - 1$   
 $j = j + S[i] + K[i \bmod \text{key\_length}]$   
 $\text{Swap}(S[i], S[j])$

Pseudo Random Generator Algorithm:

Initialization:

$i = 0$   
 $j = 0$

Generation loop:

$i = i + 1$   
 $j = j + S[i]$   
 $\text{Swap}(S[i], S[j])$   
 $\text{Output } z = S[S[i] + S[j]]$

Both algorithms are working with two arrays  $S[i]$  and  $S[j]$ . We need to mention that both of the arrays are byte size. The scrambling method relies on swapping these two arrays after each permutation. Key stream for ciphering original plain text is generated directly by these two algorithms (KSA and PRGA). In the first step, a pseudorandom seed is generated by KSA. As we can see in each cycle,  $j$  is incremented by  $S[i]$  and modulus of  $K[i]$ . We need to mention, that first 3 bytes of the  $K[i]$  are prepended by initialization vector (IV) which is generated in cycles from  $2^0$  to  $2^{24}$ . FMS attack also supposes one important weakness of the IV periodic generation that only 3<sup>rd</sup> byte is reaching  $2^{24}$  permutations per repeating the cycle. But 1<sup>st</sup> byte is repeating every  $2^8$  permutations and knowing this information, attack concerning just directly to it. As is mentioned above, both of arrays are byte type and both of algorithms are working with bytes. Therefore, we can just focus on the 1<sup>st</sup> byte of the IV, respectively to its weak value. Because of IV is transport in opened form, we can easily identify the value of the 1<sup>st</sup> byte by which is the packet also encoded. To summarize it, we know IV values, we have ciphered text and we know what we are looking for.

Finally, we will collaborate about ICV (Integrity Check Value) weaknesses. ICV is calculated from plain text and CRC32, meanwhile CRC32 is

calculated from plain text as well. For all computing, there is used simple pattern based on XOR operation between bits. No key or its part is combined during CRC and consequently ICV generating. Due to only linear dependence and independence on WEP key there is possibility to change (flip) bits without being recognized by WEP encryption mechanism.

WPA (Wi-Fi Protected Access) has been introduced in 2003 as a response to serious weaknesses of WEP protection. It exists in two different flavors, one uses TKIP (Temporal Key Integrity Protocol) which is considered to provide robust security and hence it is intended to be used at enterprise environment. The other one uses PSK (Pre-Shared Key) what is considered as less secure hence it is likely affiliated with personal use. In spite of key management improving, WPA still uses stream cipher but with robust key (typically 256 bits) what creates NP (Not Possible) time depended solving problem by using the same techniques which could be applied in WEP security. Reason why WPA uses the same core functionalities is that it has been released as immediate reaction to WEP breaks and for WPA using has been considered the same hardware, because the intent was to implement WPA backward by upgrading firmware on existing devices.

On the other hand, WPA has these two major innovations:

1. Data encryption is proceeding over TKIP respectively PSK. Each packet is encrypted by new hash from primary key called Temporal key. Moreover, integrity-checking feature guarantees that no data modification occurred during transferring.
2. Different keys are used for different data.
3. There is used EAP (Extensible Authentication Protocol) for host authentication. It is based on public-key encryption system.

Let's focus on WPA-PSK in some detail. PSK algorithm not only modify shared key per packet, but also has complex key management consisting of:

1. PSK or PMK (Pre-shared key or Pair-wise Master Key). This key is generated from password phrase. Actually, this key is not used for data encrypting, it is only a seed for PTK.
2. PTK (Pair-wise Transient Key). This key is derivate from PSK and is used to encrypt data in respective packet.
3. GTK (Group Temporal Key). This key is generated in similar ways like PTK, but its purpose is to encrypt only broadcast and multicast traffic. Idea is coming from previous key capturing techniques, when a broadcast domain is intentionally provoked to transmit some broadcast or multicast in order to reach a key by rouge access point. Therefore, there is also improving in using different key pattern like is used for regular traffic. Hence,



even if a broadcast is successfully captured by attacker, there is no PTK contented in it.

Following function is used to generate PSK from password phrase:

$$\text{PSK} = \text{PBKDF2}(\text{Pass\_Phrase}, \text{SSID}, \text{SSID\_length}, 4096, 256)$$

Many variables and constants in the function appeals as necessity of scrutiny discussion about them.

- *PBKDF2* – is Password-Based Key Derivation Function 2 [10].
- *Pass\_Phrase* – input string of characters sized from 8 to 63 characters.
- *SSID* – is the name of broadcast domain unified for all connected devices.
- *SSID\_length* – is “salt” (auxiliary information). The salt is appended in the first iteration to the end of the pass phrase.
- 4096 – is the number of desired iterations. Original number was 1000, but it has been considered as the computing power increases as the number will increase too.
- 256 – is the length of output PSK.

If we look at the function, we consider that is much more sophisticated than PRNG used in WEP protection. Very first feature is an ability to grow, and literally. It is ensured by two last constants, which are defined directly in firmware applied to HW, but it does not mean that in faster HW the constants could not be properly increased. It is really timeless solution, which was absolutely missing in the WEP and therefore the WEP was breached very soon, because its security performance has been almost the same in spite of rapid increasing of computational power of the computers following the Moore’s law. Hence the performance of personal computers achieved a level which allows doing complex set of iterations to discover key phrase in considerable time. The lesson learned has been taken from this disability to follow increasing hardware performance at cryptographic level by modifying critical algorithm parameters. To follow the increasing performance power, the iteration parameter is the most important. When the algorithm was introduced, in 2000, only 1000 iterations were considered to be satisfying level for enough robust encryption. It was also depended on RISC (Reduced Instruction Set Computer) used in related devices, which had not enough power to calculate more iterations in real time due to significant delaying in transmitting and consequently receiving packets. This could have secondary harmful impact to other running services mainly depending on high QoS (Quality of Services) index like real time video streaming, voice conference, etc. In 2005 a Kerberos standard recommended as minimal number of iterations to be 4096. It is just a recommendation

and we can see some other vendors using much greater number of iterations in their systems (i.e. IOS 4.0 uses 10000, LastPass uses 5000 iterations for client-side hashing and 100000 iterations for server-side hashing). Finally, we can see that such modification allowing implementation makes the security issue timeless and able to react on increasing computing power.

Pass Phrase string has been also enhanced from minimal 5 characters to minimal 8 characters.

Output PSK minimal size has been improving too from 64 resp. 128 bits to 256 bits in minimal configuration requirements.

Except multi-dimensional growing features, there is also other innovation proposed by Morris and Thompson [12]. It is about salting password phrase by other data in order to produce heterogeneous key. As we can see in PSK function, there are two salts (SSID and SSID length) which are scrambled with password phrase to produce a unique PSK. The salt must be chosen very carefully, to be reachable for all participants of the network. SSID is very suitable, because all participants, even those which are just connecting, know the value of SSID. Hence all participants should get equal PSKs.

As we noticed in WEP analysis, second very important issue is security of authentication process. It is process during which a new device is trying to connect to the network and hence the process where generally sensitive data can be propagated over the network what gives good opportunity for applying certain hacking techniques. In WPA case there is authentication process reinitialized always when communication occurs to be a new PTK generated. Let’s analyze the WPA authentication in detail. The authentication, probing and association process is figured out in Figure 9.

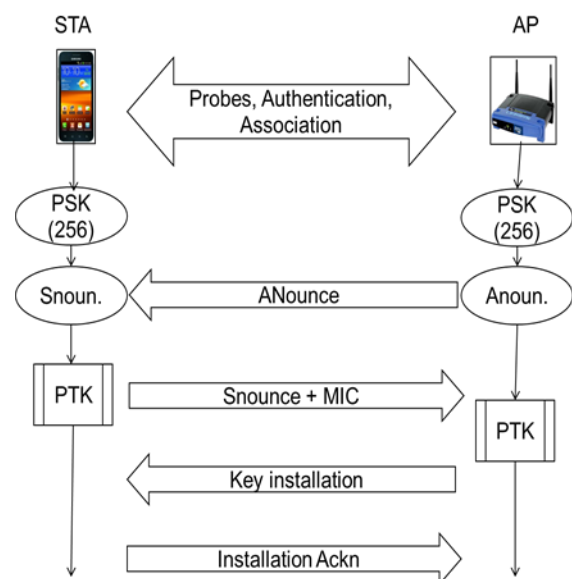


Fig. 9 WPA 4-way handshake

As we can see from the figure any communication between STA (Station) and AP (Access Point) is reinitialized by generating a new PTK. In the first step, Probes, Authentication or Association beacon is sent from AP or STA. This signal tells to opposite entity that 4-ways handshake has been just started up. In the second step, both of entities check or generate PSKs by using Password-Based Key Derivation Function 2. After the synchronous generation of PSK, both entities have the same 256 bits PSKs. In the third step, AP sends Anounce packet to STA. It is pseudo-randomly generated number and is sent in opened text without any encryption. In the same time, STA generates its pseudo-random number, Snounce. Now STA is having both Anounce and Snounce pseudo-random numbers. So STA is ready to generate PTK (Pairwise Transient Key). Then STA is sending to AP its Snounce with MIC (Message integrity check). MIC is compiling hash from the sending frame by using newly generated PTK. In that step is very important to realize that PTK is never sending over the network. When AP receives the frame with Snounce and MIC, it can generate its own PTK by using PSK, Anounce and Snounce. In the next step, after successfully verifying that PTKs are the same, AP sends hash of the message allows installing PTK valid for the session. STA generates its own hash from the preformatted message and compare it with received hash. Once the hashes are matched, STA can acknowledge it by hashed message again. Hence, we can see that all communication is strictly encrypted by one way function what is considered to be the generated hash. The communication can be inferred only indirectly from number of packets, or so on.

But what is more important in PTK theory is a unique PTK for each STA-AP session. Therefore, if an intruder somehow breaks into one session by discovering its PTK (it could be caused by some weak point of pseudo-random generator) it is not valid for other broadcasted sessions over the network. And this improving disqualifies many of attacks which were possible and easy executed over the WEP protected network.

Therefore, the attack's diversity in WPA-based security is reduced dramatically. One of the most successful attacks is described by algorithm shown in Figure 10.

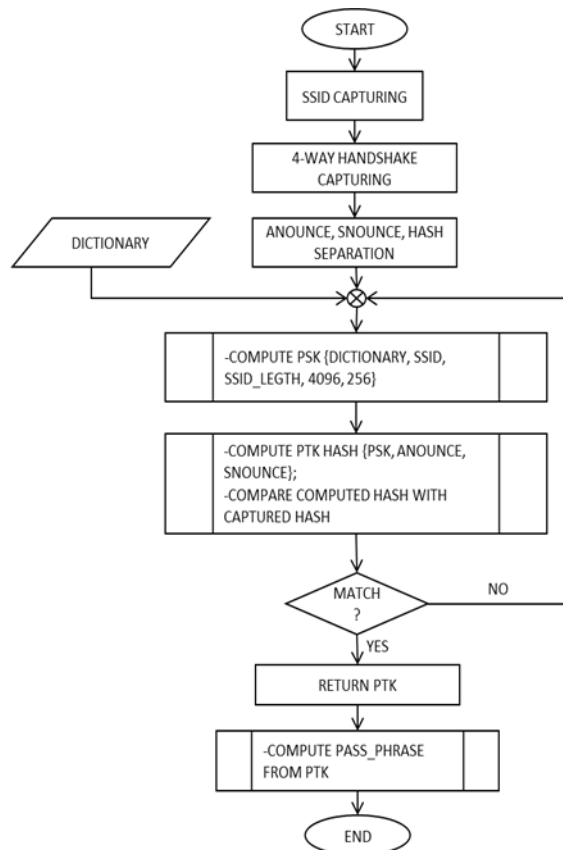
As we can see dictionary attack is fully depended on qualities of dictionary. Firstly, we need to capture a 4-way handshake packets proceeding between STA and AP. From the captured packets, we can directly extract Anounce and Snounce, because these are exchanging in opened form as a plain text. We know, that we need three ingredients to construct a PTK (PSK, Anounce, Snounce). PSK is still missing and we can forget on it, because it is never sent over network, even its footprint (i.e. its hash). But what has been also captured is hash of PTK

included in MIC. Own dictionary attack is Brute-Force type with using dictionary word base for faster passing. Dictionary word base is a record consists of numerous typical password phrases. The record is typically built up from different successful attacks of real user-accounts over the world. Last time social engineering has proofed us certain patterns in creating passwords by real users. It means, that there is no valid entropy among passwords based on statistic approach, but there have been identified certain groups of people with similar patterns in password creating (i.e. his\_name123, his\_name312, his\_name123!). This knowledge can not only reduce the size of dictionary, but also can calculate real entropy and the order index according it.

Own attack algorithm is not complicated at all. Firstly, we need to recognize SSID of the network which we want to penetrate. Prior to attack, we also need to capture at least one full record consists of 4-way handshake procedure. We can extract Anounce, Snounce and hash information directly from the captured record because it must be sent over the network during authentication process. Anounce and Snounce is the key information either for WPA process either for our attack. First procedure in the algorithm computes a PSK from Pass\_Phrase and SSID. PSK length is 256 bits and iteration deep is 4096. To complete a PTK hash we need basically three ingredients (PSK, Anounce, Snounce). As we can see, two of them we recorded at start (Anounce, Snounce). However the key is the first parameter (PSK) it must be computed per each iteration by using dictionary input. The second procedure is simple, we have computed PSK in previous step, we put PSK into has generator, compute a hash from "PSK, Anounce, Snounce" and compare the hash extracted from the real packet at start. Once there is a match, the computed hash is equal to captured one, we can be sure that the hash has been computed from Pass\_Phrase which is used by legal devices for authentication. When we obtain correct Pass\_Phrase we can use it to authenticate inside the network but there could be other techniques which can revealed our illegal activity. But those are out of range of this assumption.

From computing complexity point of view, to computed one process with using a dictionary is much more time consuming in comparison with WEP, because of 4096 iteration deep and 256 bits PSK computes per iteration. However in contrary with this computational difficulty the rest of the algorithm requires significantly less computational power. Therefore there are often available cloud resources on internet for creating "pre-computed dictionaries", where are couples of Pass\_phrases and respective PSKs to them. There is necessary just to send concrete SSID, iteration deep and length of PSK like inputs parameters to a computational cloud and it will calculate usually during idle time respective PSK to each Pass\_Phrase in the

dictionary. It can be used as a paid service for ethical hacking penetration testing, where we are verifying interval of password phrase changing against to its guessing possibility during its valid period. In such case there is very important issue “attacking performance” which requires using ultimate resources what the computing clouds stand for.



**Fig. 10** WPA/WPA2 dictionary attack

In such type of dictionary, the local algorithm is reduced only to compute a PTK from each pre-computed PSK and compare the hash with the captured one. Cloud computing can dramatically reduce computational time therefore for relevant penetration testing it is necessary to consider it too.

## 5 COMPARISON BETWEEN WEP AND WPA COMPUTATIONAL COMPLEXITY

To be Able to exactly evaluate differences between WEP and WPA attack resistance, we need to introduce unique preconditions:

1. Using the same hacking method.
2. Using the same password phrase with the same length and average entropy.
3. Using stream ciphering in both of the cases.
4. Considering all recognized weakness in both algorithms.
5. Considering the weakest version of the method of encryption.

Ad1 To see ultimate differences between the algorithms we assume full range dictionary attack. We conclude to use it also for simplifying the following analysis. When we used dictionary attack with real passphrase database, the ratio between computational complexity would be different because of passphrase XORing in the WEP could modify its entropy dramatically.

Ad2 Once we have assumed full range attack the second point is no more relevant. The entropy is considered to be maximal hence all iterations must be proceeded over the algorithm.

Ad3 The weakness of the WEP algorithm is in its PRNG cycles reduction from  $2^{32}$  to  $2^{24}$ . In case of WPA there is not known such principal elimination.

Ad4 The weakest version of the method of encryption is meant to consider very first release but not an enhanced one. Basically, to use comparable inputs, we should consider very first or very last releases. We cannot make true comparison when one input is very first release (i.e. WEP\_64) and against it other input is final release reinforced by huge know how over the life cycle (i.e. WPA2 with 512 bit key and over 10000 iterations).

When we look at the WEP encryption process, we map a 4 bytes source in range from 00:00:00:00H to 7F:7F:7F:7FH. Hence we have  $2^{28}$  combinations at source. Any of the iteration can be just valid input. Now we consider just one input as a seed for PRN generator. To generate four 40bits keys, we need to generate  $40 \times 32$  bits values what represents 40 generations per one tested iteration. However, on the other hand, for breaching WEP encryption we do not need to know input seed (XORed password phrase) because keys knowledge will be enough. As is describe above, the keys are constructed from 3<sup>rd</sup> generated bytes, so repetition period is  $2^{24}$ . There are four different keys which must be discovered to get ultimate results. But we have to consider that the length of the key is only 64 bits, what is quarter wide against the weakest key in WPA, due to we can divide the computing power by 4 what results into one cycle per iteration. But there is another aspect of the key; it is Initialization vector (IV). IV has 24 bits size what multiplies each key testing by  $2^{24}$ . Hence the final computational difficulty is  $2^{24} + 40$  what is approximately  $2^{24}$  computational complexity for testing only one possible input. When we summarize all together we are getting final computational complexity  $2^{24} \times 2^{24} = 2^{48}$  to guess any message with 100 % probability. For better imagination in figure 11 is data flow algorithm describing the process.



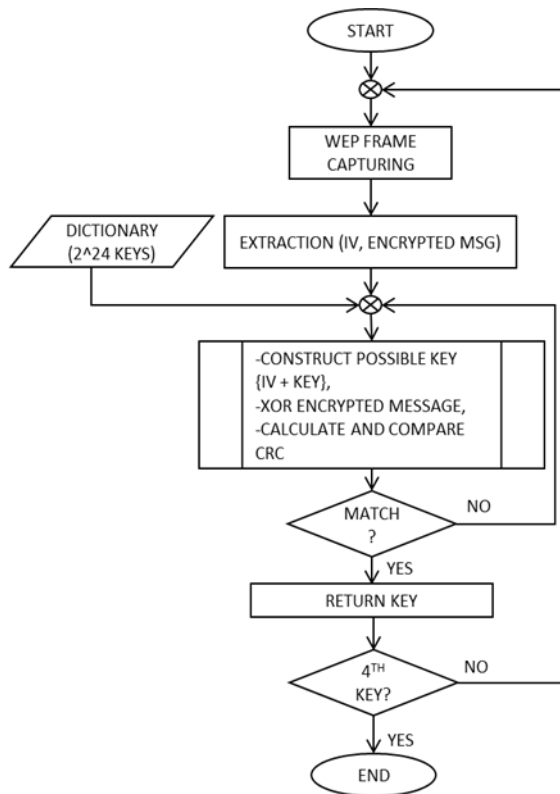


Fig. 11 WEP key dictionary attack

In case of WPA dictionary we should also consider 4 characters password string. However we are technically limited to put at least 8 characters, we have to make following calculations with 8 characters as the weakest possible password phrase. When we look at the algorithm, we need to compute  $2^{12}$  iterations per each input combination to get PSK. Consequently we construct respective PTK from PSK, Anounce and Snounce and compare captured and computed hashes.

However, minimal word input is 8 characters, considering ultimate entropy we need to proceed  $2^{56}$  combinations on input. As we mentioned, we need to calculate additional  $2^{12}$  iterations per each combination hence overall computational complexity is  $2^{68}$  to guess passphrase with 100 % probability.

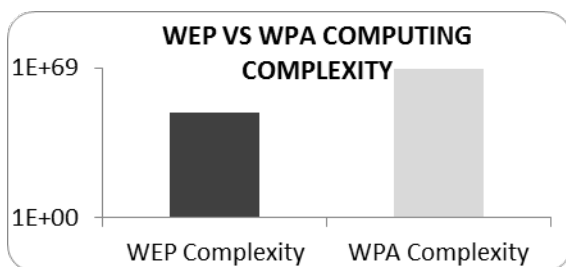


Fig. 12 WEP vs WPA computing complexity

If we compare overall computational complexity in WEP cracking ( $2^{48}$ ) with overall computational complexity in WPA cracking ( $2^{68}$ ) we can see that WPA computational complexity is  $2^{20}$  (1048576) times greater than WEP. This conclusion is only valid when we consider full range dictionary attack however WEP can be also broken with other techniques easily. For better imagination of the mentioned calculations, we can see the results graphically presented in Figure 12. The results are recalculated into  $\log_{10}$  scale.

## 6 CONCLUSION

During the research, we focused on typical WIFI protections in infrastructure networks. In each one, we tried to identify weaknesses and how they can be practically abused by malicious people. We recognized significant improvement from WEP protection level to WPA protection level. In contrary of very poor and easy to break WEP protection, WPA security is possible to tune up in such manner which doesn't allow breaching it at low-level profile resource control. We would like to emphasize that we elaborated only with direct principles of security breaking. However there are numerous other ways of breaching the security over the WIFI networks based on indirect (hidden) importing a malicious code inside a corporate network which unrevealed scanning and sending different sensitive data outside from the network. Today, there is highly developed "ethical hacking safety and security acceptance testing process" so it is more probably that sensitive information will be revealed by indirect way where the user's malicious behave is very often used for penetration to the network. Despite out of our concern, we also identified highly developing industrial segment which nowadays follows Industry 4.0 standard as extremely vulnerable over its heterogeneous network environment.

## References

- [1] OBERT, M., HARAKAE, M.: *Contemporary Cybernetic Threats Analysis*. Liptovský Mikuláš : Armed Forces Academy of General Milan Rastislav Štefánik, Science & Military, No 1, Volume 10, 2015.
- [2] STEWARD, N. J.: *Cybersecurity Now and In the Future – Our Shared Responsibility*. CISCO, 2016. Available at [http://blogs.cisco.com/security/cybersecurity-now-and-in-the-future-our-shared-responsibility?\\_ga=1.215314975.941978938.1475752258](http://blogs.cisco.com/security/cybersecurity-now-and-in-the-future-our-shared-responsibility?_ga=1.215314975.941978938.1475752258).
- [3] SHANNON, C. E.: *Prediction and Entropy of Printed English*. The Bell System Technical Journal, January, 1951.
- [4] KWONG, Y., KWOK, R.: *Peer to Peer Computing: Applications, Architecture, Protocols and Challenges*. CRC Press, 2011.

- [5] All you want to know about rouge APs. Available at: <http://www.rogueap.com>.
- [6] MAHAPATRA, A.: *How does WEP work*. North Caroline State University, 2015. Available at: <https://www.quora.com/How-does-WEP-work>.
- [7] ZHANG, Y., ZHENG, J., MA, M.: *Handbook of Research on Wireless Security*. Information Science Reference, 2008.
- [8] BEAVER, K., DAVIS, T. P.: *Hacking Wireless Networks for Dummies*. Wiley Publishing, Inc., 2005.
- [9] NEWSHAM, T.: *Applying known techniques to WEP Keys*. @STAKE, Inc., 2001. Available at: <http://www.thenewsh.com/~newsham/wlan/>.
- [10] KALISKI, B.: *Password-Based Cryptography Specification Version 2.0*. RSA Laboratories, September, 2000.
- [11] ZHU, L., JAGANATHAN, K., HARTMAN, S.: *RFC 4121 - The Kerberos version 5*. July, 2005. Available at: <https://tools.ietf.org/html/rfc4121>.
- [12] MORRIS, R., THOMPSON, K.: Password security: A case history. In *Communications of the ACM*, 22(11): 594-597, November 1979.
- [13] LAMBERT, F.: Tesla Gigafactory: a look at the robots and 'machine building the machine' at the battery factory, 31<sup>st</sup> July, 2016. Available at: <https://electrek.co/2016/07/31/tesla-gigafactory-robots-machines-battery-factory/>.
- [14] HROMADA, M., HRUZA, P., KADERKA, J., LUŇÁČEK, M., NEČAS, M., PTÁČEK, B., SKORUŠA, L., SLOŽIL, R.: *Kybernetická bezpečnost*. Praha : Powerprint s.r.o., 2015. ISBN 978-80-87994-72-6.

Eng. Martin OBERT (PhD. student)  
Armed Forces Academy of General M. R. Štefánik  
Demänová 393  
031 01 Liptovský Mikuláš  
Slovak Republic  
E-mail: martin.obert2@gmail.com

Col. (ret.) Assoc. Prof. Eng. Marcel HAKAKAL, PhD.  
Armed Forces Academy of General M. R. Štefánik  
Demänová 393  
031 01 Liptovský Mikuláš  
Slovak Republic  
E-mail: marcel.harakal@aos.sk

**Col. (ret.) Assoc. Prof. Eng. Marcel Harakal', PhD.** - He received the MSc. degree in electrical engineering from the Faculty of Electrical Engineering, Slovak Technical University in Bratislava in 1983. In 1997 he successfully finished his PhD. studies in artificial intelligence. From 1983 to 1989 he worked as a research engineer at the Military Research Institute in Liptovský Mikuláš. In 1989 he joined the Armed Forces and since then he has worked in various teaching and managerial positions at the Department of Informatics. During his university career from 2004 to 2012 he led the Department of Informatics. Currently he is in the position of Vice Rector for Science of the Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovakia.

His research interests include computer engineering, image processing, cyber security, and network operations. He is the guarantor of the bachelor degree study program "Computer systems, networks, and services". Since 2003 he has been a member of AFCEA and since September 2006 he has been in the position of Vice President for Membership of AFCEA Slovak Chapter. Since 2004 he has been the General Chairman of the International Scientific Conference "Communication and Information Technology - KIT" in Tatranské Zruby, High Tatras.

**Eng. Martin Obert** - was born in Trenčín, Slovakia in 1980. He received his Engineer degree in 2003 in Communication and Radio systems from the Military Academy in Liptovský Mikuláš. His research is aimed to security in wireless communication and its applications mainly in industry in the field of autonomous cybernetic systems.

## CHALLENGES AND THREATS FOR THE INTERNATIONAL SECURITY AS THE CONSEQUENCE OF THE RUSSIAN FEDERATION'S HYBRID WAR

Mirosław BANASIK

**Abstract:** The current situation in Ukraine confirms that the European thesis on solving conflicts with peace categories and through the road of diplomacy does not work in a perfect way. The evaluation of the Russian Federation's activity (RF) after occupying the Crimea shows that strategic objectives of Moscow spread farther. In the strategic dimension the hybrid war led by Moscow is measured up against the entire NATO as perceived being the main threat. Past experiences in Ukraine and the theory assessment show that the new generation war run by the RF embraces multi-storey efforts directed at the state's function destabilizing, changing the internal order or/and leading to the state's bankruptcy not even necessarily seizing its territory. The complex nature of the hybrid threats requires undertaking integrated actions by the international community. It seems it will be possible to reach it while having the common NATO and EU doctrine on the hybrid threats counteraction. States, particularly those endangered, should draw up and implement their own accustomed strategy of the national security that will let opposing both classical and hybrid threats, with as well as without the NATO aid.

**Keywords:** hybrid war, threats, the Russian Federation, Ukraine, NATO, the European Union.

### 1 INTRODUCTION

The Russian aggression in Ukraine in 2014 and the illegal annexation of Crimea has been the first case of forceful movement of the borderlines and incorporation of another state into the territory of aggressor since the end of the Second World War. The event changed the perception of threats to the world, especially to Europe and direct neighbors of the Russian Federation (RF). Infringement of the international rules on the peace and international security took place in defiance of the decisions of the United Nations Charter of the USA even though Russia is a permanent member of the UN. In spite of the fact that Russia signed the Final Act of the Security Conference and Cooperation in Helsinki [9] in 1975, The Budapest Memorandum on Security Assurances in 1994 is a member of the NATO-Russia Council and European Council; it does not comply with the member decisions, documents and settlements. Unprecedented infringement by Moscow the international law, restoration of the power of Russia, conduction of the expansion policy and intimidation of the West took place after all in the circumstance of quiet acceptance of the NATO and EU what can an expression of the lack of strategy of response. Restlessness of the state of former Russian republics very dependent on Russia in terms of economy and energy [28] cause W. Putin to say that the armed force of the RF can be used for protection of the Russian-speaking people that stay outside the Russian state [24]. These countries are afraid that Ukraine scenario of destabilization of the institution of state, chaos and unrighteousness can be repeated.

The situation in Ukraine confirms that the thesis of the European reasoning in the categories of peace and conflict-solving through diplomacy did not testify, as well as the frequently used throughout the last decades by the USA the strategy of *hard power*, namely the use of regular armed force. Engagement into the Russian Federation on Ukraine after the exit

from the country by W. Janukowicz opens a new epoch of the Russian strategy in reaching its political objectives, and on the other hand, changes the paradigm of employing the regular force in modern wars referred to as hybrid, non-linear or new generation wars. It turned out that the second decade of twenty first century is the decade of restricted use of the armed force which is proved by the strategy and practice of the USA, China and concealment of the use of the force by the RF in Abkhazia, the South Ossetia or Transnistria [18]. Russia in pursuit of expansion and restoration of its great power combines many so far well know methods of the use of force with new abilities gathered mainly thanks to new technologies as well as the instruments of non-military influence with modern concept of holistic and multi-dimensional influence on the weaker elements of defensive force of a hostile state. Centered structure of command and process of leadership allows leading long-standing, coordinated operations in diplomatic, informational, economic, military and cybernetic dimension. This way, Moscow reaches its strategic objectives without an official warfare. Other methods may embrace the threat of the use of nuclear weapon [10], mass use of regular armed force and pressuring through creating frozen conflicts.

The RF operation on Ukraine strengthens the conviction that European-Atlantic security becomes less and less stable and the security environment undergoes rapid transformations. Nowadays, the largest threats are posed by the Russian strategic objectives, Military Doctrine and ability possession [21].

The aim of the article is to define challenges and threats for security resulting from the concept of hybrid warfare led by the RF as well as identification of counteractive methods. Results of researches are presented by solving the problems as follow:

1. What the essence of warfare is expressed by?
2. What challenges and threats for safety do result from the concept of hybrid warfare?
3. How should the hybrid threats be counteracted?

## 2 DEFINITION OF THE HYBRID WARFARE

The theory of threats and hybrid warfare occurs when the conflict between Israel and Hezbollah closes in 2006 and basically refers to the conditionings of events of the last decade. Definitions formulated [16] do not correspond fully with what we observe in Ukraine. F. Hoffman emphasizes that the characteristic of hybrid warfare is commonness of the acts of terrorism and variety of crime forms [15]. He defined hybrid threats as an opponent who simultaneously and adaptably uses integrated combination of conventional weapon and irregular tactics, terrorism and criminal elements on the battlefield in order to reach political goals [16]. The definition above does not work in the confrontation with non-kinetic threats that take place commonly in Ukrainian conflict. Nevertheless, it indicates that as a result of hybrid warfare the political goals are reached which means that operationalization of the concept serves for realization of the strategy. Ukrainian experience proves it. Thus, the concept of hybrid warfare as distinct from those of last decades should be considered in strategical categories. Therefore, the thesis should be posed that it inscribes well in Clausewitz's paradigm of warfare conduction which says that war is only a continuation of policy by other means [11]. A. Jacobs and G. Lascoasnjaras (2015) propose a very general but also universal definition of hybrid warfare which would seem to be conceivable if it was not limited to operations with the use of violence. In their meaning, the concept of *hybrid warfare means a form of conflict with the application of violence which state and non-state actors are involved in using conventional and unconventional means of influence not limited to the battlefield or a specific unconventional of influence, not limited to the battlefield or a specific, physical territory* [17]. In the hybrid warfare, the space of influence as distinct from a traditional warfare does not limit to physical dimension and is present in other dimensions in which regular armed forces did not influence so far. Its essence is to cause planned and coveted effects which are synchronized. A. Deep states that the effects are received thanks to the employment of asymmetric technics and tactics are synchronized on multi-dimensional battlefield [13]. Multi-dimensional character of fight and the significance of synergy of the effects can be seen also by F. Hoffman [15]. His descriptive approach to the threats and hybrid warfare seems to be correct one. It is believed that hybrid warfare combines a variety of fight models and involves classical military abilities, irregular tactics applied by

irregular formations, terroristic acts, common violence and intimidation as well as criminal chaos. To follow the course, he believes that the hybrid warfare can be conducted both by state and non-state actors. He thinks that multimodal activities can be implemented by separated subjects (or even one subject), but generally they are operationally and tactically directed in the main battlefield aimed at reaching the effect of synergy in physical and psychological dimension of conflict [15]. J. Messner perceived the significance of psychological dimension. He said that informational and psychological impacts were the factors that determine the victory or failure in fight. He posed the thesis that in hybrid warfare psychology was its fourth dimension [25]. Then, as opposed to the classical war the aim of hybrid warfare is not an occupation of the territory of a hostile state but an occupation of the awareness of its society.

## 3 CHALLENGES AND THREATS OF THE HYBRID WARFARE

The assessment of Russian activities in order to conquer Crimea and involve in the war in Donbas points out that the strategic objectives of Moscow do not limit to destabilization of the situation on Ukraine, pressuring the authorities in Kijow and realization of the plan of making New Russia, but they do not go further. Restoration of the great power status of Russia and developing the spheres of influence endanger the states of the East of Europe. Hybrid warfare led by Moscow in strategical dimension is measured up against the entire NATO which is perceived as the main threat. Putin will try to humiliate NATO and undermine its reliability of alliance [28]. Russian new approach to war waging without its official declaration combines many recognizable elements with modern concept of influence of the so-called hard and soft one, with an emphasis of the other [19]. The Russian strategy does not limit to irregular armed force as it is defined by Hoffman, but predicts the use of hybrid instrument being in disposal of the entire state. Contemporary wars do not limit to the use of regular armed force. Thanks to centralized structure of command and the process of decision, Russia can lead long-lasting, coordinated operations in the diplomatic, informational, economic, military and cybernetic dimension. This way, Moscow reaches its strategic objectives without an official warfare. It turned out that non-military instruments fail to provide immediate verdicts; nonetheless, they are more effective than the armed force. The armed force as the Russian Military Doctrine indicates will be always employed in modern conflicts, but only when the influence of non-military instruments will appear to be ineffective and only in the times deciding about the final results of a conflict [10]. The phenomenon of hybrid warfare consists in

reaching strategic objectives without the need to wage a military struggle in traditional sense. It testifies the thesis posed by J. Messner who stated that the end of the twenty century put an end to the epoch of warfare according to Clausewitz's opinion as a clash of two opposing armies [25].

Russia permanently introduces the state of threat for all member states of NATO which is proved by making demonstrative flights but of armed fighter-bombers and strategic bombers. Russia provokes and tests the NATO defense system through playing with submarines in the Baltic Sea [30]. Russia runs also aggressive exercise based on the scenario of aggressive operations with the use of nuclear weapon throughout its own territory and arctic area. Defense budget raises constantly and pursue gathering new capabilities by programmes of the development of armed force planned for the period from 2010 to 2020 [31]. The background for the reforms of Russian armed force will be the concept of network centrality and non-linearity [23]. J. Bērziņš points out that in the transformation of Russian armed force the following priorities will apply [5]:

1. Departing from direct destruction in favour of direct influence;
2. Departing from direct elimination of an adversary in favour of drawing it closer and convincing him to join the attacking side;
3. Departing from armoured warfare in favour of culture warfare;
4. Departing from the use of regular general military subdivisions in favour of the compact, networked subdivisions of variety of specialisations, integrated in the informational space and private military companies;
5. Departing from traditional, tridimensional fight in favour of the informational/psychological fight and perception fight;
6. Departing from direct clashes of armies in favour of non-contact fight.

As a result of the realization of the armed force development programmes the Russian Federation intend to possess new capabilities of psychological operations, strategical misconception and strategical communication. The aim of the Russian reforms is taking strategical initiative which is the condition of victory.

Kremlin effectively applies *maskirovka* (masking) which is a part of Russian doctrine of 1930 on the strategical, operational and tactical level. However, what used to be technics of battlefield nowadays has become a strategical state tool and overshadows the entire Europe [19]. It is supported by informational fight which intends to mislead in differentiating between what is true and false, between the reality and fantasy. In the Military Doctrine of the Russian Federation of 2014 there were found records on asymmetric methods of operation that let eliminating the advantage of an

enemy, participating in the conflicts of irregular subdivisions of the armed force and private military companies. An important emphasis was put on the use of political powers and social movements directed and funded from outside [8].

Changes in the views of Russian strategists on war conduction one can see in the articles and public speeches made by the Chief of the Russian Federation General Staff [4]. Gerasimov general presented twentieth century war model called new generation war in which special emphasis is put on the measures of non-military impact used for political and strategical objectives achievement. Gerasimov can see the significance of modern technologies. Therefore, he maintains that precise strikes from a distance on selected objects of states critical infrastructure and selected military objects will be new non-contact form of future fight [4]. For the asymmetry and destabilization of hostile state throughout its territory and in all dimensions of its function he refers also the future wars as non-linear ones [14]. Foregoing experiences in Ukraine and the assessment of theories indicates that new generation warfare includes multi-storey efforts oriented towards destabilization of state function and transformation in its internal order. As opposed to the conventional warfare a centre of gravity of new generation war will be centered in the society [3]. Russian perception of modern war is based on the idea of playing war in people's minds which was pointed out by Messner. In consequence it leads to large-scale informational impact in order to gain the upper hand in their psyche, leads to frustration and moral decay of both the armoured subdivisions and civil people. In a new generation war the pursuit of deployment of combat subdivisions of the armed force only in the last resort. On the other hand, an adversary will be impelled to engage its whole potential. It will to influence the government and the entire state destructively which as a result is to lead to its failure [3]. Russian operations in Ukraine unambiguously indicate that security environment in Europe becomes unpredictable. The aim of Russian hybrid impact is pressuring and destabilization of neighbouring states without the need to seize the territory. Combination and synchronization of camouflaged non-military operations cause the effect of surprise and handicap the adequate reaction especially of international organizations functioning on the base of consensus. Hybrid warfare is dangerous, because it is easy, cheap for external aggressor yet costly and negative in its consequences for the defending one [26]. Blackmail about the use by RF nuclear weapon and large-scale use of militaries and conventional weapon as well as creating frozen conflicts is a large threat for the security of Euro-Atlantic area. In order not to prevent a large-scale crisis situation the protective operations are deliberately taken up.

#### 4 STANDING UP TO HYBRID THREATS

Coordinated and asymmetric operations by RF with employment of many instruments create a strategic ambiguity. Through complex and multidimensional influence Russia intentionally sends wrong signals, which masks its real intentions, confounds adversaries, impedes decisive process and make a response ineffective. Putin in his pursuit of division of West and influencing the weakest elements by means of hybrid strategy with the use of conventional and unconventional tactics paradoxically led to approach of NATO and the European Union (EU). Awareness of seriousness of the situation made NATO collective defense to be its highest priority and EU wants to contribute to the security as much as possible in both political and military field.

In order to ensure preparedness of the Alliance to respond to new challenges in the security area, in Newport Summit the "Readiness Action Plan" (RAP) was approved. The plan aims to enforce a collective defense of the Alliance as well as enhance the capability of crisis management. The plan elements involve measures referring to both constant need of ensuring Allies' security and strategic adaptation of forces and military measures of the Alliance to new challenges in security area [1].

In the framework of the continuation of the foregoing security measures of allied militaries applied in 2014 the Alliance decided to maintain continuous and rotational presence of Allied armies on the ground, at sea and in the air of the Eastern flank territory as well as the Baltic, Black and Mediterranean Sea. The alliance will continue to perform intensified exercises, especially in the Eastern flank territory. Scenarios of those exercises will be tailored to present challenges, particularly the threats coming from the East. Situational awareness will be enhanced by flights of AWACS aircrafts on the Eastern flank, namely, in Poland and Romania as well as by increasing the exchange of reconnaissance and intelligence information between allies and NATO's Command Structure [34]. Strengthened Baltic Air Policing will be maintained consisting of 16 aircrafts based on Siauliai airport in Lithuania, Amari in Estonia and Malbork. It is planned to enhance the cooperation between NATO's Command Structure and national commands, and up-dating of defensive plans and potential one for the countries of the Eastern flank [1].

The second part of the „Readiness Action Plan” involves adaptation measures essential to ensure a full ability of the Alliance to live up to new challenges in the security area. As part of the resources the Alliance will make reforms of NATO Response Force (NRF). It is planned to increase its number from 13 thousand to 25 thousand of soldiers. Nowadays, the NRF functioning collection will be

enforced by hard and antiaircraft units prepared to rapid deployment in the region threatened. Within the framework of NRF Very High Readiness Joint Task Force (VJTF) the so-called "Spearhead Force" will be organized. It will be a unit in size of the brigade of ground troops consisted of approximately 5 thousand supported by elements of the rest military force (maritime, air and special ones). VJTF should be capable of deployment in region threatened within 2 to 5 days since decision is made. Readiness of the elements of VJTF will be examined as part of exercises announced shortly before. Achieving complete operational readiness of VJTF is anticipated for 2016 [1]. Until then, the part of temporary VJTF will play the elements of NATO Response Force Collection of 2015 consisted of German, Dutch and Norway subdivisions [20].

Justification of decision-making process is planned in the scope of VJTF force activation. Nowadays, in order to use NATO Response Force the consent of North-Atlantic Council is required which delay the process of their activation. According to the preliminary assumptions, VJTF unit will be subordinated to NATO Command Structure on a rotational basis to one of NATO High Readiness corpses [1]. In the case of its use in NATO Eastern flank, the command of the unit would be taken up by Multinational Corps Northeast from Szczecin [6].

Parallel to the implementation of „Readiness Action Plan” the Alliance will work on strengthening capabilities in the area of response to the hybrid warfare which includes a wide spectrum of overt and covert as well as military, paramilitary and civil operations closely coordinated. The Alliance should possess the tools and procedures necessary for effective deterrence and reaction to the threats. For this reason strategic communication will be improved, new sceneries of exercises considering hybrid threats will be drawn up and coordination of NATO operations with partner states and organizations will be strengthened [1]. Critics claim that NATO prepares classical response against unconventional operations of RF. Undoubtedly, the unconventional abilities will be also needed to counteract the hybrid warfare including disinformation counteraction, subversive operations, or cyberattacks. Although decisions made by Wales determine some directions of counteracting hybrid threats, but it seems that they are the consequence of traditional thinking. It is simply impossible to face the new idea by old methods. One may ask a question here: will VJTF be able to stand up against non-state actors applying unconventional methods of fight, procedures and technics or agents running subversive activity, spreading chaos, terror and intimidation? Is not it necessary in the first place to draw up a complex untraditional strategy enabling both collective and single state being the target of hybrid attack to response [29]? Consequences of new strategy introduction need to find its reflection

in the doctrine of armed force use, programmes and trainings. However, the most important are the changes in mentality of leaders and soldiers that enable to fight in new quality conditionings. In the aspect of the operation conducted in Crimea which was not an armed attack but operationalized new form of warfare, one can ask a question: are possible legal footings of NATO and the response instruments available adequate to contemporary wars requirements called by Gerasimov *new generation wars* [4]. The momentum and scale of military operations by RF are deliberately restricted and maintained by aggressor at the level below possibly unambiguously identifiable the threshold of regular open war [2]. NATO will find it much difficult to response as the level of aggression maintain below the criteria adopted for classical threats will not allow applying collective defense instruments as it was stipulated in Article 5 of the Washington Treaty on the armed assault to one or more side of Alliance (Artykuł .., 1949). Readiness Action Plan signed in Newport should be the foundation stone of deeper changes of records in Article 5 and drawing up a new NATO strategy concept which will explicitly indicate not only how to stand up against complex hybrid threats [19].

European Union claims that hybrid threats will evaluate along with the development of new technologies. It is assessed that activities should be taken up for security of sensitive elements of state security system. The core of defense philosophy against hybrid threats consists in complex recognition of the effects possible to withstand threats. It seems to be a correct assumption that hybrid strike is designed and oriented towards the most vulnerable elements of state function [4]. In the case of Ukraine the critical ones include:

- 1) Weak government, state institution and corruption;
- 2) Weakness of security structures and state defense;
- 3) Marginalization of Russian-speaking population;
- 4) Much dependence on Russian supply of oil and gas [12].

Ukrainian defense system likewise of other states traditionally was prepared to defend against regular state armed force. It turned out that it did not live up to the requirements being the consequence of non-state actors' appearance leading the so-called *proxy war*. The thesis was proved that the sensitive areas and crucial ones for state function in the same time are: economy, energetic sector and fuel system, critical infrastructure, financial system, communication system and transport [4]. In this aspect, especially important for EU will be provision of energetic security through a supply of energy from outside and diversification of its sources. Well-recognized its own weaknesses are the basis for preparing effective security and defense system against hybrid threats [12].

The strategy of counteracting hybrid threats must consider conviction of a possible aggressor on the consequences of an operation and the price he would need to pay. Deterrence can be realized in two stages. Firstly, the consequence of sanction can be expressed by punitive operations which lead as a result to severe damages on the attacking side and may turn out to be inviable. Secondly, it can significantly raise the level of critical infrastructure and prepare the society to unpredictable consequences and negative events [4]. There is a great room for development in searching the ways of cooperation between EU and NATO in preparing a complex collection of tools for counteracting hybrid threats. Integrated operation of those organizations based on a common doctrine can be the future fundamental pillar of deterrence [12].

In conclusion it should be said that complexity of hybrid threats requires a strategy based on which the politics and guidelines for taking up coherent EU operations need to be shaped. The conclusions of debate on hybrid threats must find its reflection in new strategy of EU security. If common with NATO strategy of counteracting hybrid threats are not drawn up the EU strategy will need to be complementary with NATO strategy. Drawing up a common strategy of counteracting hybrid threats is a good chance for improvement of the relationship between EU and NATO. It should be the ground of mutual support [4]. Common EU security and defense policies in the aspect of counteracting hybrid threats is a good base for exchange of the intelligence information, building new capabilities, including situational awareness and training and exercises conduction. The priority for EU is establishment of a cell integrating information on hybrid threats. It will have a crucial meaning for warning on threats and preparing adequate response. Communication strategy will considerably improve the message directed to the Russian Federation as well as preparing of the response to any expressions of disinformation [4].

## 5 CONCLUSIONS

Taking into account a lack of firm reaction of the West, decreasing the capabilities of Ukrainian Armed Force and constantly enforced presence of Russian armies on the territory of Ukraine spreading of territorial conflict cannot be excluded as well as the intention of taking territorial control over as far as Nadniestrz and in the same time cutting off Ukraine from the Black Sea. Transfer of the methods applied by Russians in hybrid war on the other regions including Baltic States cannot be excluded as well. Majority of experts' stance is that lack of prevention of the aggressive operation by Russians on Ukraine at its present stage will result increasing threat to destabilization of the entire region of the

Middle and East of Europe. No decision of president Obama and the presidents of East of Europe States in the case of providing to Ukraine with military support is wider and wider as well as more sharply criticized also by some representatives of American administration and supreme military leaders.

Results of the researches prove that the operations of RF undertaken in Ukraine are not an improvisation but reflect an ordered employment of the all spectrum of the tool available to the opposite side. In the aspect of the all sequence of events one can pose a thesis that they inscribe well in the paradigm of Clausewitz on war conduction which says that war is only a continuation of policy by other means. I claim that hybrid operations refer to exactly those means but the rules of war conduction, its character and objectives remain all the same [3].

It seems that it is not very likely that Russia crossed the borderline of the territory of NATO, nevertheless it should be expected that through non-military operations will try to destabilize coherence of both NATO and EU. Effective response to hybrid operations will require coordinated operations of both organizations. In order to ensure it possession of a common doctrine of counteracting hybrid threats is essential. NATO should play a leading part in such areas like preparing military response, intelligence and deterrence and when necessary, intervention. It seems that in the time of peace the best element of deterrence is constant presence of NATO armies on the territory of the most threatened states. EU should be responsible for counteracting in cyberspace, energetic and migration policy and counteracting propaganda. It is intended to pursue synergy in an integrated employment of all instruments being at disposal of both organizations [4].

Extremely challenging for both organizations and member states, particularly those threatened, will be reduction of any susceptibilities and vulnerabilities to the hybrid threats. Either NATO or EU will not ensure absolute security of member states in the face of hybrid threats but will certainly help in building their resilience to them. Particular states should elaborate and implement their own non-standard strategy of national security which will allow standing up to classical and hybrid threat with and without the aid of NATO. For the realization of the strategy there need to be assigned resources that would ensure gathering the capabilities required. Undoubtedly, Eastern European countries have to modify the fundamentals of their defense structure to be able to take up future challenges [4].

## References

- [1] BANASIK, M.: (2015a) *Zdolności NATO do Działań Ekspedycyjnych w Przyszłym Środowisku Bezpieczeństwa Międzynarodowego*. Warsaw : 2015.
- [2] BANASIK, M.: (2015b) *Wyzwania dla Bezpieczeństwa Wynikające z Koncepcji Prowadzenia Wojny Nowej Generacji przez Federację Rosyjską, w Zarządzanie Bezpieczeństwem Państwa – Wyzwania i Ryzyka*. Pod red. T. Szmidka, Piotrków.
- [3] BANASIK, M.: (2015c) *Wojna Hybrydowa w Teorii i Praktyce Federacji Rosyjskiej*. In *Bellona*, no 4/2015.
- [4] BANASIK, M.: (2015d) *Nato i Unia Europejska A Doktryna Gierasimowa*, w Górka, M., Tokarz, G.: *Społeczno-Administracyjny Wymiar Bezpieczeństwa Publicznego*. Koszalin : 2016.
- [5] BĒRZIŅŠ, J.: (2014) *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. In *Policy Paper*, no 02, April. [online]. Available at: <http://www.naa.mil.lv/~media/NAA/AZPC/Publikācijas/PP%2002-2014.ashx#page=6&zoom=60,-97,327>, accessed 4.06.2015.
- [6] BIELECKI, M.: (2015) *Szczecin: Gen. Breedlove Pozytywnie O Zmianach W Korpusie NATO*. Polska Agencja Prasowa, 13 January [online]. Available at: [http://www.pap.pl/palio/html.run?\\_Instance=cms\\_www.pap.pl&\\_PageID=1&s=infopakiet&dz=kraj&idNewsComp=193014&filename=&idnews=196325&data=&status=biezace&\\_Checksum=1294321664](http://www.pap.pl/palio/html.run?_Instance=cms_www.pap.pl&_PageID=1&s=infopakiet&dz=kraj&idNewsComp=193014&filename=&idnews=196325&data=&status=biezace&_Checksum=1294321664), accessed 26.02.2015.
- [8] *Военная доктрина Российской Федерации*, (2014), 30 декабря [online]. Available at: <http://www.rg.ru/2014/12/30/doktrina-dok.html>, accessed 31.05.2015.
- [9] Conference On Security And Cooperation. In *Europe Final Act*, Helsinki 1975. [online]. Available at: <http://www.osce.org/mc/39501?download=true> accessed 10.07.2015.
- [10] CHEKINOV, S. G., BOGDANOV S. A.: (2013) *The Nature and Content of a New-Generation War, Military Thought*, No 4. Available at: [http://www.eastviewpress.com/Files/MT\\_FROM%20THE%20CURRENT%20ISSUE\\_No.4\\_2013.pdf](http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf), accessed 03.07.2015.
- [11] CLAUSEWITZ, C.: (1995) *O Wojnie*. [online]. Available at: [http://plikopedia.com/eL8pAJ/clausewitz\\_o\\_wojnie\\_download.zip](http://plikopedia.com/eL8pAJ/clausewitz_o_wojnie_download.zip), accessed 03.07.2015.
- [12] *Countering Hybrid Threats* (2015), Food-for-thought paper, European External Action Service (EEAS), Council of the European Union, 8887/15, Brussels, 13 May.



- [13] DEEP, A.: (2015) Hybrid War: Old Concept, New Techniques. In *Small Wars Journal*, 2 March. [online]. Available at: <http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques> accessed 28.05.2015.
- [14] ГЕРАСИМОВ, В. [Gerasimov] (2013), *Новые Вызовы Требуют Переосмыслить Формы И Способы Ведения Боевых Действий*, Российской Федерации, Генерал Армии, Опубликовано в выпуске № 8 (476) за 27 февраля. [online] Available at: <http://www.vpk-news.ru/articles/14632> accessed 31.05.2015.
- [15] HOFFMAN, F. G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December [online]. Available at: <http://www.comw.org/qdr/fulltext/0712hoffman.pdf>, accessed 15.07.2015.
- [16] HOFFMAN, F. G. (2009) *Hybrid Vs. Compound War, The Janus Choice: Defining Today's Multifaceted Conflict*, 1 October, [online] Available at: <http://www.armedforcesjournal.com/hybrid-vs-compound-war/>, accessed 28.05.2015.
- [17] JACOBS, A., LASCONJARIAS, G. (2015), *NATO's Hybrid Flanks: Handling Unconventional Warfare in the South and East*, NDC Rome, No 112, April [online]. Available at: [http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Fmercury.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F190786%2Fpublicationdocument\\_singledocument%2F842be548-695b-4c3e-a8ab-6c8c9f3f4038%2Fen%2Frp\\_112.pdf&ei=gBVqVeWHJsSVsgHE7YHACw&usg=AFQjCNFJHnGYCHBOfZ2SbucGZEhIRDyoVQ&bvm=bv.94455598,d.bGg](http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Fmercury.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F190786%2Fpublicationdocument_singledocument%2F842be548-695b-4c3e-a8ab-6c8c9f3f4038%2Fen%2Frp_112.pdf&ei=gBVqVeWHJsSVsgHE7YHACw&usg=AFQjCNFJHnGYCHBOfZ2SbucGZEhIRDyoVQ&bvm=bv.94455598,d.bGg), accessed 28.05.2015.
- [18] LAMBERT, M. (2015), *Hybrid War at Work in The Post-Soviet Space*, 24 May, [online] Available at: <http://estonianworld.com/security/hybrid-war-at-work-in-the-post-soviet-space/> accessed 13.07.2015.
- [19] LINDLEY-FRENCH, J. (2015) *NATO and New Ways of Warfare: Defeating Hybrid Threats*, Conference Report, 19 May [online]. Available at: [http://www.ndc.nato.int/news/current\\_news.php?icode=814](http://www.ndc.nato.int/news/current_news.php?icode=814), accessed 14.07.2015.
- [20] LORENZ, W. (2015) *Szpica NATO Potrzebuje Tarczy na Wschodniej Flance*, Biuletyn PISM no 15, Warsaw, 9 February [online]. Available at: [www.pism.pl/files/?id\\_plik=19213](http://www.pism.pl/files/?id_plik=19213), accessed 26.02.2015.
- [21] MAIGRE, M. (2015), *Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO*, German Marshall Fund of the United States, February. [online]. Available at: [http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCGQFjABahUKEwjtzpPD5IrGAhWG6CwKHU-2B7M&url=http%3A%2F%2Fwww.gmfus.org%2Ffile%2F4272%2Fdownload&ei=8CR7Ve2WF4bRswHP7J6YCW&usg=AFQjCNGaALAOq83IXw8z-o-Gu\\_YaQwCrVg&bvm=bv.95515949,d.bGg](http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCGQFjABahUKEwjtzpPD5IrGAhWG6CwKHU-2B7M&url=http%3A%2F%2Fwww.gmfus.org%2Ffile%2F4272%2Fdownload&ei=8CR7Ve2WF4bRswHP7J6YCW&usg=AFQjCNGaALAOq83IXw8z-o-Gu_YaQwCrVg&bvm=bv.95515949,d.bGg), accessed 12.06.2015.
- [23] McDERMOTT, R. (2014), *Myth and Reality—A Net Assessment of Russia's 'Hybrid Warfare' Strategy Since the Start of 2014 (Part One)*, 17 October. [online]. Available at: [http://www.jamestown.org/programs/singlet/?tx\\_ttnews\[tt\\_news\]=42966&cHash=6807c1930eae4cbece171314536d557c#.VWwltEZIPX4](http://www.jamestown.org/programs/singlet/?tx_ttnews[tt_news]=42966&cHash=6807c1930eae4cbece171314536d557c#.VWwltEZIPX4) accessed 31.06.2015.
- [24] MENKISZAK, M.: (2014) *Doktryna Putina: Tworzenie koncepcyjnych podstaw Rosyjskiej Dominacji Na Obszarze Postradzieckim*, Komentarze, Numer 131, 28 March. [online]. Available at: [http://www.osw.waw.pl/sites/default/files/komentarze\\_131.pdf](http://www.osw.waw.pl/sites/default/files/komentarze_131.pdf). accessed 07.07.2015.
- [25] МЕССНЕР, Е. Э. [Messner, E. J.] (2005) *Хочешь Мира, Победи Мятёжевойну!*, Москва. [online]. Available at: [http://militera.lib.ru/science/0/pdf/messner\\_ea01.pdf](http://militera.lib.ru/science/0/pdf/messner_ea01.pdf), accessed 02.07.2015.
- [26] POPESCU, N. (2015), *Hybrid Tactics: Neither New Nor Only Russian*, European Union Institute for Security Studies, January. [online] Available at: [http://www.iss.europa.eu/uploads/media/Alert\\_4\\_hybrid\\_warfare.pdf](http://www.iss.europa.eu/uploads/media/Alert_4_hybrid_warfare.pdf), accessed 12.06.2015.
- [27] SABAK, J. (2014) *W Rosji Powstają Prywatne Armie*, Defence24, 28 June. [online] Available at: [http://www.defence24.pl/news\\_w-rosji-powstaja-prywatne-armie](http://www.defence24.pl/news_w-rosji-powstaja-prywatne-armie), accessed 31.05.2015.
- [28] ŠEŠELGYTĖ, M. (2014, p.2) *Can Hybrid War Become the Main Security Challenge for Eastern Europe?* 17 October 2014. [online]. Available at: [http://www.europeanleadershipnetwork.org/can-hybrid-war-become-the-main-security-challenge-for-eastern-europe\\_2025.html](http://www.europeanleadershipnetwork.org/can-hybrid-war-become-the-main-security-challenge-for-eastern-europe_2025.html), accessed 07.07.2015.
- [29] SANDOR, F. (2015) *Hybrid Warfare Revisited*, Vol. 5, No 3, August. [online] Available at: <https://globalecco.org/hybrid-warfare-revisited>, accessed 14.09.2015.
- [30] SCHADLOW, N. (2015), *The Problem with Hybrid Warfare*, 2 April. [online] Available at: <http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/>, accessed 28.06.2015.
- [31] SMURA, T., LIPKA, R. (2015) *Program modernizacji Sił Zbrojnych Federacji Rosyjskiej - stan realizacji i perspektywy powodzenia*, Defence 24, 21 February. [online] Available at: <http://www.defence24.pl/Blog-program-modernizacji-sil-zbrojnych-federacji->

- rosyjskiej-stan-realizacji-i-perspektywy-powodzenia, accessed 04.07. 2015.
- [32] SUDOPLATOV, P., SUDOPLATOV, A.: (2006), *Special Tasks: The Memoirs Of An Unwanted Witness - A Soviet Spymaster*, 30 June. [online] Available at: <http://mailstar.net/sudoplat.html>, accessed 28.05.2015.
- [33] Traktat Północnoatlantycki i Ustawa O Jego Ratyfikacji (1949) [online] Available at: [https://www.bbn.gov.pl/ftp/dok/01/traktat\\_polnocnoatlantycki\\_ustawa\\_o\\_ratyfikacji.pdf](https://www.bbn.gov.pl/ftp/dok/01/traktat_polnocnoatlantycki_ustawa_o_ratyfikacji.pdf), accessed 15.07.2015.
- [34] Wales *Summit Declaration*, (2014), Newport 29 September [online] Available at: [www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](http://www.nato.int/cps/en/natohq/official_texts_112964.htm), accessed 26.02.2015.

Assoc. Prof. Mirosław BANASIK, Ph.D.  
Jan Kochanowski University in Kielce  
Żeromskiego st. 5  
25-369 Kielce  
Poland  
E-mail: rawenna2309@interia.pl

**Assoc. Prof. Mirosław BANASIK, Ph.D. -** Currently working at Jan Kochanowski University in Kielce (Poland). PhD in Humanities, certified colonel of the Polish Armed Forces, graduate (Postgraduate Studies) from the National Defence University in Warsaw and the NATO Defense College in Rome (Italy). He took hold the range of command and staff posts. Among others, he was the Deputy of the Polish National Military Representative to SHAPE (Supreme Headquarters Allied Powers Europe). The area of his scientific interests includes the issues related to the national, international security and the crisis management.

# OPTIMAL SENSOR DISLOCATION FOR TARGET LOCALIZATION IN 2D AND 3D AREA

Peter RINDZÁK

**Abstract:** The following paper describes the possibilities of UAV (Unmanned Aerial Vehicles) employment where the radar sensors are part of it in the area of NEC (Network enabled capability) in armed forces domain. The main task is to discover the methodology of how to disseminate each individual UAV in 2D and 3D area in order to achieve the best estimate of target position. Each individual optimization strategy is proven by simulation in Matlab and based on the mathematical concept expressing the sensor matrix layout.

**Keywords:** NEC, Network enabled capability, UAV, sensors, TDOA.

## 1 INTRODUCTION

Nowadays, the most important attribute across the range of conducting the military operations is the timeous information gathering as a reason of increased amount of the information which is supposed to be available for each operation staff and for all command levels while decision making process is in conduct. The main way of how to gather information is the reconnaissance. Since the modern technology development is in progress, more UAVs are employed by armed forces for that purpose. In case of necessity, UAVs are capable to be equipped by various sensor technologies. Furthermore, once the NEC architecture and its necessary services are implemented across the armed forces, information gathered from those sensors could be easily used across different levels of command.

Advantages of the task solution in the NEC area:

- high-speed network for data transfer,
- minimal failure of data transfer ratio,
- maximum level of data transfer security,
- confidentiality,
- real-time transfer of data.

A lot of time was invested in order to find the solution for this task. The authors in [1] and [2] had already performed the research on TDOA position determination, focusing on the particular real world scenarios. Secondly, the authors in [3] and [4] focused their exploration on how the accurate the localization by TDOA in fact is. Lastly, [5] and [6] describe the Cramer-Rao inequality method which is often implemented during testing and effectiveness evaluation of target's position estimate. The main goal of last mentioned is to express a lower bound on the variance of estimators.

## 2 PROBLEM FORMULATION

We can suggest, that U, S, T are sensors which each UAV consist of and Z is the aim, which position we would like to detect. Firstly, we will deal with the technology, which in fact allows us to specify the position of the aim and the position of the each UAV, secondly, with the probability of the

detection of the aim. We suppose, that each UAV will have to be situated in those positions which will allow to gain the highest probability of detection. Moreover, we will suppose that each UAV will have to be able to leave own position in particular time intervals and the rest of UAVs in network will be also capable to rearrange their positions for the purpose of the network optimization. TDOA principle (Time Difference on Arrival) will be used as the main detection method of the object localization.

The most valuable advantage of this method is the fact that the more accurate coordinates of detected object we need, the more accurate determination of the distance between sensors and time differences between each input signal at each sensor have to be achieved. There are no such difficulties to accomplish those conditions nowadays. The time intervals could be measured in nanosecond time-accuracy, what makes the accuracy of the detection in hyperbolic system more advanced.

## 3 PRINCIPLES OF TDOA AS A METHOD OF HYPERBOLIC LOCATION

The main condition of the TDOA is the fact that there must be three receivers at least, which are necessary for location. Receivers are dislocated in operational area and their locations are given.

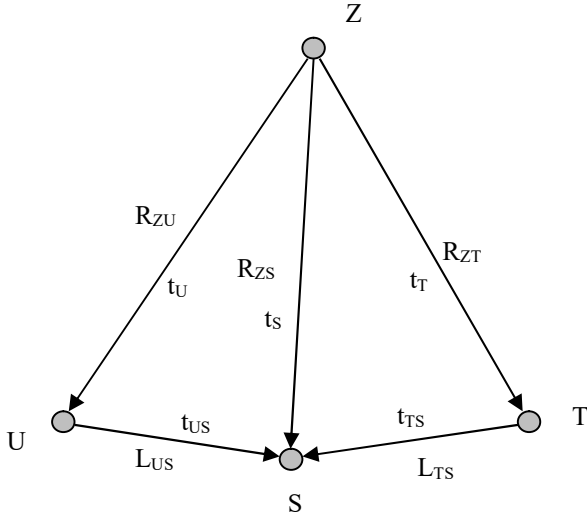
We can assume that U, S, T are sensors and their locations are given by coordinates  $U[x_U, y_U]$ ,  $S[x_S, y_S]$ ,  $T[x_T, y_T]$  and  $Z[x_Z, y_Z]$  is considered as an unknown coordinates of the object to be located.

Then:

$$ZU = R_{ZU} = c \cdot t_U \quad ZS = R_{ZS} = c \cdot t_S \quad ZT = R_{ZT} = c \cdot t_T \quad (1)$$

$$US = L_{US} = c \cdot t_{US} \quad TS = L_{TS} = c \cdot t_{TS}$$

Where  $c$  is velocity of the light and  $t_U$ ,  $t_S$ ,  $t_T$ ,  $t_{US}$ ,  $t_{TS}$  are the time intervals of the signal transition between sensors and the object or vice versa.



**Fig. 1** Principle of TDOA as a method of hyperbolic location

Time differences could be expressed as following:

$$\begin{aligned} (t_U + t_{US}) - t_S &= \tau_{US} \\ (t_T + t_{TS}) - t_S &= \tau_{TS} \end{aligned} \quad (2)$$

where  $\tau_{US}$ ,  $\tau_{TS}$  are the time differences of signal transmission.

Following formulas can be used for the calculation of hyperbolic coordinates:

$$\tau_U = \tau_{US} - \frac{L_{US}}{c} \quad \tau_T = \tau_{TS} - \frac{L_{TS}}{c} \quad (3)$$

where  $L_{US}$  and  $L_{TS}$  are distances between sensors [meter].

For better expression, it is necessary to transform hyperbolic coordinates into right angle coordinates system, which can be easily displayed in Cartesian coordinate system.

$$\tau_T = \frac{1}{c} \left( \pm \sqrt{(x - x_p)^2 + (y - y_p)^2} \pm \sqrt{x^2 + y^2} \right) \quad (4)$$

$$\tau_U = \frac{1}{c} \left( \pm \sqrt{(x - x_L)^2 + (y - y_L)^2} \pm \sqrt{x^2 + y^2} \right)$$

where  $\tau_T$  and  $\tau_U$  are hyperbolic coordinates of the signal source and  $x$  and  $y$  are right angle coordinates of the signal source.

#### 4 SENSOR DISLOCATION OPTIMIZATION IN 2D AREA

The accuracy of the TDOA method depends on the following three factors:

- accuracy of each individual sensor,
- appropriate estimation of target dislocation,
- sensor dislocation in consideration of target.

In this case we will deal with the issue of how sensor dislocation and dislocation optimization can affect an estimate of the target position.

Target position estimate is a complex variable, which is affected by several input parameters. From our perspective, the most important parameters are distance between sensors and the target, distance between each pair of sensors and an angle between each individual sensor and target.

Let assume that sensors and the target are stationary and they are dislocated in 2D, sensors are dislocated around the circle and the target is right in the middle.

During the testing and evaluation of effectiveness of estimate, the Cramer-Rao inequality is used. The main goal is to express a lower bound on the variance of estimators.

Cramer-Rao inequality (CRB) for target vector  $\bar{p} \in R^D$  and sensors  $\bar{q}_i \in R^D$ , where  $D$  expresses 2 or 3 dimensional area and  $M$  expresses the quantity of sensors, can be defined by [5]:

$$CRB = J^{-1} = (v\sigma)^2 (GG^T)^{-1} \quad (5)$$

where:

$$G = [g_{ij} \dots], (i,j) \in I, \quad \bar{g}_{ij} = \bar{g}_i - \bar{g}_j, \quad \bar{g}_i = \frac{\bar{q}_i - \bar{p}}{\|\bar{q}_i - \bar{p}\|}$$

where:

$J \dots$  is the Fischer information matrix (FIM), (its presence ensure the existence of linear independence of vectors)

$\bar{g}_i \dots$  is the vector heading from the target  $p$  to sensor  $i$ ,

$\bar{g}_{ij} \dots$  is difference between two direction vectors,

$\sigma^2 \dots$  expresses an error variance caused by Gauss noise. Set  $I$  consists of each individual sensor pair  $(i,j)$ . Matrix  $G$  contains all vectors  $\bar{g}_{ij}$ , where  $(i,j) \in I$ .

Various approaches can be used to achieve the minimum variance between predicted position and the real one.

The most common strategy is to minimize the trace of CRB [5]:

$$\min f_{CRB} = \text{tr}[J^{-1}] = (v\sigma)^2 \text{tr}[(GG^T)^{-1}] \quad (6)$$

or we can figure out the maximum of trace of FIM [5]:

$$\max f_{FIM} = \text{tr}[J] = \frac{1}{(v\sigma)^2} \text{tr}[GG^T] \quad (7)$$

Required conditions for calculation  $\min f_{CRB}$  are:

1.  $\sum_{i=1}^M \bar{g}_i = \bar{0}$
2. For matrix  $D \times M$   $g = [g_1 \dots g_M]$  must be  $gg^T = \frac{M}{D} I$

where:

$\bar{g}_i \dots$  is a vector heading from target  $p$  to sensor  $i$ ,

$M \dots$  the number of sensors,

$D \dots$  area dimension,

$I \dots$  expresses matrix, where elements on the main diagonal of the matrix are equal to 1.

In case of 2D area, the solution is the matrix, where there is the same angle between each neighbor sensors. We can express it as following [6]:

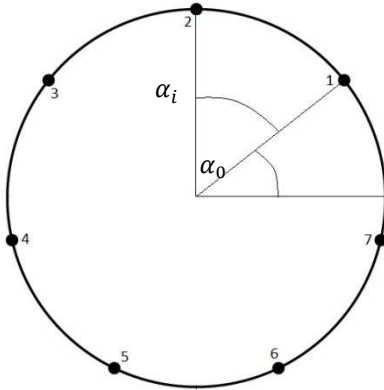
$$\alpha_i = \alpha_0 + \frac{2\pi}{M}(i-1) \quad (i=1, 2, \dots, M) \quad (8)$$

where:

$\alpha_i \dots$  is an angle of "i" sensor

$\alpha_0 \dots$  is difference between first sensor and zero angle

$M \dots$  is the number of sensors.



**Fig. 2** Dislocation of 7 sensors around the circle

For another matrices, where formula (8) is not applicable but matrices are capable to fulfill conditions of minimization of trace of CRB, the following formula can be applicable [7]:

$$\begin{aligned} \sum_{i=1}^M \cos(\alpha_i) &= 0 & \sum_{i=1}^M \sin(\alpha_i) &= 0 \\ \sum_{i=1}^M \cos(2\alpha_i) &= 0 & \sum_{i=1}^M \sin(2\alpha_i) &= 0 \end{aligned} \quad (9)$$

Table 1 shows an example of dislocation of seven sensors where formula (8) is not applicable, but formula (9) is.

**Table 1** An example of sensor dislocation

Sensor	Angle $\alpha_i$	$x_i = \cos(\alpha_i)$	$x_i = \sin(\alpha_i)$	$x_i = \cos(2\alpha_i)$	$x_i = \sin(2\alpha_i)$
1	0°	1	0	1	0
2	53°	0,601	0,798	-0,277	0,961
3	100°	-0,174	0,985	-0,941	-0,342
4	158°	-0,927	0,375	0,718	-0,695
5	202°	-0,927	-0,375	0,718	0,695
6	260°	-0,174	-0,985	-0,941	0,342
7	307°	0,601	-0,798	-0,277	-0,961
$\Sigma$		0	0	0	0

Both solutions are applicable only in the case we have considered earlier, so that sensors are dislocated around the circle and target is right in the middle.






Table 1 shows that matrix of sensors meets conditions in formula (9) and represents the group of sensors, whose dislocation is optimized for the most accurate estimate of target's position.

## 5 SENSOR DISLOCATION OPTIMIZATION IN 3D AREA

In case of sensor dislocation in 3D area we can focus our research on solutions, in which each individual sensor is dislocated symmetrically in same distance from target.

Let assume that the target is positioned in the middle of a sphere and all sensors are placed on its surface. It is known from geometry that there are exactly five relative dislocations of sensors, which are able to meet condition of symmetry. All faces of those solids are made by regular polygons – so called Platonic solids [8].

**Table 2** Solids and their nodes

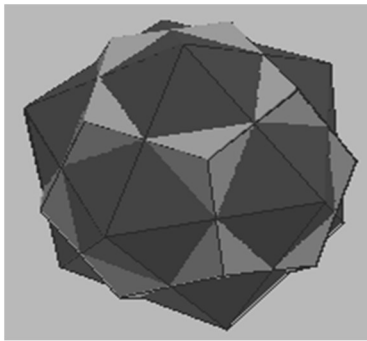
Name	Shape	Nodes $M=v$
Tetrahedron		4
Octahedron		6
Cube		8
Icosahedron		12
Dodecahedron		20

All vectors  $\bar{g}_i$  are heading from the middle of geometric solids into their nodes. The count of solids is equal to the count of sensors in sensors network. For all those solids mentioned above conditions (9) are valid.

Likewise, in case of dislocation in 2D area, Platonic solids, which are arbitrarily reversed from the center, also meet conditions (9).

Superpositions of each individual platonic solid meet conditions (9) either. In this case, the count of nodes (sensors) are summed.

A new matrix is made of multiple  $D \times M$  matrices. If for each  $D \times M$   $g = [g_1 \dots g_M]$  conditions (9) are valid, then for resultant matrix  $M = \sum_{k=1}^K M_k$  with sensors  $g = [g_1 \dots g_K]$  (9) are valid either.



**Fig. 3** Superposition of icosahedron and dodecahedron

In case we need to dislocate different number of sensors than it is number of available Platonic solids or their superpositions, it is necessary to apply the theory of spherical codes.

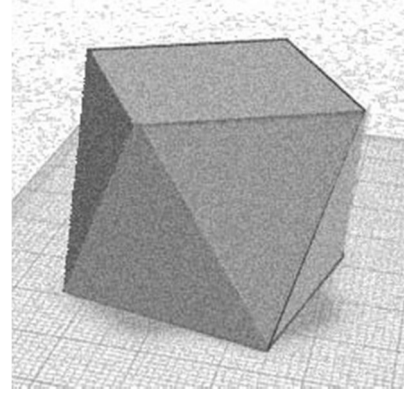
The problem can be enunciated as the necessity to dislocate a certain number of nodes over the sphere's surface, while achieving the condition of maximization of minimal distance between each other. The maximum distance is known as covering radius and resulted configuration as spherical code.

Two points on the surface of the sphere must be positioned right on the intersection of the sphere and straight.

Solutions in case of count of 4, 6, and 12 points are equal for the platonic solids. In case of 8 points, the solution is not the cube, but so called the square antiprism, where above face of the cube is rotated by 45 degrees, while the bottom face does not change its position.

Each individual solids, up to  $M=130$  nodes, are mentioned in [8].

Even though the dislocation of sensors in nodes does not form min CRB, it is being approximate. This theory can be effectively applied in practice while creating an optimal dislocation of various numbers of sensors.



**Fig. 4** Square antiprism as an example of spherical code

## 6 SIMULATIONS

We assume that our sensors are carried by UAV, they are able to communicate within the network and are capable of moving in the trajectory represented by perimeter of the circle. Second, we assume that all sensors have the same error deflection and are able to move in the same speed. The target followed by sensors is situated in the middle of the circle.

If we assume that sensors are deployed equally around the circle perimeter, then the formula (6) can be replaced as follows:

$$\sum_{i=1}^M c_i^2 g_i g_i^T = \frac{1}{D} \sum_{i=1}^M c_i^2 I_D \quad (10)$$

where:

$c_i \dots$  is error variance of the sensor  $i$ ,

$g_i \dots$  is vector pointing from the target to the sensor  $i$ ,

$M \dots$  is the number of sensors,

$D \dots$  is dimension,

$I_D \dots$  is matrix of which diagonal values are equal to 1.

If previous equality is valid, then we can assume that the sensors are dislocated optimally and the minimum value can be expressed as following:  $\sum_{i=1}^M c_i^2 g_i g_i^T$ .

In the beginning of the simulation, each individual unit was dislocated around the perimeter of the circle. The coordinates of each individual sensor  $g_i$  are expressed by  $[\cos \alpha_i, \sin \alpha_i]^T$ .

In the first step, the uniform array of optimal sensor dislocations was rotated around the center in order to identify the minimum time value necessary for sensors re-dislocation from initial location to the optimal.

In the second step, based on the formula (10) and considering criteria reflecting the minimum necessary time for initial configuration changes to the optimal setting, the sensors were re-dislocated to the optimal locations.

$\Delta$  is the variance between current value  $\sum_{i=1}^M c_i^2 g_i g_i^T$  and its minimum  $\frac{1}{D} \sum_{i=1}^M c_i^2 I_D$ . If the dislocation is optimal, the  $\Delta$  is equal to 0.

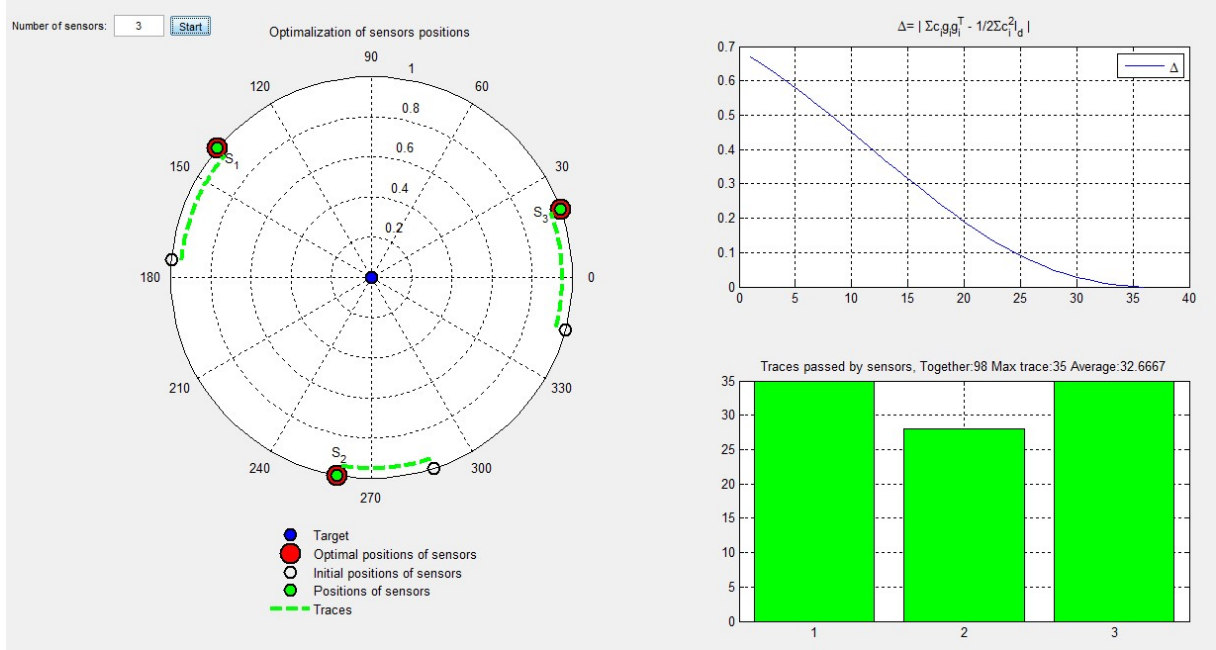


Fig. 5 The simulation of optimal dislocation of 3 sensors

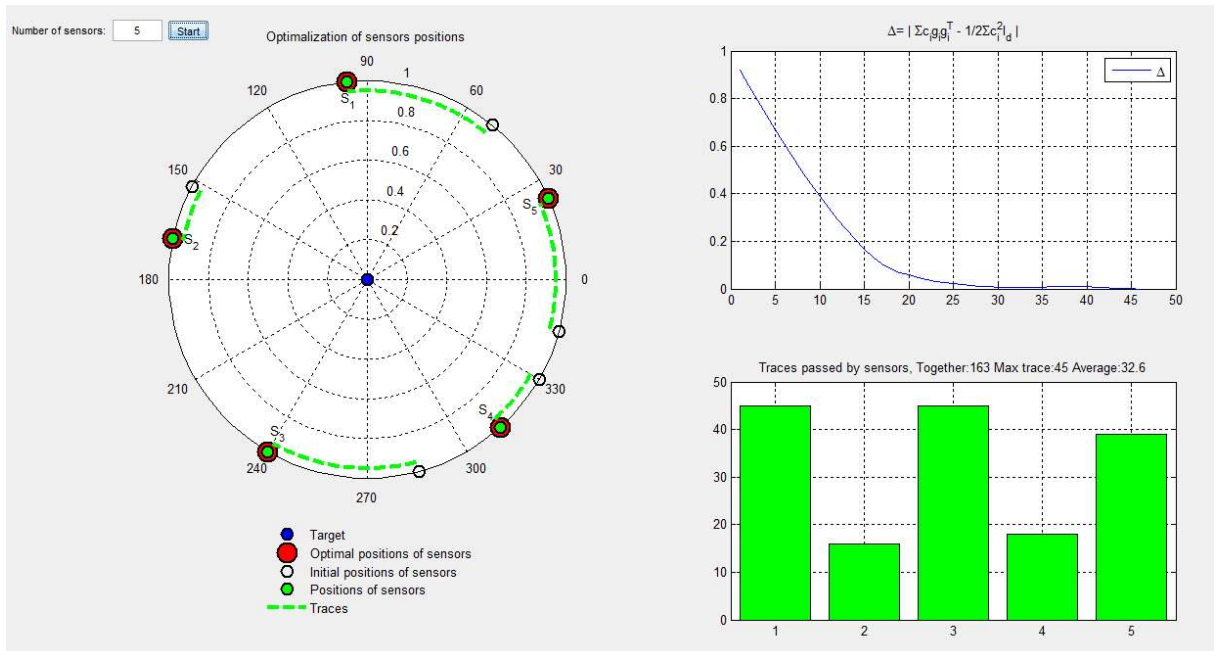


Fig. 6 The simulation of optimal dislocation of 5 sensors

## 7 CONCLUSION

An estimate of the target position is difficult process, which is influenced by several input values, e.g. distance between sensor and the target and the distance between each pair of sensors in case of sensor network installed.

In this paper we were dealing with the optimization strategy of sensors and the target dislocation. Both sensors and target were dislocated in 2D or 3D area around the circle (in case of 3D on sphere surface) and target was situated right in the middle.

It was presented that Platon solids create minimum CRB and therefore represent the collection of nodes, where individual units of sensor network should be dislocated. However, in practice it is more appropriate to use solids of spherical codes, even though they do not create minimum CRB, but are approximating. This solution is suitable for sensor network, which can consist of even 130 units.

The previous simulation validates our mathematical assumptions regarding the optimal sensor network dislocation in 2D while achieving the most accurate estimation of the target. The minimum time requirement condition for initial UAV configuration change to the optimal was also met.

Further on, it would be useful to focus on cases, e.g. sensors are set only in a certain, predetermined cone of observation area (to avoid being compromised or in cases where observation area is inflicted by obstacles).

Both methods require mathematical description/formulation of 3D area since it is the most accurate and reflects real conditions.

The main goal of the previous mathematical study is to determine the appropriate mathematical model, based on which we will be able to define the dependency of the final information entropy from the current sensor's matrix dislocation.

## References

- [1] CARTER, G. C. ed.: Special issue on time delay estimation. In *IEEE Trans. Acoust. Speech, Signal Processing*, vol. 29, June 1981.
- [2] CARTER, G. C., ed.: Coherence and Time Delay Estimation. In *IEEE Press*, 1993.
- [3] TORRIERI, D. J.: Statistical theory of passive location systems. In *IEEE Trans. Aerosp. Electron. Syst.*, vol. 20, p.183-197, 1984.
- [4] SPIRITO, M. A.: On the accuracy of cellular mobile station location estimation. In *IEEE Trans. Veh. Technol.*, vol. 50, p.674-685, 2001.
- [5] YANG, B., SCHEUING, J.: Cramer-Rao bound and optimum sensor array for source localization from TDOA. In *IEEE ICASSP*, 2005, vol. 4, p. 961-964.
- [6] YANG, B.: Different sensor placement strategies for TDOA based localization. In *Proceedings of the 2007 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 2, pp. II-1093-II-1096, Apr. 2007.
- [7] ISAACS, J. T., KLEIN, D. J., HESPAH, J. P.: Optimal sensor placement for time difference of arrival localization. In *Proceedings of the 48<sup>th</sup> Conference on Decision and Control* (pp. 7878-7884), Shanghai, China, 2009.
- [8] SLOANE, N. J. A., HARDIN, R. H., SMITH, W.D.: Spherical codes. Available at: <http://www.research.att.com/njas/packings/>.
- [9] ZHAO, S., CHEN, B. M., LEE, T. H.: Optimal sensor placement for target localisation and tracking in 2D and 3D. In *International Journal of Control*, 2013, 86(10): 1687-1704
- [10] IEEE Trans. Aerospace and Electron. Systems. In *Statistical theory of passive location systems*, vol. 20, p.183-198.
- [11] FARINA, A., STUDER, F. A.: *Radar data processing, Hertfordshire*. UK : 1985.
- [12] REN, W., CAO, Y. C.: Distributed Coordination of Multi-agent Networks. In *New York: Springer 2011*.
- [13] OUSINGSAWAT, J., CAMPBELL, M. E.: Optimal Cooperative reconnaissance using multiple vehicles. In *Journal of Guidance, Control and Dynamics*, 2007, p.122-132.
- [14] HU, J. W., XU, J., XIE, L. H.: *Cooperative search and exploration in robotic networks. Unmanned systems*, 2013, p. 121-142.

Eng. Peter RINDZÁK  
Ministry of Defence of the Slovak Republic  
Kutuzovova 8  
832 47 Bratislava  
Slovak Republic  
E-mail: peter.rindzak@gmail.com

**Eng. Peter Rindzák** – was born in Humenné, Slovakia in 1983. He received his M.Sc. (Ing.) at the Academy of the Armed Forces of General Milan Rastislav Štefánik in Liptovský Mikuláš. His research interests are modeling, simulation, measurement, optimal deployment of sensor arrays and information entropy.



# SWOT ANALYSIS TOOL FOR RESTRUCTURING OF SELECTED ORGANIZATIONS SECURITY AND PUBLIC ORDER

Mariusz ROZWADOWSKI

**Abstract:** Transformation of social and economic, with which we have to deal with in recent years in Poland, apart from the positive aspects, has generated a lot of negative phenomena, new types of crime. This situation compels the police, as the basic organization of the subsystem of security and public order to improve efficiency. Improving the effectiveness of that determines the effectiveness of the whole system of security and public order and the delivery of services provided by this organization in the field of security and public order. The paper presents definitions, determinants and models of safety management as well as the positive and negative phenomena associated with the method of SWOT in the selected units of the Police.

**Keywords:** qualitative management, police, security, public safety, SWOT.

## 1 ADMISSION

An element isolated from the public security subsystem designed to ensure security and public order is the police. The activities of this organization is to provide public services in ensuring the security of citizens. It is desirable, therefore, permanently making efforts to improve its activities in all areas. The result of such action would be fuller achievement of the objectives and functions to which these services has been appointed, effective use of financial resources, raising the level of social assessment of the effectiveness of their activities and increase employee satisfaction with their work<sup>1</sup>. Changes in the existing method of managing the organization should aim at achieving the objectives of the organization, rationalize its operations while a fuller meeting citizens' expectations<sup>2</sup>. These changes can be implemented by improving the organization, identifying key processes, as well as the modification of the methods specific tasks. The need for having to make changes in the functioning of public organizations<sup>3</sup> is still valid, because an attempt was made to adapt the SWOT analysis to restructure the selected unit of the Regional Police Headquarters in Krakow.

## 2 TYPES AND FORMS OF ORGANIZATION

Organization (etymologically derived from the Greek. Organon, Latin. Organum specialized part that serves a function in total)<sup>4</sup>, ambiguous and

interdisciplinary concept in the field of management science, sociology, psychology. In management science, and above all, in their sub discipline sciences organizations, usually it takes three meaning of the organization, namely<sup>5</sup>:

1. Organization in the sense of substantive - as an entity for the complex with related parts. In this sense, the concept of the organization is synonymous with the concept of the institution (e.g. This organization is highly profitable).
2. Organization in the sense of a functional - as the process of making things complex. In this sense, the concept of the organization is synonymous with the concept of the organization (eg. The organization of sporting events is the domain of the activities of our committee).
3. Organization in the sense of attribute-based - as a set of characteristics for things organized. In this sense, the concept of the organization is synonymous with the concept of organized (eg. In this house there is excellent organization).

Analyzing the literature it can be concluded that among the organizations non-profit, there are two different types of entities:

- public organizations,
- non-governmental organizations (private).

Public organizations are non-profit organizations created at the initiative of the state administration or local government entities, which are dependent on the founding bodies carrying out a public service activity, or one that is available to every citizen of the country. Public organizations provide service activities for the benefit of society, carry out tasks defined by the state in the relevant normative acts and are financed from public funds. In this group of organizations are public institutions of culture, health, education, science, local government, social justice, security / example. Police / national defense. Funding of public organizations from the state budget and budgets of local government units

<sup>1</sup> ZUBRZYCKI, A.: Doskonalenie jakości pracy jednostki policji-wybrane metody, „Zarządzanie Publiczne”. In *Zeszyty Naukowe Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego*, 2006, nr 2, s.66.

<sup>2</sup> KOŻUCH, A., KOŻUCH, B., PLAGO, A.: *Podstawy zarządzania organizacjami*. Kraków : Fundacja Współczesne Zarządzanie, 2005, s. 180.

<sup>3</sup> KOŻUCH, B.: *Specyficzne cechy organizacji publicznych*. Białystok : Fundacja Współczesne Zarządzanie, 2005, s. 34.

<sup>4</sup> BIELSKI, M.: *Organizacje – istota, struktury, procesy*. wyd. II, Wyd. UŁ, Łódź 1997, s. 68.

<sup>5</sup> *Podstawy nauki o organizacji*, red. MAREK, S., BIAŁASIEWICZ, M., Warszawa : PWE, 2008, s. 15.

reduces the area of autonomy directions of spending the funds received, as well as the need to manage on the basis of a highly formalized procedures<sup>6</sup>.

Public organizations, on which rests the protection and management of the security of citizens carrying out their tasks based on the existing legal norms must also be taken into account; the sense of security of the citizens in the area, determinants and security models. Accordingly diagnosed determinants of security management and the application of appropriate security models makes it possible to characterize the existing threats and their impact. It also allows creation forecasts safety and build a system of early warning. On the basis of the models developed procedures to identify risks. You can also develop the skills and habits to identify hazards, which in turn provides opportunities to avoid certain risks or minimize the damage.

### 3 DEFINITIONS AND DETERMINANTS SAFETY MANAGEMENT

All socio-economic formations treat security as one the most important values in human life. The man with the development of civilization creates for himself and other growing threats, because safety, as the value is appreciated by both individuals and whole societies.

Leading the discussion ontological, epistemological and axiological on the essence of which is security, J. July states, "... the construction of power refers to the man and only to him, but the recall of the human being in three other dimensions"<sup>7</sup>:

- the life of another human being,
- life of a set of people who formed a social group (society),
- the life of the human species (humanity).

Personal security and individual sense of security becomes the most important, constitutional value<sup>8</sup>. Security is the ability for creative activity of the subject and indicates the status of objective involving no threat, perceived subjectively by individuals or groups<sup>9</sup>. Some authors distinguish between positive understanding of safety, as the formation of certain of survival, possession and freedoms of others and development entity, as the understanding of the negative defining security as

the absence of threats<sup>10</sup>. Safety is the desired state characterized by a sense of confidence and lack of danger in which man has a foothold in the community, well-functioning legal system and the apparatus of state power. No risk is objective and can be diagnosed and tested to determine the factors threatening the protected values. In contrast is the second element of the concept of security - a sense of confidence. It has, in fact, subjective and results directly from the actual threats, but it is also conditional on construction of mental man, his emotional state and external factors<sup>11</sup>.

The concept of safety in everyday language means a condition in which the individual has a sense of confidence back in the second person or a well-functioning legal system.

The opposite of security is a state of emergency being<sup>12</sup> the primary determinant. According to L. F. Korzeniowski threat is a potential cause of an unwanted condition. Threats category are not spontaneous, always refer to some entity<sup>13</sup>. They have for this entity destructive. These risks may cause harmful consequences for the body. To generate threats are needed in the opportunities that lie in the same body, which relate to its surroundings or entity relationships with the environment<sup>14</sup>.

Through safety management can eliminate the impact of determinants, or so far to minimize the likelihood of their impact on the situation that it is difficult to be regarded as dangerous in the data created by the operator of the conditions.

Undoubtedly, important for security management is the ability to analyze risk. It should be noted that the risk is sometimes defined differently depending on the purpose of the author.

The risk is objectified uncertainty of any adverse events, the risk varies with uncertainty, and not the degree of probability<sup>15</sup>. According to W. F. Samuelson and S. G. Marx<sup>16</sup> risks or uncertainties interchangeably occurs when there is more than one possible outcome of our decision. For further analysis adopted by L. F. Korzeniowski, that risk is

<sup>6</sup> KOWALCZEWSKI, W.: *Zarządzanie organizacjami w teorii i praktyce*. Warszawa : Difin, 2008. s. 77-78.

<sup>7</sup> LIPIEC, J.: *Świat wartości*. Kraków : Wydawnictwo Fall, 2001. s. 76.

<sup>8</sup> IV poprawka (Karta Praw) z roku 1791 roku do Konstytucji Stanów Zjednoczonych Ameryki.

<sup>9</sup> KORZENIOWSKI, L.: *Zarządzanie bezpieczeństwem. Rynek, ryzyko, zagrożenia, ochrona*. Kraków : PSB, 2000. s. 437.

<sup>10</sup> NEY, J. S. Jr.: *Problemy badań nad bezpieczeństwem*. Sprawy Międzynarodowe, 1989, nr 6. s. 51-64.

<sup>11</sup> CZOP, A.: *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce*. Katowice : 2014. s. 33.

<sup>12</sup> DUNAJ, B.: (red. nauk.): *Popularny Słownik Języka Polskiego*. Warszawa : 1999. s. 30.

<sup>13</sup> KORZENIOWSKI, L. F.: *Securitologia - Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków : EAS, 2008. s. 58.

<sup>14</sup> KORZENIOWSKI, L.: *Zarządzanie...* op.cit. 2001. s. 21.

<sup>15</sup> WILLET, A.H.: *The Economic Theory of Risk Insurance*. Philadelphia : 1951, s. 6.

<sup>16</sup> SAMUELSON, W. F., MARKS, S. G.: *Ekonomia menedżerska*. Warszawa : PWE, 1998. s. 32.

a function of hazard and the probability of its occurrence<sup>17</sup>.

Risk management is the identification, measurement, control and manage the risk in order to minimize and protect against risk<sup>18</sup>.

Risk management can be divided into the following stages:

- identification consisting in determining what risks and to what period is threatened by the entity,
- quantification, or measurement using different methods depending on the type of risk and the size of the potential damage,
- decide the conditions where it is possible to determine the risks for the expected result and the probability of a particular outcome is known or possible to estimate,
- control designed to examine the effectiveness of projects undertaken to reduce risk.

The value of the security changes over time, as ambient conditions change, and man and society can change. It should, therefore be concluded, that these changes must be observed and must influence the change in the level of security through the promotion of sustainable security<sup>19</sup>, it is possible to create a reasonably safe society<sup>20</sup>.

Public safety is a very broad and difficult to define. The reason for this is, inter alia, the growth of social life. There are new threats, changing the law, all these elements influence the shaping of public safety. Due to the wide range of risks and impacts on the public safety, concepts and understanding of safety and security, adjusts to the real dangers present in everyday life.

E. Ura the concept of public security determines the state in which the general public to an unspecified individual, who lives in the state and society, there is no danger, regardless of what would have been its source. E. Ura believes that the protection of public safety belongs to the state, which outlines the boundaries of safety and speaks, which is inconsistent with the safety and interferes or may interfere with normal functioning of the state.

Public safety is one of the subsystems widely understood state security system referred to as internally coordinated set of elements of organizational, human and material aimed at countering any threat to the state, and in particular the political, economic, psychosocial, environmental

and military<sup>21</sup>. Its most important goal is to ensure order against phenomena criminal, environmental hazards and to ensure public order<sup>22</sup>.

Systems included in the subsystem of public safety, including the police, are responsible for the tasks in the maintenance of security and public order. Express constitutional duty of the state to ensure the safety of the country/realization of art. 146 Constitution<sup>23</sup>. For the security system as a whole, as well as shaping the individual subsystems and create specific models of their operation corresponds to the state as an institution. This is reflected in the provisions of the Constitution of the Republic of Poland/Polish<sup>24</sup>. Ties and organizational rules about the structure of the state, unions and mutual relations between its elements, and above all, the way of public financing and the legally defined purpose and scope of the tasks of the safety tend to consider public safety for the system - a unified, organized and harmonized whole<sup>25</sup>.

#### 4 SWOT ANALYSIS OF GENESIS, FACTORS AND CONDITIONS

SWOT analysis is one of the basic methods of strategic analysis of the company. The method name is an acronym of English words strengths (strong side), weaknesses (weaknesses), opportunities (opportunities or potential occurring in the environment), threats (threats likely or existing in the environment). It can be used for enterprise-wide or in individual areas of its operation, eg. Marketing, finance, manufacturing, etc. The basic assumptions of the SWOT analysis were developed in the 50s and 60s of the twentieth century by scientists and business consultants working in the Harvard Business School, and described in "Business Policy".

In the years 1960-1970 the Stanford Research Institute conducted the study on behalf of the largest US companies, whose aim was to identify ways to improve strategic planning processes and to avoid errors in planning. The result of this research was to develop four groups of factors determining the effects of planning activities:

- factors of good (satisfactory) in the present (Satisfactory),

<sup>17</sup> KORZENIOWSKI, L.F.: *Menedżment*. Kraków : EAS, 2010. s. 180.

<sup>18</sup> DZIAWGO, D.: Zarządzanie ryzykiem w banku komercyjnym. In *Bankowość. Podręcznik dla studentów*. Poznań : WSB, 1999. s. 351-398.

<sup>19</sup> WELANDER, G., SVANSTROM, L., EKMAN, R.: *Safety Promotion and Introduction*. Revised edition. Stockholm : Krolinska Institutet, 2004. s. 10.

<sup>20</sup> Ibidem, s. 11.

<sup>21</sup> *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa : AON, 2002. s. 139.

<sup>22</sup> LISIECKI, M., KWIATKOWSKA-BASAŁAJ, B.: Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia. In *Zarządzanie bezpieczeństwem*. (red. nauk.) Tyrała P., Kraków : Wydawnictwo Profesjonalnej Szkoły Biznesu, 2000. s. 57-58.

<sup>23</sup> *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz. U. z 1997. nr.78, poz. 483).

<sup>24</sup> Dz.U. z 1997 r. Nr 78, poz. 483 z późn. Zm.

<sup>25</sup> SKRZYDŁO, W.: *Ustrój polityczny RP w świetle Konstytucji z 1997r.* Kraków : Zakamycze, 1998, s. 114-115.

- factors of good (positive) in the future - opportunities (Opportunity),
- bad factors in the present - Error (Fault),
- bad factors in the future - threats (Threat).

SWOT analysis basically has not changed since its inception. Today it is in the curricula of all management courses as the primary method of analysis of strategic enterprises and organizations. Its implementation requires the involvement of many people in leadership positions but also specialists at lower levels. Is carried out by an external consultant or employee with the right skills. The basic stages of SWOT analysis are as follows:

1. Stage in which the explanation of all involved employees why efforts are analytical (they are usually carried out prior to the essential strategic changes).
2. This step is necessary to ensure a uniform approach to the analysis of the team participants.
3. Development of individual lists of strengths/weaknesses, opportunities and threats - each team member yourself first draw up a list of all the factors considered by it to be relevant to the strategic position of the company.
4. Lists the individual integration, the development of common matrix SWOT, more coherent terminology, selection factors less important.

5. Discussion and sincere dialogue between all participants involved in the study, in terms of the conclusions of the list of factors presented an integrated, looking at issues from different points of view.
6. Develop plans and options for action in the future, includes the presentation of the initial strategy, which will then be substantiate the management of the organization and implemented.

In order to prepare a SWOT analysis, you must identify and classify all factors affecting the current and future situation of the company (its position in the market). The analysis uses two basic criteria for classification:

- factors external to the organization (affecting both positive and negative) identified using methods such as scenario analysis, PEST method, etc.
- internal conditions (positive and negative) - characterizing the state of the company across all major groups of resources (personnel, financial resources, knowledge, technical resources, etc.).

The combination of the above mentioned groups of factors emerge four specific analytical categories, filling the fields SWOT matrix (Figure 1):



Fig. 1 Scheme matrix made during the SWOT analysis

- Strengths are internal factors-positive - strengths, ie. Values of the organization, which positively distinguish it in the environment and from the competition, they are called. key success factors enabling organizations to adapt it to the changing conditions of the market environment,
- Weaknesses organizations are internal factors-negative. As a consequence of resource constraints and insufficient qualifications of

employees and management. Weaknesses are also connected with all other areas of functioning, which limit the efficiency of its operations and respond to changing customer requirements and competitors' activities,

- Opportunities (external positive) - are any existing or anticipated processes, trends and phenomena occurring in the environment of the organization, which properly used can become

the impetus for its development and help to weaken the impact of possible emerging risks,

- Threats (external negative) - that all processes, trends and phenomena occurring in the environment of the organization, which constitute or may constitute a barrier to the development of the organization, hinder its operation, increase operating costs or may lead to the collapse of the company.

As a result of the analysis is obtained four separate list of factors, ie strengths of the organization (to be strengthened), weaknesses (which you have to compensate), opportunities (to be used) and threats (to be avoided).

Most management methods and techniques over time from use and replaced with new solutions, the SWOT analysis, after more than half a century has lost nothing of its popularity. Firstly, this is because it can be used in any situation, flexibly adapts to the specifics of each organization.

Secondly, it gives management the ability to quickly and systematically collect information on the most important factors characterizing the situation of the organization. Timeless SWOT analysis is mainly due to its simplicity and wide range of applications. It is used in non-profit organizations, public administration institutions, informal groups as a first step plan more or less complex operations.

## 5 SWOT ANALYSIS ATTEMPT TO APPLY FOR RESTRUCTURING OF SELECTED UNITS POLICE IN KRAKOW

In 2005, the Provincial Police Headquarters in Krakow appointed the Quality Management /the team included officers command of the provincial police in Krakow and author of the publication/. The team's objective was to analyze the functioning of the various departments of the Regional Police Headquarters. The team is to carry out research used the SWOT analysis. It was found that because of its advantages is used in all areas of strategic planning as a universal tool for the first phase of strategic analysis, it can be used in the first stage of quality management in the Police Headquarters. The essence of the SWOT analysis is to answer the following questions<sup>56</sup>:

- What particular is characterized by the organization?
- What is its strength?
- What is the weakness of the organization in the environment?
- What are the chances possible to use to strengthen the position of the company?

- What hazards may limit or hamper the functioning of the organization or sub-systems?

Following the recommendations of the SWOT in all departments of the Regional Police Headquarters /Headquarters/ in Krakow, an analysis of the strengths, weaknesses, threats and opportunities diagnosed. Summary of strategic factors SWOT analysis for sub-division of the Independent Anti-Terrorist Police Regional Police Headquarters Cracow shown in Table 1.

The most important weaknesses ATPR include: uncertainty of positions on the announced structural changes constantly, weak level of preparation tasks by other cells (eg. Low object recognition), deficiencies in equipment.

Strengths of this organization are: a high level of training and skills possessed by the police Anti-Terrorist Police Regional /ATPR/, fit, independent instructors, commitment and mobility policemen. As the threat raised: unsuited to the realities of the rules, in some cases, simply do not exist, the lack of an agreement with the health service regarding. Use ambulance resuscitation, the structure of ATPR is imposed by Police Headquarters (regional conditions are different), the provisions general police eg. In terms of shooting do not fit the realities associated with training services counterterrorism eg. the provisions concerning: use sharpshooter, no police regulations concerning the use of a helicopter, the structure of Anti-Terrorist Police Regional /ATPR/ is imposed by Police Headquarters.

Opportunities for this unit by officers were: the creation of task forces on solid personal setup would make it easier to perform tasks and planning, training and holidays - greater effectiveness of training, the exclusion of police activities in the area covered by provisions relating to civil eg. tenders for specialist equipment, employment of medical and equipping ambulance resuscitation.

Using the SWOT analysis to organizational changes did not bring changes in the structure of the organization and the expected effects, despite the obvious potential benefits. This was associated primarily with the uncertainty cast occupied by police posts and the persistent structural changes. A very important from the point of view of the specificity of action ATPR was weak level of preparation, by other police departments, tasks ATPR (eg. Low object recognition). Significant external factors for this unit were deficiencies in equipment specialist characteristic of the formation, unsuited to the realities of the legal provisions (eg. The rules on the use of sniper or use the helicopter). The organizational structure of ATPR is imposed by the Police Headquarters while regional conditions are quite different, which makes it not getting to the needs of the province of Malopolska. These factors aroused resistance and discontent among officers ATPR.

<sup>56</sup> SZCZEPAŃSKA, K.: *Metody i techniki TQM*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej. 2009, s. 199.

**Table 1** Factors strategic SWOT analysis of the sub-division of the Independent Anti-Terrorist Police Regional Police Headquarters

Weaknesses	Strengths	Threats	Chances
<ol style="list-style-type: none"> <li>1. Uncertainty positions on the announced structural changes constantly.</li> <li>2. Current structure make it difficult to schedule tasks, but also leave and training.</li> <li>3. Poor level of preparation tasks by other police cell.</li> <li>4. Deficiencies in equipment hardware.</li> </ol>	<ol style="list-style-type: none"> <li>1. High level of training and skills possessed by the police ATPR.</li> <li>2. Athletic, independent instructors.</li> <li>3. Commitment and mobility policemen.</li> </ol>	<ol style="list-style-type: none"> <li>1. Living up to the realities of the rules, in some cases, simply do not exist.</li> <li>2. Lack of an appropriate agreement with the health service regarding. Use of resuscitation ambulance.</li> <li>3. Structure of Anti-Terrorist Police Regional is imposed by Police Headquarters.</li> <li>4. The provisions of general police. In the field of fire do not fit the realities associated with training services anti-terrorist.</li> </ol>	<ol style="list-style-type: none"> <li>1. Creation of a section of solid compositions of personal.</li> <li>2. Exclusion Anti-Terrorist Police Regional activities in the area covered by provisions of general police.</li> <li>3. Employment doctor and equipping ambulance resuscitation owned by the prevention branch police.</li> </ol>

Source: Own calculations based on data from the Audit Regional Police Headquarters in Krakow.

Analysis of the SWOT analysis has been carried out in all departments of Provincial Police Headquarters /PPH/. External company conducted a proper audit. After successful completion of the Provincial Police Headquarters in Krakow received in 2005. ISO 9001 certification Based on the SWOT introduces a number of new procedures in the implementation of official tasks. However, the procedure for carrying out certain activities, often lengthened their performance, caused preparing additional documentation. This aroused the opposition and dissatisfaction of employees, besides the certificate must be updated annually by the audit, which raised significant costs for Provincial Police Headquarters. By decision of the Voivodship Police Commander in Cracow in 2006, the annual audit was abandoned and the PPH lost its ISO certificate. The procedures developed by SWOT were also discontinued. From 2006 until now, no quality management is used in any police unit of the Małopolskie voivodship.

## 6 CONCLUSION

Social and economic change, with which we have to deal with in recent years in Poland, apart from the positive aspects, they have generated a lot of negative phenomena, new types of crime,

otherwise we can observe an increase in the legal awareness of citizens. These elements are forcing the police, as the basis for the organization of a subsystem of security and public order to improve efficiency. Her improvement determines the effectiveness of the system and keep pace with the rising expectations of consumers - citizens of the Republic of Poland. Existing circumstances necessitate the constant improvement, to organize the effective implementation of the main /achieve a state in which there will be committed offenses/. It is necessary, therefore making constant improvement activities in all areas of activity Police. Positive changes in the existing management organizations, public safety and order, should aim, therefore, to optimize their operations, proper implementation of the functions and objectives of the organization, improve the efficiency of services provided at the same time meeting the expectations of 'clients' internal and external. This can be achieved by improving the organization, ensuring the achievement of its objectives and functions, modification of processes key, as well as ways to improve the implementation of tasks. It is important to use management methods were adapted to the specific functioning of the organization and its individual components.

## References

- [1] BIELSKI, M.: *Organizacje – istota, struktury, procesy*. wyd. II, Wyd. UŁ, Łódź 1997.
- [2] CZOP, A.: *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce*. Katowice : 2014.
- [3] DUNAJ, B.: (red. nauk.) *Popularny Słownik Języka Polskiego*. Warszawa : 1999.
- [4] DZIAWGO, D.: Zarządzanie ryzykiem w banku komercyjnym. In *Bankowość*. Podręcznik dla studentów. Poznań : WSB, 1999.
- [5] IV poprawka (Karta Praw) z roku 1791 roku do Konstytucji Stanów Zjednoczonych Ameryki.
- [6] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997. nr. 78, poz. 483).
- [7] KORZENIOWSKI, L. F. I.: *Securitologia - Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków : EAS, 2008.
- [8] KORZENIOWSKI, L.F.: *Zarządzanie bezpieczeństwem. Rynek, ryzyko, zagrożenia, ochrona*. Kraków : PSB, 2000.
- [9] KORZENIOWSKI, L. F.: *Menedżment*. Kraków : EAS, 2010.
- [10] KOWALCZEWSKI, W.: *Zarządzanie organizacjami w teorii i praktyce*. Warszawa : Difin, 2008.
- [11] KOŻUCH, A., KOŻUCH, B., PLAGO, A.: *Podstawy zarządzania organizacjami*. Kraków : Fundacja Współczesne Zarządzanie, 2005.
- [12] KOŻUCH, B.: *Specyficzne cechy organizacji publicznych*. Białystok : Fundacja Współczesne Zarządzanie, 2005.
- [13] LEAMED, A., CHRISTENSEN, C., ANDREWS, R. S., GUTH, D.: *Business Policy: Text and Cases*, Homewood. Illinois : Irwin, 1965.
- [14] LIPIEC, J.: *Świat wartości*. Kraków : Wydawnictwo Fall, 2001.
- [15] LISIECKI, M., KWIATKOWSKA-BASAŁAJ B.: Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia. In *Zarządzanie bezpieczeństwem*. (red. nauk.) Tyrała P., Kraków : Wydawnictwo Profesjonalnej Szkoły Biznesu, 2000.
- [16] NEY, J. S. Jr.: Problemy badań nad bezpieczeństwem. In *Sprawy Międzynarodowe*, 1989, nr 6.
- [17] *Podstawy nauki o organizacji*. red. MAREK S., BIAŁASIEWICZ, M.: Warszawa : PWE, 2008.
- [18] SAMUELSON, W. F., MARKS, S. G.: *Ekonomia menedżerska*. Warszawa : PWE, 1998.
- [19] SKRZYDŁO, W.: *Ustrój polityczny RP w świetle Konstytucji z 1997*. Kraków : Zakamycze, 1998.
- [20] *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa : AON, 2002.
- [21] SZCZEPAŃSKA, K.: *Metody i techniki TQM*. Warszawa : Oficyna Wydawnicza Politechniki Warszawskiej, 2009.
- [22] WELANDER, G., SVANSTROM, L., EKMAN, R.: *Safety Promotion and Introduction*. Revised edition. Stockholm : Krolinska Institutet, 2004.
- [23] WILLET, A. H.: *The Economic Theory of Risk Insurance*. Philadelphia, 195.
- [24] ZUBRZYCKI, A.: *Doskonalenie jakości pracy jednostki policji-wybrane metody*, „Zarządzanie Publiczne”. Zeszyty Naukowe Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego, 2006.

Dr. Mariusz ROZWADOWSKI, PhD.  
 Krakow University of Economics  
 Rakowicka Street 27  
 31-510 Krakow  
 Poland  
 E-mail: rozwadom@uek.krakow.pl

**Dr. Mariusz Rozwadowski, PhD.** - was born in Krakow in 1960. In 1986 graduated from the Cracow University of Economics with a degree in economics. In 1992 completed postgraduate studies at the Police School in Szczytno. He is police major in a resting state. Since 2007 have been working at the Cracow University of Economics as a Plenipotentiary for the Protection and Protection of Classified Information. In 2011 defended his Ph.D. thesis at the Cracow University of Economics and obtained a PhD in Economics from the discipline of management science. His research interests are focused on: Security management, human resources management in security and public order organizations, crisis management, business intelligence. He is an expert and examiner in the profession of property protection and also a member of the European Association for Security, the National Association for the Protection of Classified Information.

## UKRAINE IN DIRE STRAITS: THE CONUNDRUM OF ENSURING ITS MILITARY SECURITY

Oleg POSHEDIN, Maryna CHULAIEVSKA

**Abstract:** This article examines how Ukraine, under the exigency of Russia's aggression, can ensure its military security and state sovereignty. The following are examined: the possibility of ensuring the military security of Ukraine through its participation in international organisations, signing bilateral and multilateral international treaties and strengthening its defence capability. Non-aligned or neutral status is considered as a possibility for neutralising military threats to Ukraine. The conclusion is that only NATO membership can guarantee the comprehensive military security of Ukraine.

**Keywords:** military security, sovereignty, Ukraine, the Russian Federation, the UN, NATO, the European Union.

### 1 INTRODUCTION

Even though the former National Security Strategy of Ukraine, which had been approved in 2012, acknowledged 'the existence of tendencies to revise national borders beyond the norms of international law', it stressed that 'internal challenges to national security (government inefficiency, corruption, lack of competitiveness in Ukrainian economy etc.) for Ukraine were more urgent to national security' (2012).

However, an overt military aggression by the Russian Federation against Ukraine has concretised the issue of the military security of our country.

Thus, the new National Security Strategy states that 'the aggressive activities of Russia are undertaken in order to deplete Ukraine's economy and undermine social and political stability aiming at the destruction of the Ukrainian state and the seizure of its territory' (2015).

Given the Russian Federation's constant military threat, ensuring the military security of Ukraine has become the most pressing issue for our country. It's commonly known that military security is an integral part of national security. For example, the Dictionary of Military and Associated Terms of the US Ministry of Defense does not define military security as such but distinguishes defensive components as an essential part of national security. The dictionary emphasises that national security encompasses both national defence and international relations (2016).

In other words, military security characterises the ability of the state to have an effective defence that provides a reliable protection of its sovereignty and territorial integrity against encroachments of a foreign military force.

The article aims to determine how under Russian aggression Ukraine can ensure its own military security and sovereignty. To achieve the objective, this article studies the possibility of ensuring Ukraine's military security through participation in international organisations with the help of bilateral and multilateral international agreements, and by strengthening defence capability of Ukraine. Neutral or non-aligned status, as a possibility to neutralise

military threats faced by Ukraine, is also considered in this paper.

### 2 RESULTS

Military security of a state can be strengthened through its participation in international collective security organisations.

It's assumed that a key role in maintaining peace and resolving conflicts should belong to the United Nations (UN). Thereby theoretically it's exactly the UN that should have responded in a proper manner to annexation of our country's territory. In practice, however, possessing the right of veto at the UN Security Council (UNSC), the Russian Federation has been blocking any resolution that condemns its aggression against Ukraine, and does not allow the UN mechanisms to protect our country's territorial integrity.

The Guardian notes that Russia used its veto powers four times to block resolutions on Syria that Moscow sees as damaging to its ally, the regime of Bashar al-Assad. It has also been preventing any common action on the situation in Ukraine where it is a party to the conflict, having annexed Crimea and pursuing a covert military campaign in support of eastern separatists [5].

On 15 March 2014, the UNSC failed to adopt a draft resolution on resolving the crisis in Ukraine. Russia used the right of veto during the vote on the draft, which was submitted by the US Delegation and several other UNSC members. Thirteen UNSC members voted in favour of the draft text with China abstaining. The resolution would have reaffirmed Ukraine's 'sovereignty, independence, unity and territorial integrity' and declared that 'Sunday's referendum which could lead to Crimea's break with Ukraine and union with Russia can have no validity' [9].

Moreover, hiding its own war crimes on the occupied territories of Ukraine, Russia blocked the UNSC resolution on the establishment of a tribunal for prosecution of those responsible for the crash of the Malaysian airliner 'Boeing' MH17, shot down over the Donetsk region in July 2014.



Thus, all the above convinces us that the UN Security Council reform is the cornerstone of the UN's renewal. Some time ago, France came up with a proposal that the five UNSC permanent members suspend voluntarily using their veto right in situations where genocide occurs or other mass atrocities are committed. The UNSC reform is actively supported by Germany, Japan, India and other countries [5].

However, we should be realists and understand clearly that in the near future major changes in the UNSC are very unlikely to happen and the veto right of its five permanent members will continue to doom the whole organisation to inactivity in cases of violation of international law.

In these circumstances, Ukraine can only use the UN General Assembly as a forum to help convey its view to the global community and keep constantly issues condemning Russia's aggression against Ukraine on the UN agenda.

For example, the UN General Assembly resolution 'The territorial integrity of Ukraine' No 68/262, adopted on March 27, 2014, reaffirmed 'the sovereignty, political independence and territorial integrity of Ukraine within its internationally recognised borders and called upon all states to desist and to refrain from actions aimed at the partial or complete breach of the national unity and territorial integrity of Ukraine'. In addition to this, the resolution emphasises that 'the referendum held in Crimea and Sevastopol on March 16, 2014, having had no validity, cannot form the basis for any alteration of the status of the Autonomous Republic of Crimea or of the city of Sevastopol' (2014).

In October 2015, Ukraine got the non-permanent member status of the UN Security Council for the period of two years and began its duties on 1 January 2016. UNSC non-permanent membership provides our state with additional opportunities to present agenda to the Security Council related to the restoration of the territorial integrity of Ukraine, but no more.

Therefore, from all the above we can conclude that in situations where Ukraine stands against the aggressor, the Russian Federation – which is a UNSC permanent member – there is no sense in relying on protection of Ukrainian national interests by the UN. Ukraine can only use the UN platform as a tool of political and moral pressure on Russia and for informing the international community about the truth about the events related to the occupation of Crimea and Russia's support of terrorists in Eastern Ukraine.

The Organization for Security and Co-operation in Europe (OSCE) is the second security organisation, membership of which should have protected Ukraine from Russia's invasion and, in general, should have contributed to upholding our country's territorial integrity.

However, it should be noted that the OSCE has still not become a full-fledged international organisation with its own charter and other legal documents, which are an integral part of such an institution. Because of limited resources (the OSCE does not have the levers of power, it relies only on its authority to urge parties to end a conflict), today the organisation cannot effectively deal with contemporary threats and challenges.

Moreover, in the case of Russia's aggression against Ukraine (due to the fact that OSCE's decisions are adopted by consensus) Russia did everything so that to only display its insincere interest in resolving the conflict in Eastern Ukraine and actually prevented the extension of a mandate of the OSCE Special Monitoring Mission to Ukraine. Because of this, mission members have been able to observe only a few hundred meters of territory out of several hundred kilometres of the uncontrolled by the Ukrainian government area.

Russia cannot be regarded otherwise than carrying out a consistent policy of hiding from the international community the obvious evidences of Russia's direct involvement in the conflict in the Donbas region.

Thus, in Ukraine the power of the Organization for Security and Cooperation in Europe is controlled by Russia and is blocked by it in the same way as in the case of the UN Security Council.

The European Union and NATO are two organisations that are part of the Euro-Atlantic system of international security – the guarantee of the military security of its members.

As for the EU, it can be said that with the implementation of the Lisbon Treaty on December 1, 2009, the EU defence policy acquired a new quality and was given a new name – the Common Security and Defence Policy.

The Common Security and Defence Policy is an integral part of the EU Common Foreign and Security Policy. 'It includes the progressive framing of a common Union defence policy (when the European Council, acting unanimously, so decides) and gives it an operational capacity drawing on civil and military assets that the EU can use on missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter' [3].

The mutual provision and assistance clause of the Treaty on European Union is of a big importance in the context of the EU defence policy. This clause obliges the EU Member States to provide necessary aid and assistance to other Member States by all the means in their power if a Member State becomes the victim of armed aggression within its territory.

The Treaty on European Union opened a number of new opportunities for deepening the integration of Member States in defence. In particular, it provides for a permanent structured cooperation network – an

alliance of a group of the EU countries based on shared interests and aspirations in the field of defence. Permanent structured cooperation is established by paragraph 6 of Article 42 of the Treaty on European Union and is open to all Member States.

Of equal importance is the solidarity clause contained in the Treaty on the Functioning of the European Union. According to Article 222 of this Treaty, 'if a Member State becomes the object of a terrorist attack or the victim of a natural or man-made disaster, the Union and the Member States shall act jointly in a spirit of solidarity. The Union will mobilise all means that are at its disposal, including military resources provided by Member States' [3]. Thus, although the EU is now at the stage of the creation of collective defence, clauses on mutual assistance of the Treaty on European Union and the solidarity clause of the Treaty on the Functioning of the European Union ensure reliably a military security of the EU Member States.

It should be noted that a new EU Strategy stresses the need to strengthen the defence component of the European Union [1]. The provisions of this Strategy have already been translated into the EU's practical actions (Council conclusions on implementing the EU global strategy in the area of security and defence, 2016).

Cooperation with the EU within the framework of the Common Security and Defence Policy is an important part of the European integration course for Ukraine. However, such cooperation is not able to ensure fully the military security of Ukraine because the aforementioned EU solidarity and mutual assistance provisions apply only to the EU Member States and do not apply to EU partner countries.

So, what are the prospects for our country of ensuring its military security through membership in the European Union?

In 2014 Ukraine signed the Association Agreement with the EU (The Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part), which actually is a program for reforming all spheres of public life in Ukraine. Compliance with this Agreement is a long and painstaking process, which, in the opinion of the authors of this article, will take many years.

The magnitude and complexity of reforms in Ukrainian society, the EU's unwillingness to expand and unwillingness of some member states to see Ukraine becoming an EU member consist the major obstruction to our country's European aspirations. even in the case of significant progress in the implementation of domestic reforms.

Concerning the subject of the North Atlantic Treaty Organization (NATO), it should be noted that it is the sole international agreement in the Euro-Atlantic area which contains collective security

commitments on common defence. Article 5 of the Washington Treaty holds that 'an armed attack against one or more NATO members in Europe or North America shall be considered an attack against them all' (The North Atlantic Treaty, 1949). Hence, NATO membership guarantees military security of member states and has been for many countries a source of compensation for the lack of their own military resources necessary for ensuring their territorial integrity and immunity to external attacks.

So, what are the chances of Ukraine to ensure its military security through NATO membership? In order to answer this question, we will use a formula proposed by Wolfgang Ischinger.

To measure whether any country should be invited to become a NATO member, Ischinger proposes a very simple three-step test: 'Is there a consensus within the respective country regarding the application for NATO membership? Do all NATO partners agree to invite the country? Would this NATO membership enhance European security?' (2015). Only if the answer to all three questions is positive, as Wolfgang Ischinger rightly states, can this country be invited to join the Alliance.

Regarding Ukrainian citizens' support of the idea of joining NATO, it should be noted that for a long time (from 2006 to 2012), this support did not exceed 16 %. Since the beginning of Russia's aggression, this support has been steadily increasing and, according to the latest public opinion polls, reached 48 % [13]. Provided that there is an increasing awareness campaign, this percentage could continue to grow and turn into more convincing figures.

Ischinger himself gives the answer to the second question in his article arguing that 'we should avoid getting caught up in new discussions about Ukraine's NATO membership' (2015).

Ischinger's opinion could be seen as his personal one, if only such views were not shared by officials of certain other NATO member states. For example, in February 2015, before his visit to Ukraine, the French President Hollande stated clearly that France was 'opposing Ukraine's NATO membership' [17].

Giving an answer to the third question is pretty easy. Ukraine's NATO membership would mean NATO's involvement in the conflict with Russia (due to Russia's aggression against Ukraine and because of the fact that the expansion of NATO is mentioned in the Military Doctrine of the Russian Federation as one of the main 'external military threats to the Russian Federation' [12].

Considering all the above and the fact that all NATO decisions are adopted by consensus, the prospects of Ukraine's NATO membership in the near future looks rather bleak.

For obvious reasons, the Collective Security Treaty Organization (CSTO) has not been considered in this article as a mechanism for ensuring military security of Ukraine. You cannot

look for guarantees of sovereignty from the state which is an aggressor. It is worth recalling that in addition to Russia two other CSTO members – Armenia and Belarus – voted against the UN General Assembly Resolution ‘Territorial integrity of Ukraine’ № 68/262.

When speaking about guaranteeing the military security of Ukraine through bilateral and multilateral international treaties, we should first recall the Memorandum on Security Assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons (the so-called 1994 Budapest Memorandum). It should be noted that the document didn't guarantee Ukraine's security in any way (how this could become possible is the subject of a separate study and is not considered here).

According to the Memorandum, the Russian Federation, the United Kingdom and the United States ‘reaffirmed their commitment to Ukraine in accordance with the principles of the Final Act of the CSCE to respect the independence, sovereignty and existing borders of Ukraine’ (Меморандум про гарантії безпеки, 1994). Russia consistently ignores these obligations, and the other signatory countries do not consider themselves responsible for protecting the territorial integrity of Ukraine.

The Russian Federation also violates its obligations to refrain from using weapons against the territorial integrity of Ukraine — by annexing Crimea, arming terrorists in Eastern Ukraine and sending mercenaries to fight against Ukrainian government forces. Moreover, Russia did violate the Memorandum's clauses long before the invasion of Crimea. According to the terms of the Memorandum, Russia made a commitment to refrain from economic pressure that seeks to subordinate to Russia's own interests the exercise by Ukraine of the rights inherent in her sovereignty (here we should recall many trade wars between Russia and Ukraine, which purpose was and remains the slowdown of Ukraine's European aspirations).

In addition, Russia violated its obligations to respect the territorial integrity and inviolability of Ukraine's borders in accordance with such documents as the ‘Treaty of Friendship, Cooperation and Partnership between Ukraine and the Russian Federation’ dated 31 May 1997 and the ‘Agreement between Ukraine and the Russian Federation on Ukrainian-Russian state border’ dated 28 January 2003. [15]

Nobody is seriously considering the non-aligned or neutral status as a means of neutralising military threats to Ukraine. Considerations about such status for Ukraine have been occasionally expressed by foreign specialists (for example, Henry Kissinger [4]. But such decisions are not considered in terms of guarantees of territorial integrity and independence of our country. In fact, these proposals aim to appease the Russian Federation and recognise

Ukraine as part of the sphere of the Russian interest. The former non-aligned status of Ukraine did not protect the state from Russia's external aggression. Neutral status does not guarantee the territorial integrity of our country, given Russia's brutal violation of international law.

The vast majority of domestic researchers regard the enhancement of Ukrainian defence as the only guarantee of the military security of Ukraine.

Formation and development priorities for the security and defence sector, which are expected to provide an adequate and flexible response to threats to the sovereignty of Ukraine, are listed in Ukraine's National Security Strategy and the Military Doctrine. There is no need for this article to refer to these documents (which, in the opinion of the authors, were duly prepared, and which take into account the particular condition of international security). Let's try to figure out just how Ukraine's capacity enables and allows it to turn, first of all, the Armed Forces of Ukraine into a reliable guarantor of the territorial integrity of the country.

We'd like to stress that since the very beginning of Ukraine's independence our country's defence has not been a priority area of activity, without exception, for all its heads of state and government. The so-called ‘reform’ of the Armed Forces of Ukraine instead of forming an optimal structure able to meet effectively various national security challenges, in fact resulted in the reduction of its number and its virtual destruction.

During the parliamentary hearings ‘On the status and prospects of the military organisation and security sector of Ukraine’ in May 2012, the then Chairman of the Parliamentary Committee on National Security and Defence, Anatoly Hrytsenko (also the Defence Minister in 2005-2007), stressed: ‘The situation in the army is close to a disaster. The officer corps is demoralised. The Armed Forces cannot perform tasks in full even in peacetime; the Army hasn't got any combat-ready battalions, the Air Force hasn't got any fully efficient squadrons, the Naval Forces haven't got any naval squadrons that could carry out all its missions as required’ [18].

Recent developments related to Russia's aggression in Crimea and Eastern Ukraine forced the country's leadership to turn to the reconstruction of the Armed Forces. Although much of work has already been done, we have to admit that the Ukrainian Army has to these days been doing all the fighting using obsolete armour and artillery systems – the same kind of weapons that Russia has been supplying terrorists in the east with, hoping to conceal as much as possible her backing of the one particular part of the conflict. However, this is still not a true modern war which Putin is waging against Ukraine.

Today, the Army is undergoing the process of transformation, but it still lacks the newest weapons, without which Ukraine's military will never become

a factor of deterrence against Russia's aggression. Ukraine needs a professional army, equipped with high-precision weapons, unmanned systems, air defence, modern aircraft etc. Obviously, the Ukrainian government cannot afford to buy all these kinds of weapons. Ukraine's gross domestic product has been falling because of Russia's aggression in the east and in Crimea. Ukraine lost a large number of enterprises, its external debt has since been increasing, its pension fund has been facing a permanent deficit. There are other urgent tasks, such as recovery of the war-damaged infrastructure and upholding the rights of internally displaced persons (whose total number exceeds a million people – men, women and children).

We should acknowledge openly the following truth: the problem of the Ukrainian defence capability cannot be solved quickly and in a short term. It is a laborious, long and very costly process. And even more, because of the disparity between Russia and Ukraine, Ukraine is not able to defeat Russia in an armed confrontation under any circumstances.

### 3 CONCLUSIONS

We have to conclude that none of the options considered here can guarantee Ukraine's military security. Under current conditions, the most effective options, in the opinion of the authors, are:

1. Combination of diplomatic efforts within the framework of international organisations with;
2. Ukraine's military reform with the US and NATO aid and assistance;
3. Keeping EU and US sanctions imposed on Russia in place to react on Russia's continuing aggression against Ukraine.

However, it should be noted that the only possible guarantee of Ukraine's military security is her NATO membership. In December 2014, the Parliament of Ukraine abolished the neutral status of Ukraine.

The decision of the Ukrainian parliament establishes a legislative framework for its future application to join the Membership Action Plan for NATO membership. NATO, unlike the EU, hasn't got strict criteria for its membership (apart from the clauses of the 1949 North Atlantic Treaty, which states that NATO membership is open to any European state 'which is able to implement the principles of the Treaty (democracy, individual freedom, the rule of law) and to contribute to the security of the North Atlantic area' (1949). All this simplifies the NATO admission procedure for any country to join the Alliance.

After stabilising the situation in Ukraine, the issue of Ukraine's NATO membership should be kept on the agenda, because only NATO membership will secure our country from the

constant threat of Russia. Despite the fact that, unlike Georgia, the prospect of Ukraine's NATO membership was not mentioned in the Final Declaration of NATO's Summit in Warsaw [10], the political situation in the world is changing and when the opportunity to join NATO opens, Ukraine should be ready for this moment.

Today, we should focus on the Armed Forces of Ukraine adopting NATO military standards and achieving the required level of compatibility in the areas of logistics, doctrine, tactics, training, communication and so on. At the same time, we should remember that NATO admits the whole country, not just its armed forces. Much will depend on economic reforms, a real fight against corruption, introduction of an independent judiciary etc. Ukraine should become attractive for Western partners, instead of being perceived as a source of permanent problems.

At the same time, Ukrainian diplomacy must explain at all levels and expose to the international community the fact that the notion of the impossibility of Ukraine joining NATO is nothing else than the recognition of the Ukrainian territory as being within the sphere of Russian influence, connivance at its aggression and neglecting Ukraine's aspirations to become a truly sovereign country, free from the Russian dictatorship for ever.

### References

- [1] *A Global Strategy for the European Union's Foreign and Security Policy* (2016). Available at: [https://eeas.europa.eu/top\\_stories/pdf/eugs\\_review\\_web.pdf](https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf), Accessed 5.11.2016.
- [2] *Council conclusions on implementing the EU global strategy in the area of security and defence* (2016). Available at: <http://www.consilium.europa.eu/en/press/press-releases/2016/11/14-conclusions-eu-global-strategy-security-defence/>, Accessed 20.11.2016.
- [3] *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union* (2012). Available at: [http://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC\\_2&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF), Accessed 2.11.2016.
- [4] *Jacob Heilbrunn, spoke with Henry Kissinger* (2015). Available at: <http://nationalinterest.org/feature/the-interview-henry-kissinger-13615>, Accessed 3.11.2016.
- [5] *Julian Borger, Bastien Inzaurrealde. 'Russian vetoes are putting UN security council's legitimacy at risk, says US'* (2015). Available at: <https://www.theguardian.com/world/2015/sep/23/russian-vetoes-putting-un-security-council-legitimacy-at-risk-says-us>, Accessed 1.11.2016.

- [6] Resolution adopted by the General Assembly on 27 March 2014 68/262. Territorial integrity of Ukraine (2014). Available at: [http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a\\_res\\_68\\_262.pdf](http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_68_262.pdf), Accessed 20.11.2016.
- [7] The Joint Publication (JP) 1-02, Department of Defense (2016). Dictionary of Military and Associated Terms. Available at: [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf), Accessed 20.11.2016.
- [8] *The North Atlantic Treaty* (1949). Available at: [http://www.nato.int/cps/en/natolive/official\\_texts\\_17120.htm](http://www.nato.int/cps/en/natolive/official_texts_17120.htm), Accessed 20.11.2016.
- [9] *UN Security Council action on Crimea referendum blocked* (2014). Available at: <http://www.un.org/apps/news/story.asp?NewsID=47362#.Vh5DHyuJ0u8>, Accessed 19.11.2016.
- [10] Warsaw Summit Communiqué (2016). Available at: [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](http://www.nato.int/cps/en/natohq/official_texts_133169.htm), Accessed 22/11/2016.
- [11] ISCHINGER, W. (2015), 'A task of generations. Russia and the West', *Per Concordiam: Journal of European Security and Defense Issues*, 6(3): 9. Available at [http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F\\_Publications/perConcordiam/pC\\_V6N3\\_en.pdf](http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V6N3_en.pdf) - Accessed 20/11/2016.
- [12] Военная доктрина Российской Федерации (2014) [The Military Doctrine of the Russian Federation]. Available at: <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>, Accessed 20.11.2016.
- [13] Динаміка суспільно-політичних настроїв: вересень 2015 [The dynamics of social and political attitudes: September 2015]. Available at: [http://ratinggroup.ua/files/ratinggroup/reg\\_files/survey\\_of\\_ukrainian\\_public\\_opinion\\_september\\_7-21\\_2015\\_ua\\_0001.pdf](http://ratinggroup.ua/files/ratinggroup/reg_files/survey_of_ukrainian_public_opinion_september_7-21_2015_ua_0001.pdf), Accessed 20.11.2016.
- [14] Договір між Україною і Російською Федерацією про українсько-російський державний кордон (2003) [Agreement between Ukraine and the Russian Federation on Ukrainian-Russian state border]. Available at: [http://zakon2.rada.gov.ua/laws/show/643\\_157](http://zakon2.rada.gov.ua/laws/show/643_157), Accessed 20.11.2016.
- [15] Договір про дружбу, співробітництво і партнерство між Україною і Російською Федерацією (1997) [Treaty of Friendship, Cooperation and Partnership between Ukraine and the Russian Federation]. Available at: [http://zakon2.rada.gov.ua/laws/show/643\\_006](http://zakon2.rada.gov.ua/laws/show/643_006), Accessed 20.11.2016.
- [16] Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї (1994) [The Memorandum on Security Assurances in connection with Ukraine's accession to the Treaty on the Non-Proliferation of Nuclear Weapons]. Available at: [http://zakon2.rada.gov.ua/laws/show/998\\_158](http://zakon2.rada.gov.ua/laws/show/998_158), Accessed 20.11.2016.
- [17] Олланд перед визитом в Київ: 'Франція проти вступлення України в НАТО' (2015) [Mr Hollande said that France was 'opposed to Ukraine joining NATO' before the visit to Kyiv]. Available at: [http://www.bbc.com/ukrainian/ukraine\\_in\\_russian/2015/02/150205\\_ru\\_s\\_hollande\\_merkel\\_update](http://www.bbc.com/ukrainian/ukraine_in_russian/2015/02/150205_ru_s_hollande_merkel_update), Accessed 20.10.2016.
- [18] Парламентські слухання 'Про стан та перспективи розвитку воєнної організації та сектору безпеки України' (2012) [Parliamentary hearings 'On the status and prospects of development of Military organization and the Security Sector of Ukraine']. Available at: [http://komnbo.rada.gov.ua/komnbo/control/uk/publish/printable\\_article?art\\_id=47988](http://komnbo.rada.gov.ua/komnbo/control/uk/publish/printable_article?art_id=47988), Accessed 20.11.2016.
- [19] Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 (2015) [The National Security Strategy of Ukraine (2015) approved by the Decree of the President of Ukraine of 05.26.2015, № 287/2015]. Available at: <http://zakon3.rada.gov.ua/laws/show/287/2015>, Accessed 21.11.2016.
- [20] Стратегія національної безпеки України 'Україна у світі, що змінюється' (2012) [The National Security Strategy of Ukraine 'Ukraine in a changing world']. Available at: <http://zakon2.rada.gov.ua/laws/show/105/2007>, Accessed 22.11.2016.

Assoc. Prof. Oleg POSHEDIN, Ph.D.  
The Globalization, European Integration and National Security Management Department  
The National Academy of Public Administration  
Office of the President of Ukraine  
Pugachova str. 12/2, r. 401  
Kiev, Ukraine 040 50  
E-mail: poshedino@gmail.com

Assoc. Prof. Maryna CHULAIEVSKA, Ph.D.  
The Globalization, European Integration and National Security Management Department  
The National Academy of Public Administration  
Office of the President of Ukraine  
Pugachova str. 12/2, r. 401  
Kiev, Ukraine 040 50  
E-mail: a4u.chulaievaska@gmail.com

**Assoc. Prof. Oleg Poshedin, Ph.D.** - was born in Chygyev, Kharkiv region, Ukraine in 1962. Served 32 years in the military, colonel (rtd), to include participating in relief operations following the 1986 Chernobyl Atomic Power Station catastrophe. He received his M.Sc. degree in 1996 from Taras Shevchenko Kyiv University and Ph.D. degree in military history from the National Defense Academy in 2001. His research interests are international relations, European integration, Euro-Atlantic security, military history.

**Assoc. Prof. Maryna Chulaievska, Ph.D.** - was born in Vinnytsia region, Ukraine in 1979. She received her Ph.D. degree in public administration at the National Academy of public administration, office of the President of Ukraine, in 2013. She is the Assoc. Prof. of the Department of Globalisation, European integration and national security management. Her research interests are security and defence policies, migration, international agreements.



**ARMED FORCES ACADEMY OF GENERAL MILAN RASTISLAV ŠTEFÁNIK**  
**Security and Defence Department**

**Invites you to**  
8<sup>th</sup> International Scientific Conference

**NATIONAL AND INTERNATIONAL SECURITY 2017**

**26<sup>th</sup> – 27<sup>th</sup> October 2017**

Co-organizers  
Ministry of Defence of the Slovak Republic  
General Staff of the Armed Forces of the Slovak Republic  
University of Defence Brno, Czech Republic  
War Studies University Warsaw, Poland  
Apeiron Academy of Security of Public and Individual Krakow, Poland  
Matej Bel University, Banská Bystrica, Slovak Republic  
Academy of the Police Force, Bratislava, Slovak Republic

The International Scientific Conference is organized under auspice of

**Minister of Defence of the Slovak Republic**  
**Peter GAJDOŠ**

and

**Chief of the General Staff of the Armed Forces of the Slovak Republic**  
**Gen. Milan MAXIM**

<http://www.aos.sk/struktura/katedry/kbo/NMB2017/index.php?go=1>

## THE GENDER ISSUE IN THE POLISH ARMED FORCES ON THE EXAMPLE OF PEACE AND STABILIZATION OPERATIONS

Dariusz KOZERAWSKI

**Abstract:** The paper presents the engagement of Polish Military Contingents in international activities as stabilization and peace missions carried out in Afghanistan and Iraq. Moreover the author emphasizes the support role of women-soldiers serving in the Polish Armed Forces in international peace and stabilization operations led within UN and NATO, namely in the Balkans, Afghanistan and Iraq. This paper also brings closer the question of the crisis situations causes and the relations between their participants – stressing the attention on women-soldiers – based on unique field research provided by the author in the Republic of Iraq, Kosovo, Bosnia and Afghanistan.

**Keywords:** gender issue, Polish woman-soldiers, peace and stabilization missions, international security.

The composition of one of most radically hierarchic dispositional groups in the State<sup>1</sup> as the armed forces since 1989 is characterized by a growing number of female soldiers. It is however worth noticing that this ever growing percentage of women in the military personnel of the Polish Army is still relatively low in relation to the majority of the Member States of the North Atlantic Alliance<sup>2</sup>. Due to the gender question which is valid alike in the Atlantic Alliance as in the Polish Armed Forces, the attempt to approximate the role and scope of the tasks that are to be performed by female soldiers during peacekeeping and stabilization missions (these missions are ones of the few areas of the Polish Army activities, where soldiers face the military action in terms of real challenges and threats) seems to be fully justified.

The end of the "Cold War" in the late eighties and early nineties of the 20<sup>th</sup> century and the related such uneven events like political transformation in Poland and other Central and Eastern European countries, the fall of the "Berlin Wall" and the unification of the German states, the Warsaw Pact dissolution, the disintegration of the Soviet Union - permanently altered the international situation in the old continent and globally. The international community through international organizations tried to prevent or limit the negative effects of the conducted armed conflicts during that period<sup>3</sup>. International peacekeeping or stabilization operations were one of the ways to prevent or mitigate tensions between the warring states or within them. It may be recalled that in the recent

literature peacekeeping operations are defined as a set of activities undertaken by entities or actors of international relations in order to prevent, interrupt, mitigate, contain and blank armed conflicts of an international or internal range through the intervention of peacekeepers with the mandate of an international organization for the restoration and maintenance of peace in a region in crisis<sup>4</sup>.

At the beginning of the 21<sup>st</sup> century, there were implemented a number of international military operations known as stabilization or antiterrorist missions. They can not be clearly classified into the category of peacekeeping operations because often when they started, there was no explicit support from the United Nations or other international organizations, sanctioning the use of force in the framework of military interventions. Examples of such activities may be the operation in Iraq (since 2003), carried out by coalition forces without the support of the United Nations (UN), nor the Organization for Security and Cooperation in Europe (OSCE), European Union (EU) or North Atlantic Treaty Organization (NATO)<sup>5</sup>.

Subject to constant changes, the international situation brings a number of widely known and new threats/challenges to international security. They can be applied to such security areas as: political; economic (determining the independence of

<sup>1</sup> KOZERAWSKI, D. S.: Oficerowie Wojska Polskiego w międzynarodowych operacjach pokojowych na Bałkanach jako przykład grupy dyspozycyjnej. In *Bezpieczeństwo narodowe a grupy dyspozycyjne*, (eds.) J. Maciejewski, O. Nowaczyk, Wrocław 2005, p. 227-236.

<sup>2</sup> As an example, in 2016 that represents about 4,5 % of the total human resources in Polish Armed Forces, while in Slovakia it is about 10 %, and in the USA 15 %.

<sup>3</sup> CESARZ, Z., STADTMÜLLER, E.: *Problemy polityczne współczesnego świata*. Wrocław : 2002, p. 91-100.

<sup>4</sup> Compare with Kozerański, D. S., *Kontyngenty Wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973-1999. Konflikty - interwencje - bezpieczeństwo*. Toruń : Wyd. Adam Marszałek, 2012. p. 42; *Przygotowanie żołnierzy WP do międzynarodowych ćwiczeń, operacji pokojowych i stabilizacyjnych (1953-2004)*, ed. Kozerański D. S. Wrocław 2004, p. 7-9; *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa : 2002, p. 92; W. E. Gilman, D. E. Herold, *Peacekeeping Challenges to Euro-Atlantic Security*, NATO Defence College, Rome 1994, p. 21.

<sup>5</sup> KOZERAWSKI, D. S.: Rola i zadania kobiet oficerów Wojska Polskiego w operacjach pokojowych i stabilizacyjnych w procesie utrzymania bezpieczeństwa międzynarodowego w latach 1973-2006. In *Kobiety w grupach dyspozycyjnych społeczeństwa*, eds. Dojwa K., Maciejewski J., Wrocław : Wyd. Uniwersytetu Wrocławskiego, 2007. p. 242 and next.

decision-making on economic issues, the ability to provide optimal socio-economic development, keeping favorable foreign exchange); cultural and social (referring to the maintenance of social peace, respect for human rights and civil rights, freedom and democratization of socio-political control mechanisms and effects of the actions of authority); culture and civilization (about: the free development of spiritual and national identity; lack of political indoctrination and ideological society inculcating values foreign to the cultural sphere to which it belongs; opportunities for social, political and cultural self-realization)<sup>6</sup>.

The collapse of the two-bloc division of the world, which took place in the early nineties, led to major changes in understanding the role of the armed forces as one of the factors significantly affecting the state of national security in the context of national and global level. As part of the major trends of changes which today are subject to the Polish Armed Forces and many other European countries should be distinguished the following ones<sup>7</sup>: the evolution of the function of military force in the development of the world; internationalization (globalization) of military forces in the dimension of institutionalized; search for full professionalization; the military emancipation of women; modulating military structures; a paradigm shift aimed at the use of force to maximize the precision of destruction; dispersion (scattering) of the phenomenon of war and asymmetric impacts in the armed struggle (in quantitative and qualitative terms); changing the ratio between the forces of shock and facilities support activities (in his favor); strategic reorientation of the mission of the army (from territorial defense to defend the interests of political and economic conducted also outside the country); economization of defense (military sphere).

The experience of the nature and characteristics of contemporary conflict helped to formulate the main tasks facing the national (state) armed forces. Besides the primary purpose of their functioning consisting in the defense of the sovereignty and independence of the country, the armed forces - in terms of construction and maintenance of international security - should<sup>8</sup>: participate in UN

peacekeeping missions and crisis operations within NATO; engage in conducting anti-terrorist operations and stabilization or operation of this type organized by coalitions of states; to participate in liquidation of natural disasters and ecological failure and cooperate in humanitarian operations; take part in rescue operations in case of disasters on land and in search and rescue at sea.

The use of the social potential of the country concerned may have a significant impact on the level of implementation of the aforementioned functions and tasks in the armed forces in the national and international environments. The gender issue - including the role and place of women in the structures of a dispositional state group, namely, its armed forces - deserve special emphasis. With regard to the situation of the Polish Army in this point it should be noted that due to the relatively low percentage of participation of female personnel in its structures (for a few years one of the last places in the NATO) and the relatively slow progress of the integration of gender within the military organization<sup>9</sup> - the scale of this phenomenon is not proportional to its importance.

International peacekeeping and stabilization operations are undoubtedly ones of the few areas of the troops associated with the performance of tasks in real time and under real conditions<sup>10</sup>. It should be emphasized that Polish Armed Forces have an extremely rich experience in this kind of activity in the international arena<sup>11</sup>.

From the first half of the fifties (since 1953) the Polish Army has been performing tasks in international peacekeeping operations (missions of observation character)<sup>12</sup>. Even from the very beginning, women were included in the Neutral Nations Supervisory Commission in Korea and the

---

*kompetencje oficerów wobec wyzwań współczesności*, eds. Jarmoszko S., Stępień R., Warszawa : 2005, p. 218-219.

<sup>6</sup> DAWIDCZYK, A.: *Nowe zagrożenia i szanse dla bezpieczeństwa Polski na progu XXI wieku*. Warszawa : 2001, p. 17; Berent Z., *Pokój międzynarodowy i bezpieczeństwo – próba definicji*, „Sprawy Międzynarodowe”, z. 6, 1998, p. 120.

<sup>7</sup> KOZERAWSKI, D. S.: *Rola i zadania kobiet oficerów*, p. 243 and next.; Jarmoszko S., *Osobliwości rozwoju sił zbrojnych początku XXI wieku*. In *Wojsko wobec wyzwań współczesnego świata*, eds. Cieślarczyk M., Dębska A. Warszawa : 2005, s. 119.

<sup>8</sup> Strategia Bezpieczeństwa Narodowego RP, Warszawa 2014, p. 10 and next.; Kozerański D.S., *Rola i zadania kobiet oficerów...*, p. 243 and next; Huzarski M., *Współczesne zagrożenia militarne w kontekście przygotowania kadr oficerskich*. In *Humanistyczne*

<sup>9</sup> DĘBSKA, A.: *Współczesny dyskurs instytucjonalny ponad zmienną płci*. In *Wojsko wobec wyzwań współczesnego świata*, eds. Cieślarczyk M., Dębska A., Warszawa 2005, p. 102.

<sup>10</sup> On the Polish territory soldiers of the PAF get prepared to the future tasks, they are not subject to the threats occurring in real terms in areas of past or actual conflicts.

<sup>11</sup> See more: *Międzynarodowe operacje pokojowe i stabilizacyjne w polskiej polityce bezpieczeństwa w XX i XXI wieku*, ed. Kozerański D. S., Warszawa 2016, p. 10 and next; *Udział jednostek wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973 – 2003*, ed. Kozerański D.S., Warszawa 2004, p. 9-21; *Międzynarodowe operacje pokojowe. Planowanie, zadania, warunki i sposoby realizacji*, ed. D.S. Kozerański, Warszawa 2003, p. 77-94.

<sup>12</sup> Observation missions were most of all monitoring missions about the situation in a Niven region and supervision missions of the international agreements provisions.



Neutral Nations Repatriation Commission by performing translation tasks. Similar projects were implemented in the Commission of Control and Supervision on the Indochina Peninsula in 1954<sup>13</sup>.

The first compact Polish military contingent (under the name Polish Army Special Unit - PWJS) took part in the international operation UNEF II<sup>14</sup> in the Middle East in 1973. The unit was established after requesting the UN Secretary General (on the basis of Security Council Resolution No. 340 of October 25, 1973 r.) to the Polish government for agreeing to participate in the quota of Polish Armed Forces in the Middle East.

The most important tasks performed by the Polish female military personnel during the mission included medical care of the entire peacekeeping UNEF II, including in particular the service polyclinic hospital for 50 beds and providing specialist medical care<sup>15</sup>. It should be emphasized that the vast majority of women carried out their tasks under contract as "dressed in uniforms of army civilian employees". The key positions though were occupied by the military doctors with officers degrees, including women.

Polish Contingents/Quotas (until 1992) implemented mainly logistical tasks within the next missions in the Middle East, Namibia and Cambodia. At that time already an important role was played by the female officers staff. Particular emphasis is given to the operations of UNIFIL<sup>16</sup> in Lebanon, where the Polish side was responsible for securing the medical mission by conducting a field hospital (June 1992). In the first period, it was a more than 60-person medical unit, which in April 1994, joined the logistics battalion and engineering cluster subdivisions counting a total of more than 500 people. Since June 1996, in the area of missions, the Polish side also has had a grouping of repair sub-units. It should be emphasized that the main tasks of female military personnel was to provide medical care to the entire staff of UNIFIL within the field hospital and perform tasks related to the provision of humanitarian aid to the local population<sup>17</sup>.

In the course of peacekeeping operations, in which Poland issued logistics quotas, female soldiers performed tasks primarily on positions related to medical care. The most frequently taken up positions included: head of medical group, laboratory supervisor, commander of the medical group<sup>18</sup>.

For the first time a Polish unit in a battalion number began to perform operational tasks from April 1992, within the UNPROFOR peacekeeping operation in the former Yugoslavia<sup>19</sup>. In the second half of the nineties the Polish military contingents began participation in international peace operations led by the North Atlantic Alliance. The introduction and maintenance of peace carried out in the framework of international peacekeeping operations in the Balkans, such as IFOR<sup>20</sup> (1996) and SFOR<sup>21</sup> (1996-2004) in Bosnia and Herzegovina, AFOR<sup>22</sup> in Albania and KFOR<sup>23</sup> in Kosovo (Since 1999)<sup>24</sup>.

During the peacekeeping operations in the Balkans women soldiers of the PAF primarily performed logistics tasks (mostly as medical staff). Other positions occupied by Polish female staff (eg. the position of translators) were filled out by people with language skills but who were not soldiers<sup>25</sup>.

w międzynarodowych ..., p. 13 - 14; F. Gągor, K. Paszkowski, op. cit., p. 154.

<sup>18</sup> Women in the rank of Ensign performed tasks of: section commander, medical rescuer, nurse, and ladies in the rank of N.C.O. performed tasks of medical rescuers or nurse, Raport: służba kobiet w SZ RP..., p. 5.

<sup>19</sup> UNPROFOR - *United Nations Protection Forces*.

<sup>20</sup> IFOR - *Implementation Forces*.

<sup>21</sup> SFOR - *Stabilization Forces*.

<sup>22</sup> AFOR - *Albanian Forces*.

<sup>23</sup> KFOR - *Kosovo Forces*.

<sup>24</sup> See more: AIMON, 1675.00.18, Uchwała nr 141/95 Rady Ministrów z dn. 5.12.1995 r. w sprawie polskiego kontyngentu wojskowego w Siłach Implementacyjnych w Bośni (IFOR), k. 186-189; ibidem, 1675.00.1, Uchwała nr 146/96 Rady Ministrów z dnia 17.12.1996 r. w sprawie utworzenia Polskiego Kontyngentu Wojskowego w Siłach Stabilizacyjnych w Bośni (SFOR), c. 165-167; D. Kozerański, *Polish-American Military Co-operation in Peace Support Operations in Bosnia and Herzegovina* (1996-1999), „Ad Americam”, nr 6, Kraków 2005, p. 83-93; idem, *The Participation of Polish Military Units in Peace Operations in 1992-1999*, „Sbornik VVŠ”, PV, nr 1, Vyškov 2004, s. 131; *Umieędzynarodowiony konflikt wewnętrzny*, red. J. Pawłowski, A. Ciupiński, Warszawa 2001, p. 118; R. B. Oakley, M. J. Dziedzic, E. M. Goldeberg, *Policing the New World Disorder. Peace Operations and Public Security*, Washington 1998, p. 275.

<sup>25</sup> As an example during the operations SFOR in Bosnia and Herzegovina civilians appointed to military positions of translators (regular position of lieutenant) performed their tasks in PAF military uniforms during the mission, without being earlier in the army. This situation concerned a whole group of civilian translators (female as male). Often it was criticized by

<sup>13</sup> *Kobiety w armii. Udział kobiet w misjach pokojowych i stabilizacyjnych*. Warszawa : Wyd. MON, 2012.

<sup>14</sup> UNEF II - [ang.] *United Nations Emergency Force - Intervention Forces of the UN being a continuation of the UNEF I* (1956-1967).

<sup>15</sup> KOZERAWSKI, D. S.: *Rola i zadania kobiet oficerów*. p. 245 and next. *Udział jednostek Wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973 - 2003*, ed. Kozerański D., Warszawa 2004, p. 10; Zapałowski L., *Operacje pokojowe ONZ*, Kraków 1989, p. 205.

<sup>16</sup> UNIFIL - [ang.] *United Nations Interim Force in Lebanon* - temporary UN forces in Lebanon.

<sup>17</sup> KOZERAWSKI, D.: *The Participation of Polish Military Units in Peace Operations in 1992 - 1999*. [in:] *Sbornik VVŠ* PV, no. 1, Vyškov 2004, p. 128 - 129; *Udział jednostek Wojska Polskiego*

The basic limitations for increasing the participation of female soldiers in international peacekeeping and stabilization operations was the lack of wider opportunities in the nineties for young female students to continue their education in military academies. Therefore the employed women in the army, except for professional qualifications (eg. medical), did not have the knowledge nor the skills necessary to perform different types of tasks (eg. operational staff officer). This situation, in turn, determined the lack of the possibility to designate a female candidate to the position of command and ordnance in the composition of the contingent of international peacekeepers<sup>26</sup>.

During the international Peace Support Operations in the Balkans led by the NATO, the Polish battalion was part of the Nordic-Polish Brigade, followed by the Nordic-Polish Battle Group and worked with units from Denmark, Finland, Norway and Sweden. The tasks performed by women soldiers of the mentioned nations covered a much wider range of activities than was the case in the Polish contingent. For example, Danish, Finnish and Swedish female staff served as officers of operational or logistical units and in the Norwegian battalion outside medical care (provided for the whole brigade) ladies were responsible for the preparation and management of operations, medical evacuation, liaison activities and civil-military cooperation. It should be added that the Finnish mechanized detachments also included women<sup>27</sup>.

Polish membership in NATO (12<sup>th</sup> March 1999) entailed e.g. the adoption of NATO standards, including those concerning the increase in the number of women in Polish Armed Forces<sup>28</sup> (eg. in the US Army military personnel female was about 15 % of the total manpower). It should be noted, however, that in Polish conditions, the process was relatively slow. During that period, the higher military education system created wider opportunities than in the nineties for studying in military schools and academies for female high school alumni's (since 1999). Despite this, the number of women in the structures of PAF, in relation to other NATO armies, as mentioned earlier, is still not significant.

The NATO undertook a wide action to implement the Policy Gender Mainstreaming based on UN Security Council Resolution 1325 on women, peace and security (2000). It is worth noticing that in 2009 another Resolution no. 1889 was issued calling for increased participation of women in the peace processes, and a Directive on Strategic Commands Bi-SC 40-1 on the implementation of

UNSC Resolution 1325 and issues related to gender equality, including measures of protection during armed conflict to the command structures of NATO. The main objectives of the above the Directive was to:

- Integrating gender equality into all phases of activities Wax Alliance;
- Provide conscious perception of gender equality at all levels throughout the chain of command;
- Integration issues dot. Gender equality in the context of the operation is seen as an additional benefit.

It should be emphasized that the Directive of Strategic Commands Bi-SC 40-1 applies to all organizational units of NATO sending staff to support operations and missions approved by the North Atlantic Council.

Particularly significant change in the perception of security on the national and global level - including those related to terrorism - was brought at the beginning of the 21<sup>st</sup> century. The attack on the World Trade Center in New York on 11<sup>th</sup> September 2001 became the main cause of the so-called counter-terrorism operations. Examples of these actions were carried out under the auspices of the UN and NATO in Afghanistan (since 2001.) And the coalition operation in Iraq (since 2003)<sup>29</sup>.

The Polish state involved politically and militarily on the side of the allied forces called anti-terrorist coalition. It should be emphasized that the Iraqi operation is carried out by the coalition of countries led by the United States, but without formal support from the UN or NATO. During the stabilization operation<sup>30</sup> in Iraq (as stated on media demand by the then government) women soldiers performed unusually wide tasks for Polish conditions of operations conduct. In addition to standard logistics projects associated with the medical care measures, they implemented tasks in positions of operational officers and administrative functions in international units or staffs<sup>31</sup>. Particular emphasis is given to performed tasks

the military personnel of the operation, Kozerański D.S., *Rola i zadania kobiet oficerów...*, p. 246.

<sup>26</sup> Ibidem, p. 246-247.

<sup>27</sup> KOZERAŃSKI, D. S. : *Rola i zadania kobiet oficerów...*, p. 247 and next.

<sup>28</sup> DĘBSKA, A.: *Kobieta w mundurze...* p. 40-42.

<sup>29</sup> See more in Kozerański, D. S., *Międzynarodowe działania stabilizacyjne w świetle doświadczeń X zmiany PKW Irak w 2008 roku*. Warszawa : 2010. *Military Conflicts in XX Century - Political and Military Aspects*, ed. Kozerański, D. S., Warsaw : 2010; *Działania stabilizacyjne – aspekty strategiczne. Konflikty, interwencje, bezpieczeństwo*, ed. D.S. Kozerański, Warszawa 2011.

<sup>30</sup> The notion of „stabilization actions” for argumentation purposes to the public opinion in Poland concerning the military presence in Iraq, was to explain the unoffensive character of the mission. The use of the notion Peace Operation was legally banned as it did not have the UN nor the NATO consent.

<sup>31</sup> On the basis of an interview with a female participant of the operations. In Iraq on 15th January 2005.

in the field of civil-military cooperation (CIMIC)<sup>32</sup>. Those came to, inter alia, supervise the implementation of a wide range of projects aimed at improving the living conditions of the population (eg. investment program, water and sanitation, education, improved health care, humanitarian aid to the poorest population groups, and others)<sup>33</sup>.

It should be highlighted that the headquarters of the US and the British forces during the attack on Iraq did not use women to perform tasks in the framework of direct armed force. Instead, the female staff played an important role in the armed support of combat operations. Similar procedures are used in the stabilization operations in the areas of responsibility - including the Polish ones.

When analyzing gender issues, with particular emphasis on the role and scope of the tasks performed by the women-soldiers in international peacekeeping and stabilization operations can highlight several important concerns. In peacekeeping operations carried out until 1989 (the period of the Polish People's Republic), in which NEC performed mainly in charge of handling the logistical tasks of female personnel were limited mainly to activities in the field of medical security, as exemplified by the activities of hospitals/medical centers in peacekeeping operations in the Middle East.

The changes occurring in the Polish Army in the early 90-ies did not substantially increase the number of jobs and tasks carried out by female military personnel in international peacekeeping and stabilization operations. The turning point was the Polish accession to NATO which contributed to the gradual improvement of the situation. As part of the stabilization operations conducted in Iraq, female soldiers performed several task positions in the operational corps and civil-military cooperation. The most commonly held positions included posts of: the commander or chief specialist of CIMIC / civilian-military advisor and the head of the liaison officer<sup>34</sup>. In turn, in Afghanistan, women-soldiers in other armies performed the tasks of logistics and operational officers. For example, about 20 % of the

manpower of US operations of ISAF and Enduring Freedom were women<sup>35</sup>.

For instance, in 2005 Polish soldiers participated in twelve (continued and newly started) peacekeeping and stabilization operations. They were attended by 4 819 soldiers and military employees, including 61 women soldiers (about 1.3 % of the total)<sup>36</sup>. In 2009 in the aforementioned operations attended 96 female soldiers (1.35 % of total participants), in 2010 - 111 women (2.22 %) in 2011 this number was 140 female soldiers, which accounted for 2.25 % of all participants in operations outside the country<sup>37</sup>.

In conclusion it should be emphasized that the gender issue associated and the associated increase rate in the number of women in the Polish Army and their participation in international peacekeeping and stabilization operations does not inspire too much optimism. It should be noted, however, that after 1999, tentatives in enlarging female military personnel have become slightly larger than in the previous period. The main factors that determine and in the coming years can positively change the scope of tasks performed by women soldiers are to be sought e.g. in international developments affecting the nature of contemporary armed conflicts and the lines in the next transformation processes of Polish Armed Forces.

## References

- [1] BERENT, Z.: Pokój międzynarodowy i bezpieczeństwo – próba definicji. In *Sprawy Międzynarodowe*, p. 6, 1998.
- [2] CESARZ, Z., STADTMÜLLER, E.: *Problemy polityczne współczesnego świata*. Wrocław : 2002.
- [3] DAWIDCZYK, A.: *Nowe zagrożenia i szanse dla bezpieczeństwa Polski na progu XXI wieku*. Warszawa : 2001.
- [4] DĘBSKA, A.: Współczesny dyskurs instytucjonalny ponad zmienną płci. In *Wojsko wobec wyzwań współczesnego świata*, ed. M. Cieślarczyk, A. Dębiska. Warszawa : 2005.
- [5] *Działania stabilizacyjne – aspekty strategiczne. Konflikty, interwencje, bezpieczeństwo*, red. D. S. Kozerański. Warszawa : 2011.
- [6] GILMAN, W. E., HEROLD, D. E.: *Peacekeeping Challenges to Euro-Atlantic Security*. Rome : NATO Defence College, 1994.

<sup>32</sup> CIMIC - Civil Military Co-operation.

<sup>33</sup> See more: Kozerański D.S., *Międzynarodowe działania stabilizacyjne w świetle doświadczeń X zmiany PKW Irak w 2008 roku*, Warszawa 2010, p. 113 and next; idem, *Rola i zadania kobiet oficerów...*, p. 248; *Operacja „Iracka Wolność”*, Scientific Conference materials, Warsaw 2003; „*Iracka Wolność*”, *Myśl Wojskowa*, dodat. spec., Warszawa 2003; Z. Moszumański, Z. Palski, *Wojsko Polskie w Iraku*, Warszawa 2003; *Trudna stabilizacja*, Materiały z konferencji naukowej, Warszawa 2004.

<sup>34</sup> Raport: służba kobiet w SZ RP..., p. 5.

<sup>35</sup> On the basis of field research provided in Afghanistan by the author between 2009 and 2012.

<sup>36</sup> Report: służba kobiet w SZ RP..., p. 5.

<sup>37</sup> ISAF in Afghanistan, PKW UNMIBH – Bosnia and Hercegovina, PKW KFOR – Kosowo, *Kobiety w armii. Udział polskich kobiet w misjach pokojowych i stabilizacyjnych*, Wyd. MON, Warszawa 2012.

- [7] HUZARSKI, M.: Współczesne zagrożenia militarne w kontekście przygotowania kadr oficerskich. In *Humanistyczne kompetencje oficerów wobec wyzwań współczesności*, ed. S. Jarmoszek, R. Stępień. Warszawa : 2005.
- [8] *Iracka Wolność*, Myśl Wojskowa, add. spec., Warszawa : 2003..
- [9] JARMOSZKO, S.: Osobliwości rozwoju sił zbrojnych początku XXI wieku. In *Wojsko wobec wyzwań współczesnego świata*, ed. M. Cieślarczyk, A. Dębska. Warszawa : 2005.
- [10] *Kobiety w armii. Udział polskich kobiet w misjach pokojowych i stabilizacyjnych*, ed. MOD. Warszawa : 2012.
- [11] KOZERAWSKI, D. S.: Konflikty zbrojne na Bałkanach i próby ich rozwiązania pod koniec XX wieku. In *Zeszyty Naukowe Akademii Obrony Narodowej*, nr 4. Warszawa : 2003.
- [12] KOZERAWSKI, D. S.: The Participation of Polish Military Units in Peace Operations in 1992 – 1999. In *Sbornik VVŠ PV*, nr 1. Vyškov: 2004.
- [13] KOZERAWSKI, D. S.: *Polish-American Military Co-operation in Peace Support Operations in Bosnia and Herzegovina (1996-1999)*. Ad Americam, nr 6. Kraków : 2005.
- [14] KOZERAWSKI, D. S.: Oficerowie Wojska Polskiego w międzynarodowych operacjach pokojowych na Bałkanach jako przykład grupy dyspozycyjnej. In *Bezpieczeństwo narodowe a grupy dyspozycyjne*, red. J. Maciejewski, O. Nowaczyk, Wrocław 2005.
- [15] KOZERAWSKI, D. S.: Rola i zadania kobiet oficerów Wojska Polskiego w operacjach pokojowych i stabilizacyjnych w procesie utrzymania bezpieczeństwa międzynarodowego w latach 1973-2006. In *Kobiety w grupach dyspozycyjnych społeczeństwa*, ed. K. Dojwa, J. Maciejewski. Wrocław : Wyd. Uniwersytetu Wrocławskiego, 2007.
- [16] KOZERAWSKI, D. S.: *Międzynarodowe działania stabilizacyjne w świetle doświadczeń X zmiany PKW Irak w 2008 roku*. Warszawa : 2010.
- [17] KOZERAWSKI, D. S.: *Kontyngenty Wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973-1999. Konflikty - interwencje - bezpieczeństwo*, ed. Adam Marszałek. Toruń : 2012.
- [18] *Międzynarodowe operacje pokojowe i stabilizacyjne w polskiej polityce bezpieczeństwa w XX i XXI wieku*, ed. D. S. Kozerański. Warszawa : 2016.
- [19] *Międzynarodowe operacje pokojowe. Planowanie, zadania, warunki i sposoby realizacji*, ed. D.S. Kozerański. Warszawa : 2003.
- [20] *Military Conflicts in XX Century - Political and Military Aspects*, ed. D. S. Kozerański. Warsaw : 2010.
- [21] MOSZUMAŃSKI, Z., PALSKI, Z.: *Wojsko Polskie w Iraku*. Warszawa : 2003.
- [22] OAKLEY, R. B., DZIEDZIC, M. J., GOLDEBERG, E. M.: *Policing the New World Disorder. Peace Operations and Public Security*. Washington : 1998.
- [23] *Operacja „Iracka Wolność”*. Warszawa : 2003.
- [24] *Przygotowanie żołnierzy WP do międzynarodowych ćwiczeń, operacji pokojowych i stabilizacyjnych (1953–2004)*, ed. D. S. Kozerański. Wrocław : 2004.
- [25] *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa : 2002.
- [26] *Strategia Bezpieczeństwa Narodowego RP*. Warszawa : 2014.
- [27] *Trudna stabilizacja*. Warszawa : 2004.
- [28] *Udział jednostek wojska Polskiego w międzynarodowych operacjach pokojowych w latach 1973 – 2003*, ed. D. S. Kozerański. Warszawa : 2004.
- [29] *Umiędzynarodowiony konflikt wewnętrzny*. ed. J. Pawłowski, A. Ciupiński, Warszawa 2001.
- [30] ZAPĄŁOWSKI, L.: *Operacje pokojowe ONZ*. Kraków : 1989.

Prof. (Col. ret.) Eng. Dariusz KOZERAWSKI, Ph.D.  
Police Academy in Szczecino  
St. Marszałka Józefa Piłsudskiego  
12-108 Szczecino  
Poland  
E-mail: d\_kozerański@op.pl

**Prof. (Col. ret.) Eng. Dariusz Kozerański, Ph.D.** - He received his M.Sc. and Ph.D., Assoc. Prof. and title Prof. degrees at the Wrocław University (Poland). His area of expertise is international security relations, conflict studies, security strategy and military history. He was: Rector-Commandant of National Defence University in Warsaw (since 2014-2016); vice Rector of NDU for Military Affairs and International Cooperation (2013-2014); Head of the Chair of Strategy and Geostrategy (2008-2013), Head of the Chair of European (2007-2008). He is a member of Euro-Atlantic Conflict Studies Working Group of the PfP Consortium of Defence Academies and Security Studies Institutes, the Society of Military Historians and Military History Working Group, Society of Polish Geopolitics. He was a member of V-4 Educational Platform and Central European Forum of Military Education. He possesses the status of the veteran of international operations. He realized fieldworks in zones of war and stabilization activities (Bosnia and Herzegovina 1998-1999; Moldavia - 2006; Iraq - 2008, 2014; Afghanistan 2009, 2012; Kosovo - 2012).

# POSSIBILITIES IN DEVELOPMENT OF THERMAL CAMOUFLAGING

Samuel FILÍPEK, Peter DROPPA

**Abstract:** The paper discusses the possible approaches in development of thermal camouflaging systems for the mobile military technics. In general, it is possible either to insulate the heat inside the vehicle or to design the camouflaging systems with the vented walls. Which way has a higher potential in the next development? To investigate the possibilities of thermal camouflaging firstly we have realized some mathematical calculations, then we have designed a simulation models that we have tested in the software Area 2010. After all we have also designed some real samples of the thermal camouflaging panel and we have realized the experiments in the real conditions. More you can discover in our paper.

**Keywords:** mobile military technics, thermal camouflage, heat flux calculations, thermovision, camouflaging systems.

## 1 INTRODUCTION

In searching for an ideal solution in thermal camouflaging of the mobile military technics it is necessary to make a lot of analysis. Before the experiments, it is recommended to realize more model situations that should be modeled and analyzed in the appropriate software. During the preparative phase of the project it is also convenient to realize also some mathematical calculations of the heat flux. Many constructors of nowadays military vehicles use the internal insulating materials to insulate the hull of vehicle, expecting that this way of hull insulation is effective. We have tried to model some camouflaging situations to ensure if this way of camouflaging the vehicle is really as effective as it is generally expected.

## 2 MATHEMATICAL CALCULATIONS

In general, we divide the heat transfer in three main ways. Firstly we can talk about the conduction, than about the convection and the last but not least about the radiation. Many of calculations forget to consider an important part of the heat transfer, the radiation. The radiation solves the invisible infrared radiation that otherwise do not affect the general heat flux so much as the convection and the conduction, but if we forget to consider the effect of the radiation, in higher surface temperatures we can get the false results. [1] To calculate the heat transfer in a multilayer wall by conduction, convection and by radiation we can use following formulas:

$$\dot{q} = k (t_1 - t_2) \quad [W \cdot m^{-2}] \quad (1)$$

where

$$k = \left( \frac{1}{\alpha_1 + \alpha_r} + \frac{\delta_1}{\lambda_1} + \frac{\delta_2}{\lambda_2} + \frac{\delta_3}{\lambda_3} + \frac{1}{\alpha_2} \right)^{-1} \quad [W \cdot m^{-2} \cdot K^{-1}] \quad (2)$$

where

$$\alpha_r = \frac{\varepsilon_{01} C_o}{t_{s0} - t_{s1}} \left[ \left( \frac{t_{s0}}{100} \right)^4 - \left( \frac{t_{s1}}{100} \right)^4 \right] \quad [W \cdot m^{-2} \cdot K^{-1}] \quad (3)$$

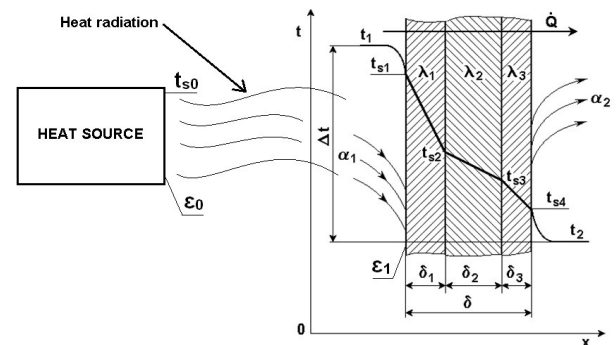
where

$$\varepsilon_{01} = \left( \frac{1}{\varepsilon_0} - \frac{1}{2} + \frac{1}{\varepsilon_1} - \frac{1}{2} \right)^{-1} \quad [-] \quad (4)$$

and

$$C_o = 5,77 \quad [W \cdot m^{-2} \cdot K^{-4}] \quad (5)$$

The heat transfer in a multilayer wall by conduction, convection and by radiation is demonstrated in the Figure 1.



**Fig. 1** The heat transfer in multilayer wall by conduction, convection and radiation [1]

## 3 SIMULATIONS

In modeling the situation we have used following materials (Tab. 1) [2], [3].

In order to gain a simulation of a thermal flux through the material we have had to simulate certain boundary conditions on the model (Tab. 2). On the left side of the situation, there are simulated the interior conditions inside of the vehicle. On the right side of the situation, there are simulated the exterior conditions outside of the vehicle.

**Table 1** Material contributions

Material	d [m]	$\lambda$ [W.m <sup>-2</sup> .K <sup>-1</sup> ]	h [m]	$\varepsilon$ [-]	Abb -rev
Armor "2P" used in construction of BVP-2	0,02	52	1	-	A
External camouflaging khaki paint	0,0015	0,2	0,5	-	P
Insulating paint "Thermal-Tec"	0,02	0,05	0,5	-	TT
Galvanized (zinc-coated) steel sheet used as an external thermal shield	0,0015	52	0,5	-	SS
Air space between armor and the thermal shield	0,003	-	0,5	0,85	AS
Insulating aluminum foil Thermoflex (Den Braven)	0,002	0,038	0,5	-	IF

**Table 2** Boundary conditions

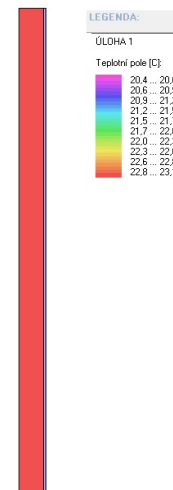
Simulation	Position	T [°C]	$\alpha$ [W.m <sup>-2</sup> .K <sup>-1</sup> ]	R [m <sup>2</sup> .K <sup>1</sup> .W <sup>-1</sup> ]	$\Delta$ [%]
Interior	Left	40	8	0,125	50
Exterior	Right	15	25	0,04	80

### 3.1 Simulations of the heat flux

To evaluate the insulating properties of the insulating materials, we have observed mainly the camouflaging potential of the insulating materials. This camouflaging potential is corresponding to a reduction of the vehicle's hull external surface temperature  $\Delta t_{pot}$  (Tab. 1). Concurrently we will observe an increase of the vehicle's hull internal surface temperature. This increase of the temperature is caused by using the insulating materials and we will mark it as  $\Delta t_{int}$  (Tab. 1). This parameter may substantially interfere with the comfort of the crew, but also to the reliability of the vehicle [4].

#### 3.1.1 Simulation Nr. 1

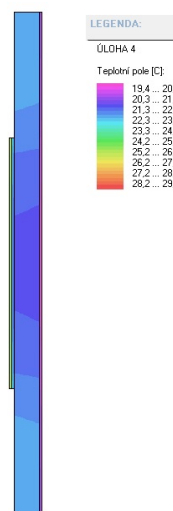
Modeled situation: A+P (Tab. 1). Situation description: Armor "2P" covered by the khaki camouflaging external paint (Fig. 2).

**Fig. 2** Geometry of detail, heat flux, thermal scale**Table 3** Table of the minimal and maximal temperatures in a horizontal axle

The armor without insulation		The armor with insulation	
Interior	Exterior	Interior	Exterior
$t_{i \min}$ [°C]	$t_{e \max}$ [°C]	$t_{i \max}$ [°C]	$t_{e \min}$ [°C]
23,11	20,37	-	-
$\Delta t = 2,74$		$\Delta t = -$	

#### 3.1.2 Simulation Nr. 4

Modeled situation: IF+TT+A+P (Tab. 1). Situation description: Armor "2P" covered by the khaki camouflaging external paint. The vehicle's hull is insulated from the inside by the insulating paint Thermal – Tec and the insulating aluminum foil Thermoflex (Fig. 3).

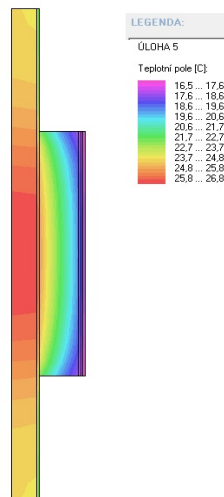
**Fig. 3** Geometry of detail, heat flux, thermal scale

**Table 4** Table of the minimal and maximal temperatures in a horizontal axle

The armor without insulation		The armor with insulation	
Interior	Exterior	Interior	Exterior
$t_{i \min }[^{\circ} \mathrm{C}]$	$t_{e \max }[^{\circ} \mathrm{C}]$	$t_{i \max }[^{\circ} \mathrm{C}]$	$t_{e \min }[^{\circ} \mathrm{C}]$
22,57	20,01	28,34	19,35
$\Delta t=2,56$		$\Delta t=8,99$	
Increase of the vehicle's hull internal surface temperature: $\Delta t_{\text {int }}=t_{i \max }-t_{i \min }=5,77^{\circ} \mathrm{C}$			
Reduction of the vehicle's hull external surface temperature: $\Delta t_{\text {pot }}=t_{e \max }-t_{e \min }=0,66^{\circ} \mathrm{C}$			

**3.1.3 Simulation Nr. 5**

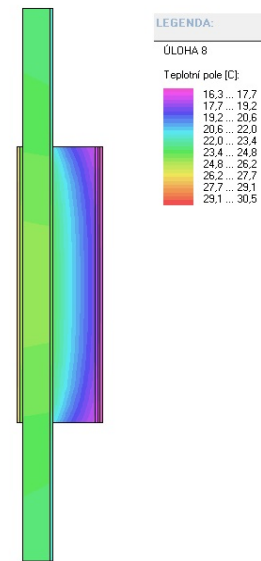
Modeled situation: A+P+AS+TT+SS+TT (Tab. 1). Situation description: Armor "2P" covered by the khaki camouflaging external paint. The vehicle's hull is insulated from the outside by the thermal shield that is fixed on the outside of the vehicle. The thermal shield consists of the steel sheet painted by insulating paint Thermal – Tec. Between the thermal shield and the hull there is an air space (Fig. 4).

**Fig. 4** Geometry of detail, heat flux, thermal scale**Table 5** Table of the minimal and maximal temperatures in a horizontal axle

The armor without insulation		The armor with insulation	
Interior	Exterior	Interior	Exterior
$t_{i \min }[^{\circ} \mathrm{C}]$	$t_{e \max }[^{\circ} \mathrm{C}]$	$t_{i \max }[^{\circ} \mathrm{C}]$	$t_{e \min }[^{\circ} \mathrm{C}]$
24,44	21,26	26,82	17,25
$\Delta t=3,18$		$\Delta t=9,57$	
Increase of the vehicle's hull internal surface temperature: $\Delta t_{\text {int }}=t_{i \max }-t_{i \min }=2,38^{\circ} \mathrm{C}$			
Reduction of the vehicle's hull external surface temperature: $\Delta t_{\text {pot }}=t_{e \max }-t_{e \min }=4,01^{\circ} \mathrm{C}$			

**3.1.4 Simulation Nr. 8**

Modeled situation: IF+TT+A+P+AS+TT+SS+TT (Tab. 1). Situation description: This situation is a combination of the simulations Nr. 4 and Nr. 5. Armor "2P" covered by the khaki camouflaging external paint. The vehicle's hull is insulated from the inside by the insulating paint Thermal – Tec and the insulating aluminum foil Thermoflex. The vehicle's hull is also insulated from the outside by the thermal shield that is fixed on the outside of the vehicle. The thermal shield consists of the steel sheet painted by insulating paint Thermal – Tec. Between the thermal shield and the hull there is an air space (Fig. 5).

**Fig. 5** Geometry of detail, heat flux, thermal scale**Table 6** Table of the minimal and maximal temperatures in a horizontal axle

The armor without insulation		The armor with insulation	
interior	exterior	interior	exterior
$t_{i \min }[^{\circ} \mathrm{C}]$	$t_{e \max }[^{\circ} \mathrm{C}]$	$t_{i \max }[^{\circ} \mathrm{C}]$	$t_{e \min }[^{\circ} \mathrm{C}]$
23,78	20,82	30,5	16,91
$\Delta t=2,96$		$\Delta t=13,59$	
Increase of the vehicle's hull internal surface temperature: $\Delta t_{\text {int }}=t_{i \max }-t_{i \min }=6,72^{\circ} \mathrm{C}$			
Reduction of the vehicle's hull external surface temperature: $\Delta t_{\text {ext }}=t_{e \max }-t_{e \min }=3,91^{\circ} \mathrm{C}$			

**3.2 Comparison of the measurement's results**

In the following table (Tab. 7) we can compare the results of measurements.

As the Table 7 shows, adding insulation layers to the armor from inside the hull of the vehicle reaches only minimal reduction of the external surface of the

vehicle (minimal camouflaging potential), but reaches an undesirable effect of increasing the temperature of the internal surface of the vehicle's hull.

**Table 7** Comparison of measurement's results

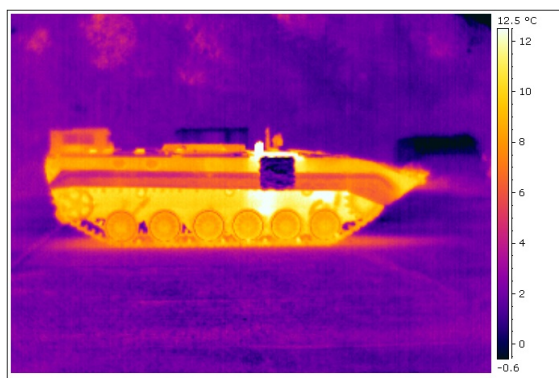
Simul. Nr.	Modeled situation	$\Delta t_{int}$ [°C]	$\Delta t_{pot}$ [°C]
1	A+P	-	-
2	TT+A+P	2,04	0,24
3	IF+A+P	4,57	0,52
4	IF+TT+A+P	5,77	0,66
5	A+P+AS+TT+SS+TT	2,38	4,01
6	TT+A+P+AS+TT+SS+T T	3,89	3,98
7	IF+A+P+AS+TT+SS+TT	5,79	3,92
8	IF+TT+A+P+AS+TT+SS +TT	6,72	3,91

A substantially greater potential for camouflaging reaches the use of the thermal shield, which is separated from the vehicle by an air-space. At the same time the application of the external insulating layers (the thermal shield) applied on the exterior of the vehicle increases the temperature of the internal surface of the vehicle's hull only minimally.

The simulations also showed an interesting fact that after application of the thermal shield on the outside, any additional application of the insulating materials on the inner side of the vehicle's hull appears as counterproductive. After application of the thermal shield, the more we isolate interior parts of the hull using insulating materials, the more we reduced masking potential  $\Delta t_{pot}$  and the more we increase the temperature of the inner surface of the vehicle's hull.

#### 4 EXPERIMENTS ON MOBILE MILITARY TECHNIQS

One of many solutions how to camouflage the mobile military technics is the thermal shield. We have designed a panel (Fig. 6) and fastened it on the hull of the vehicle OT-90 Hybrid.



**Fig. 6** Experiments with the thermal camouflaging

In the Figure 6 we can see the results of the experimental thermovision measurements [5].

#### 5 CONCLUSION

Camouflaging the military vehicle in the infrared area of the electromagnetic spectrum is not an easy task [2], [4]. To gain some helpful results it is necessary to make a lot of calculations, simulations and of course at the end it is necessary to make also the experimental measurements. As a result of our 10 years lasting research in calculations, modeling and experiments we were able to reduce the surface temperature of the BMP-2 in the area of the hull from 9°C to 5°C and in the area of the engine even from 15°C to 5°C. These results make a good potential for the next research in the area of thermal camouflaging.

#### References

- [1] FERSTL, K., MASARYK, M.: *Prenos tepla, Slovenská technická univerzita*. Bratislava : Nakladateľstvo STU, 2011. ISBN 978-80-227-3534-6.
- [2] DROPPA, P. et al.: *Potlačenie demaskujúcich príznakov vojenskej techniky a vojaka v IČ oblasti spektra. Záverečná správa / Sprac. Peter Droppa ... [et al.]*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2010. 132 s.
- [3] DROPPA, P., FILÍPEK, S.: Porovnanie a vyhodnotenie náterových systémov pre zníženie termovíznych príznakov vojenskej techniky = Comparison and interpretation paints systems for decreasing thermovision indications of military techniques. In *Science & Military*, Vol. 3, No. 1 (2008), s. 10-13. ISSN 1336-8885.
- [4] HOLST, G. C.: *Common Sense Approach to Thermal Imaging*, JCD Publishing 2832 Cove Trail, Winter Park, Florida 2000, FL 32789. ISBN 0-9640000-7-5.
- [5] DROPPA, P., FILÍPEK, S.: The application of new progressive technologies for military mobile technics camouflaging: In *Transport Means 2013: Proceedings of the 17<sup>th</sup> International Conference*. Kaunas : Kaunas University of Technology, 2013. ISSN 1822-296X. p. 297-303.

Eng. Samuel FILÍPEK  
Armed Forces Academy of general M. R. Štefánik  
Department of Mechanical Engineering  
Demänová 393  
031 01 Liptovský Mikuláš  
Slovak Republic  
E-mail: samko.filipek@gmail.com



Prof. Eng. Peter DROPPA, PhD.  
Armed Forces Academy of general M. R. Štefánik  
Department of Mechanical Engineering  
Demänová 393  
031 01 Liptovský Mikuláš  
Slovak Republic  
E-mail: peter.droppa@aos.sk

**Prof. Eng. Peter Droppa, PhD.** – was born in Liptovský Mikuláš, Slovakia, in 1960. He received the M.Sc. degree in 1984, Ph.D. degree in 2003. Assoc. Prof. position in 2007 and Professor in 2013 of the Brno University of Defence. He is currently head of the Department of Mechanical Engineering of Armed Forces Academy of general M. R. Štefánik, Liptovský Mikuláš.

**Eng. Samuel Filípek** - was born in 1987 in Bratislava, Slovakia. He received the M.Sc. degree in 2012 in Armament and Technics of Armed Forces from the Department of Mechanical Engineering, Armed Forces Academy in Liptovský Mikuláš. He is currently a PhD. student at the same institution. His research interests include the thermal camouflaging of mobile military technology. He is a project engineer for planning the conveyor technology at Volkswagen Slovakia, a.s. in Bratislava.



## FSTA 2018

### THE FOURTEENTH INTERNATIONAL CONFERENCE ON FUZZY SET THEORY AND APPLICATIONS

**January 28 - February 2, 2018**

Liptovský Ján, Slovak Republic

The 14-th Conference on Fuzzy Set Theory and Applications FSTA 2018 will take place under the auspices of the Department of Mathematics and Descriptive Geometry of Faculty of Civil Engineering of Slovak University of Technology in Bratislava, the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš and the Working Group for Fuzzy Set Theory and Applications of the Slovak Mathematical and Physical Association, in co-operation with EUSFLAT working group AGOP and SIPKES s.r.o.

#### INTERNATIONAL SCIENTIFIC PROGRAMME COMMITTEE

Chair persons: MESIAR Radko (Slovak Republic), SAMINGER-PLATZ Susanne (Austria)

#### SCIENTIFIC PROGRAMME

The Conference Scientific Programme will consist of special invited plenary lectures, invited and contributed parallel sessions. Rooms can be provided for workshops and special invited sessions during the conference. Please, send all suggestions for workshops and invited sessions to Prof. Radko Mesiar ([radko.mesiar@stuba.sk](mailto:radko.mesiar@stuba.sk)) no later than September 15, 2017.

More details: See the Conference website [www.math.sk/fsta](http://www.math.sk/fsta)