Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2463-9575
Junij 2016 – 18/št. 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2463-9575
UDK 355.5(479.4)(055)

Junij 2016 – 18/št. 2

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Izdajatelj Publisher	Generalštab Slovenske vojske General Staff of the Slovenian Armed Forces
Glavni urednik Executive Editor	generalmajor Alan Geder (OF-7)
Odgovorni urednik Managing Editor	dr. Liliana Brožič
Uredniški odbor Editorial Board	višja vojaška uslužbenka XIII. razreda dr. Valerija Bernik (OF-4) višji vojaški uslužbenec XIV. razreda dr. Denis Čaleta (OF-5) polkovnik dr. Tomaž Kladnik (OF-5) dr. Igor Kotnik polkovnik dr. Vojko Obrulj (OF-5) dr. Maja Garb
Sekretar Secretary	višja praporščakinja Nataša Cankar (OR-9)
Uredniški svet Editorial Council	dr. Andrej Anžič, Evropska pravna fakulteta, Nova Gorica dr. Gorazd Bajc, Narodna in študijska knjižnica, Trst dr. Anton Bebler, Fakulteta za družbene vede, Ljubljana dr. Damir Črnčec, Fakulteta za državne in evropske študije, Brdo dr. Bastian Giegerich, International Institute for Strategic Studies, London dr. Olivera Injac, Univerzitet Donja Gorica, Podgorica dr. Sergei Konoplyev, Harward University, Cambridge generalmajor v pokoju Ladislav Lipič (OF-7, ret.) dr. Julie T. Manta, US Army War College, Carlise dr. Thomas Mockaitis, DePaul University, Chicago dr. Klaus Olshausen (OF-8, ret.), Clausewitz-Gesellschaft e.V., Hamburg generalpodpolkovnik dr. Iztok Podbregar (OF-8), Fakulteta za organizacijske vede, Kranj dr. Tibor Szvircsev Tresh, Militärakademie an der ETH, Zürich dr. Thomas Young, Center for Civil-Military Relations, Monterey
Prevajanje Translation	Justi Carey, Vlasta Deželak Iris Žnidarič
Lektoriranje Proofreading	Služba za strateško komuniciranje
Oblikovanje Design & Graphic	Skupina Opus Design
Tisk Print	Prima Print d.o.o.
ISSN	2232-2825 (tiskana različica/print version) 2463-9575 (spletna različica/ on line version)
Naklada Edition	300 izvodov/copies
Revija je dostopna na spletni strani Publication web page	http://www.slovenskavojska.si/publikacije/ sodobni-vojaski-izzivi/ http://www.slovenskavojska.si/en/publications/contemporary-military-challenges/
E-naslov urednice Managing Editor e-mail address	liliana.brozic@mors.si

Prispevki, objavljeni v Sodobnih vojaških izzivih, niso uradno stališče Slovenske vojske niti organov, iz katerih so avtorji prispevkov.
Publikacija je uvrščena v bibliografsko zbirko podatkov COBISS.SI in PAIS International.

Articles, published in the Contemporary Military Challenges do not reflect the official viewpoint of the Slovenian Armed Forces nor the bodies in which the authors of articles are employed.
The publication is indexed in bibliography databases COBISS.SI and PAIS International.

MEDNARODNA VARNOSTNA SKUPNOST NA RAZPOTJU

»Zoperstavljanje hibridnim grožnjam ni zgolj vojaški problem, zato tudi obravnava ne more biti omejena samo na vojaško stroko, temveč zahteva sodelovanje vseh, ki se ukvarjajo z varnostjo v najširšem smislu.«

Vinko Vegič: Pojav in konceptualizacija
hibridnega vojskovanja, 2016, str. 89

INTERNATIONAL SECURITY COMMUNITY ON CROSSROADS

»Countering hybrid threats is not only a military problem. Therefore, their consideration cannot be limited solely to the military domain; it requires the engagement of all who deal with security in the broadest sense.«

Vinko Vegič: Emergence and conceptualization
of hybrid warfare, 2016, p. 89

VSEBINA
CONTENTS

7

Liliana Brožič

UVODNIK
MEDNARODNA VARNOSTNA SKUPNOST NA RAZPOTJU

11

Liliana Brožič

EDITORIAL
INTERNATIONAL SECURITY COMMUNITY AT THE CROSSROADS

15

Viktor Potočnik

ČETRTA GENERACIJA VOJSKOVANJA
Prvi del: GEOPOLITIČNI OKVIR SLOVENSKE VARNOSTI
FOURTH GENERATION WARFARE
Part 1: GEOPOLITICAL FRAMEWORK TO SLOVENIAN SECURITY

29

Staša Novak

NATO IN KIBERNETSKO ODVRAČANJE
NATO AND CYBER DETERRENCE

51

József Padányi
László Földi

IZKUŠNJE MADŽARSKIH OBRAMBNIH SIL, PRIDOBLJENE PRI RAZMESTITVI INŽENIRSKIH OVIR MED VSEEVROPSKO MIGRANTSKO KRIZO LETA 2015
LESSONS LEARNED FOR THE HUNGARIAN DEFENCE FORCES FROM THE DEPLOYMENT OF ENGINEER OBSTACLES DURING THE 2015 EUROPE-WIDE MASS-MIGRATION EMERGENCY

59

Metodi Hadji-Janev
Marija Jankuloska

IZZIVI UPORABE DRONOV V DRŽAVAH JUGOVZHODNE EVROPE
THE CHALLENGES OF DRONE USAGE BY SOUTHEAST EUROPEAN COUNTRIES

73

József Kis-Benedek

ISLAMSKA DRŽAVA IRAKA IN LEVANTA TER MEDNARODNI BOJ PROTI NJEJ
ISLAMIC STATE OF IRAQ AND THE LEVANT AND THE INTERNATIONAL FIGHT AGAINST IT

89

Aleš Avsec

CIKEL USPOSABLJANJA NAMENSKIH SIL BATALJONSKE BOJNE SKUPINE
BATTLE GROUP TRAINING CYCLE

107

SLIKOVNO GRADIVO
PHOTOS

115

AVTORJI
AUTHORS

121

NAVODILA AVTORJEM ZA OBLIKOVANJE PRISPEVKOV

127

INSTRUCTIONS FOR THE AUTHORS OF PAPERS

Liliana Brožič

UVODNIK

MEDNARODNA VARNOSTNA SKUPNOST NA RAZPOTJU

Mednarodna varnostna skupnost je na razpotju in nove prave smeri išče že nekaj časa. Ustaljene smernice delovanja so se spremenile, za nekatera področja pa se zdi, da jih preprosto ni več. Veliko dejavnikov je vplivalo na razmeroma visoko raven varnosti, ki smo jo zaznavali v zadnjih nekaj letih. Finančna kriza, ki je začela kazati svoje zobe v letih 2008 in 2009, je pomembno spremenila evropske oborožene sile, njihovo strukturo, organiziranost in razvoj. Mnogi so se tolažili, da to ne pomeni posebne težave, saj smo razmeroma varni. Raziskave javnega mnenja v Sloveniji so kazale zaznavanje ogroženosti predvsem zaradi naravnih nesreč in socialno-ekonomske ogroženosti. Postopoma, a vseeno razmeroma hitro, se je vse spremenilo. Spomladi leta 2014 je bil na Krimu referendum o njegovi priključitvi k Ruski federaciji. Začelo se je rožljanje z orožjem, ki je doživelo različne odzive v mednarodni skupnosti in vplivalo na spremenjene odnose med Natom in Rusijo. Te spremembe so bile tudi predmet razprave na vrhu Nata julija letos v Varšavi.

Že leta 2012 so začeli mediji vse pogosteje poročati o povečani migracijski problematiki v Sredozemskem morju in o težavah, ki jih je imela s tem pojavom Italija. Do konca lanskega leta so migracije z jugovzhoda dosegle neslutene razsežnosti in temeljito pretresle temelje Evropske unije. Nekateri teroristični napadi v evropskih mestih, ki naj bi jih organizirali in izvedli migranti, so pomembno vplivali na spremenjeno razumevanje nove (ne)varnosti. Nekateri so se novega razumevanja varnosti lotili znanstveno. Tako je npr. Obramboslovni raziskovani center na Fakulteti za družbene vede objavil rezultate raziskave o stališčih slovenskega javnega mnenja do varnosti, ki so jih ugotavljali leta 2015/2016. Med drugim navajajo, da je nedavna migrantska kriza vplivala na slovensko javnost, ki množične migracije, ilegalne in ekonomske priseljence dojema kot pomemben razlog za svojo zaskrbljenost. Avtorji raziskave ugotavljajo izrazito povečanje sprejemljivosti zamisli, da Policiji pri varovanju meje pred ilegalnimi prehodi pomaga Slovenska vojska. Pomembno veliko je tudi strinjanje z zamislijo o tem, da naj vojska pomaga tudi pri boju proti terorizmu, kar je bilo pred pojavom množičnih migracij nepredstavljivo. Kot navajajo avtorji raziskave, se je v zadnjih treh letih za dobrih 20 odstotkov povečala tudi podpora slovenske javnosti udeležbi Slovenije v mednarodnih operacijah in na misijah. Povečal se je tudi delež javnosti, ki podpira predloge za povečanje obrambnega proračuna. Pa se bo res in kako kmalu?

Na novo evropsko obrambno strategijo še kar čakamo. Čakamo na nove rešitve, na dogovore med političnimi odločevalci …

V vmesnem času pa pri različnih avtorjih nastajajo različne izkušnje. Nekateri so se odločili, da jih delijo z našimi bralci.

Viktor Potočnik se v članku *Četrta generacija vojskovanja: geopolitični okvir slovenske varnosti (1. del)* sprašuje, kako geopolitika vpliva na varnostne razmere v svetu, katera so sodobna varnostna tveganja in kako lahko vplivajo na Slovenijo. Slovenska vojska ima pri zagotavljanju nacionalne varnosti pomembno vlogo, zato se Potočnik sprašuje, ali je dovolj pripravljena, da se zoperstavi morebitnim tveganjem, in predstavi dejstva, za katera meni, da lahko ključno vplivajo na slovensko nacionalno varnost.

Kibernetske grožnje so ena izmed modernejših oblik ogrožanja varnosti. V prejšnji številki Sodobnih vojaških izzivov se je definiciji kibernetskih groženj posvetil Vinko Vegič**.** V tej številki nadaljujemo temo s člankom *Nato in kibernetsko odvračanje,* ki ga je napisala **Staša Novak**. Kot pravi, Nato v resnici uporablja nekatere elemente kibernetskega odvračanja, ki temeljijo na močni obrambi, deklaratorni politiki in odzivnih ukrepih. Ti pa ne pomenijo Natovih ofenzivnih kibernetskih zmogljivosti, temveč možnost za odzivanje kolektivne obrambe na kibernetski napad, pri čemer se uporabijo vsa razpoložljiva sredstva.

Povečano število migrantov na poti v boljšo prihodnost je presenetilo mnoge na Balkanu, čeprav so številne institucije in posamezniki opozarjali na to možnost. O nekaterih izkušnjah in odzivih naše sosede Madžarske sta **József Padányi** in **László Földi** napisala članek *Izkušnje Madžarskih obrambnih sil, pridobljene pri razmestitvi inženirskih ovir med vseevropsko migrantsko krizo leta 2015*. V članku sta se osredotočila predvsem na aktivnosti madžarske vojske.

V regiji Jugovzhodne Evrope je bilo nekaj primerov terorističnih napadov, pišeta **Metodi Hadji-Janev** in **Marija Jankuloska** in ugotavljata, da se je uporaba dronov pri zoperstavljanju terorizmu v svetu izkazala kot učinkovita. V članku *Izzivi uporabe dronov v državah Jugovzhodne Evrope* proučujeta možnosti njihove uporabe v domači regiji.

József Kis-Benedek je pripravil članek z naslovom *Islamska država Iraka in Levanta ter mednarodni boj proti njej,* v katerem nas seznanja z nastankom tega pojava in njegovimi pojavnimi oblikami v različnih državah na Bližnjem vzhodu, z njihovim odzivom in odzivom drugih mednarodnih akterjev, ki imajo svoje interese v tem delu sveta. Ne pozabi omeniti tudi vprašanja Kurdov in pojava prostovoljnih borcev, ki se prihajajo borit v Sirijo in Irak.

Bataljonska bojna skupina in evalvacija njenega usposabljanja sta motiv za članek z naslovom *Cikel usposabljanja namenskih sil bataljonske bojne skupine.* V njem **Aleš Avsec** primerja način usposabljanja pripadnikov te enote v Slovenski vojski z načinom usposabljanja podobnih enot v Združenih državah Amerike. Ali je primerjava med dvema tako različnima državama sploh mogoča?

Liliana Brožič

EDITORIAL

INTERNATIONAL SECURITY COMMUNITY AT THE CROSSROADS

For some time already, the international security community has been at a crossroads and looking for new right directions. The established operational guidelines have changed, and in some areas, it seems that they simply no longer exist. There are many factors which have had an effect on the relatively high level of security we have witnessed in the last few years. The financial crisis, which started to show its teeth in 2008 and 2009, has seriously changed the European armed forces, their structure, organization and development. Many comforted themselves that this does not constitute a significant problem, since we are relatively safe. Public opinion surveys in Slovenia revealed that most of all, people feel threatened by natural disasters and socio-economic situation. However, gradually but relatively quickly, everything has changed. In the spring of 2014, Crimea held a referendum on its annexation to the Russian Federation. The rattling of weapons began, provoking different reactions in the international community and resulting in altered relations between NATO and Russia. These changes were also discussed at the July NATO Summit in Warsaw.

Two years earlier, in 2012, the media increasingly reported on the soaring migration problems in the Mediterranean Sea and difficulties suffered by Italy due to those phenomena. By the end of last year, migrations from the Southeast reached unimaginable proportions and gave a profound shock to the foundations of the European Union. Some terrorist attacks in European cities, which were said to be organized and carried out by migrants, had a significant impact on the altered understanding of the new (in)security. Some experts adopted a scientific approach to the new understanding of safety. The Defence Research Centre of the Faculty of Social Sciences, for example, published the results of a survey on the opinions of the Slovenian public regarding safety, which was carried out in 2015/2016. Among other things, the findings show that the recent migrant crisis has affected the Slovenian public, which perceives mass migrations as well as illegal and economic migrants as an important reason of concern. The authors of the survey observed a marked increase in the acceptance of the idea that in the protection of borders from illegal crossings, the Police are assisted by the Slovenian Armed Forces. A significantly high number of people also agreed with the idea that the armed forces should help in the fight against terrorism which, before the occurrence of mass migrations, was unthinkable. According to the authors of the survey, in the last three years, the support of the Slovenian public to the participation of Slovenia in international operations and missions has also grown by more than 20 percent. In addition, the proportion of the public which supports proposals to increase the defence budget has gone up. But will it actually increase, and how soon?

We are still waiting for the new European defence strategy. We are anticipating new solutions, agreements between the decision-makers, etc.

In the meantime, different authors went through various experiences. Some of them have decided to share them with our readers.

In his article *Fourth Generation Warfare: Geopolitical Framework to Slovenian Security (Part 1)*,**Viktor Potočnik** explores the issue of how geopolitics impacts the global security situation, what are the contemporary security risks and how they can affect Slovenia. In ensuring national security, the Slovenian Armed Forces play an important role. Consequently, Potočnik raises the question of whether they have a sufficient level of readiness to withstand potential risks, and presents the facts which he believes can have a key influence on the Slovenian national security.

Cyber threats represent one of the most modern forms of security threats. In the previous issue of the Contemporary Military Challenges, Vinko Vegič provided the definition of cyber threats. This issue continues this theme with the article *NATO and Cyber Deterrence*, written by **Staša Novak**. According to her, NATO is *de facto* already pursuing certain elements of cyber deterrence based on strong defence, declaratory policy and responsive measures. However, responsive measures are not NATO offensive cyber capabilities, but the possibility of a collective defence response to a cyber attack, which implies a response with all available means.

The increased number of migrants on their way to a better future has surprised many people in the Balkans, although numerous institutions and individuals had warned of this possibility before. Some experiences and responses of Slovenia's neighbour, Hungary, are presented in an article by **József Padányi** and **László Földi,** titled *Lessons Learned for the Hungarian Defence Forces from the Deployment of Engineer Obstacles during the 2015 Europe-Wide Mass-Migration Emergency*. The article focuses mainly on the activities of the Hungarian armed forces.

Metodi Hadji-Janev and **Marija Jankuloska** point out that the region of South-Eastern Europe has witnessed some examples of terrorist attacks and observe that the use of drones for countering global terrorism proved to be effective. Their article

The Challenges of Drone Usage by Southeast European Countries examines the possibilities of their use in the home region.

In his article titled *Islamic State of Iraq and the Levant and the International Fight against It*, **József Kis-Benedek** discusses the origins of this phenomenon and its manifestations in various Middle East countries, as well as the response of those countries and other international actors who share an interest in this part of the world. He also calls attention to the question of the Kurds and the emergence of volunteer fighters who are coming to Syria and Iraq to fight.

The Battalion Battle Group and the evaluation of its training is the subject of the article titled *Battle Group Training Cycle*, in which **Aleš Avsec** compares the methods of training of these units in the Slovenian Armed Forces with the training of similar units in the United States of America. Is it even possible to compare two countries which are that different?

Viktor Potočnik

ČETRTA GENERACIJA VOJSKOVANJA PRVI DEL: GEOPOLITIČNI OKVIR SLOVENSKE VARNOSTI

FOURTH GENERATION WARFARE PART 1: GEOPOLITICAL FRAMEWORK TO SLOVENIAN SECURITY

Povzetek Pred vami je prvi od treh člankov, ki bodo obravnavali četrto generacijo vojskovanja. Te obsežne teme se bomo najprej lotili s postavitvijo geopolitičnega konteksta za Republiko Slovenijo z vidika novih varnostnih izzivov. Posebej se bomo v prvem delu ukvarjali s kontekstom spopada, na katerega bi se morali pripraviti in se ustrezno organizirati. V naslednjih dveh delih pa bomo podrobneje pogledali izzive, postavljene pred nacionalnovarnostni sistem in Slovensko vojsko v tem geopolitičnem kontekstu. Predstavili bomo nujne spremembe in mogoč pogled na njihovo uresničevanje v nacionalnovarnostnem sistemu in Slovenski vojski znotraj njega.

Ključne besede ***Geopolitika, Republika Slovenija, Slovenska vojska, četrta generacija vojskovanja.***

Abstract This is the first in a series of three articles dealing with fourth generation warfare. To understand the fourth generation warfare as it applies to Slovenia we will first set the geopolitical context in light of the upcoming security challenges. Specifically, the article in front of you deals with the context of conflict we should organize and prepare for. In the subsequent two articles we will look in more detail at the challenges facing the national-security system as a whole, and the Slovenian Armed Forces in particular. We will put forward proposals for some of the required changes in the national-security system and the SAF.

Key words ***Geopolitics, Republic of Slovenia, Slovenian Armed Forces, fourth generation warfare.***

Introduction

"Just as Alexander's exploits only reached the Middle Ages as a dim, fantastic tale, so in the future people will probably look back upon the twentieth century as a period of mighty empires, vast armies and incredible fighting machines that have crumbled into dust" (van Creveld, 1991, str. 224).

Very little has been written on geostrategic and geopolitical situation of the Republic of Slovenia (RS). This is in our opinion essential to understand and grade the long-term suitability of the solutions in its national-security system. Especially the answer to the question of what kind of war can we expect and how do we conduct it? What is war in the 21st century? And what does it all mean for the RS and its armed forces in particular? For the Alliance (NATO) as a whole the answers to the questions above are pretty clear and can be found in the publication such as the Framework for Future Alliance Operations (2015). We, however, do not have such an analysis at a national level to use as a base to transform and/or develop the national-security system and the Slovenian Armed Forces (SAF) in particular. Pieces of information on the subject can be found in political and strategic documents of the RS. The Resolution on National Security Strategy (2010) and Defence Strategy (2012) include a short geopolitical analysis, a description of security threats and even a statement that the probability of state on state conflict has diminished considerably while at the same time the asymmetric threats coming from non-state actors have grown considerably. (ReSNV, 2010, & OS, 2012) Despite that they do not envision any changes necessary to national-security system corresponding to these new realities. We can only assume that the assessment of the political and strategic level in RS is that the entire national-security system and the SAF within it is perfectly capable of dealing with the new realities and the upcoming threats. The migrant crisis in the EU has proven even to the general public that this could not be further from the truth. The above-mentioned documents are of course political in their nature and from those we have come to expect big words and statements about the changing world, without offering any real solutions or priorities to face those changes.

Therefore, it is our aim to look at these key questions concerning the national-security system in the RS through geopolitics. How geopolitics affects the RS, and how it looks at the threats facing the SAF. We will try to answer the question of what kind of conflict we can expect on the territory of the RS, within the wider conflict expectations of the Alliance. This should provide us with an idea of how to appropriately train, equip and organize the SAF. In the conclusion to this part we will try to offer the direction of the system changes necessary in our national-security system.

1 CURRENT SECURITY (HYBRID) THREATS

To better understand the geopolitical context we have to understand the current and future security environment. The current security environment is diverse, complex and dynamic (Kotnik, 2012, p.14). We believe that the key to understanding it is to first understand that a nation-state is no longer the dominant player in geopolitics. Next to it we have international organizations, international corporations, international non-governmental organizations and other non-state actors (even individuals) with regional and global ambitions. However, all these human actors are not the only ones representing different security challenges. Climate change, natural disasters, and health crisis (epidemic outbreaks) come with their own security challenges independent of human will.

In describing the current security environment we most often come across the term “hybrid threats”. However there is no unifying definition as to what the term means. NATO talks about hybrid warfare, while the EU talks about hybrid threats. At the same time NATO doctrine uses the term asymmetric threat, defining it as “A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result” (AAP-06, 2013, p. 2-A-20). We can even say that the 28 NATO member states cannot come to a consensus as to what hybrid threat and hybrid warfare are. (Puyvelde, 2015) Schadlow even says that there is nothing new to the terms, and that in speaking of hybrid threats/warfare we mean nothing but a complex mix of already known forms of warfare (Schadlow, 2015).

We believe that the scope of warfare has changed and that it involves all elements of a functioning society on a level never seen before. The national-security systems need to be ready for an enemy, which will act in not only the military spectrum, but at the same time in information/cyber space, using the psychological and economic operations and all other elements of (national) power at his disposal. And above all he will not recognize any sovereignty of a nation-state, and by that the lines between internal and external security are/will become blurred.

2 GEOPOLITICAL/GEOSTRATEGIC CONTEXT

»Geopolitics is about perspective. It is about how one views the world«
(Sempa, 2002, str. 4).

Size of a county is an important fact in geopolitics, but by far not the most important one. Historically some of the world’s largest countries have never been geopolitically important and vice versa some of the smaller ones have been. As Sempa would say »Geographical position—where a country is located relative to other countries—is more important than size« (Sempa, 2002, p. 5). Other factors, influencing its ability to pursue its interest on a world stage include the size of population, economy, technology, military power and the form of rule. However all other factors, except geography, change in time. Only the geographical position remains constant, even though its value can change in time (Sempa, 2002).

At first glance it seems irrelevant to consider geopolitics in cases of a small country like Slovenia, with limited sources to influence or conduct its own geopolitics. That may even be true. However this does not mean that we should be indifferent to world geopolitics. Geopolitics of the great players has a profound influence on small countries like Slovenia. For example, the case of the migrant crisis in 2015, which was not caused or influenced by Slovenia, has had a profound influence on the perceptions of (in)security of its population. Geopolitical theory influences the conduct of nation-states and other players in the international system in choosing their foreign policy, identifying possible threats and responding to them, and finally even how the wars are being conducted. The most famous are the geopolitical theories of sea power by Alfred

Thayer Mahan and World Island by Halford Mackinder. Mahan's theory is based on the premises that the greatness of a nation is directly linked to its ability to control world oceans in peace and war. In that the key role is placed in the ability to control key locations (straits, canals, ports) and in the combat power of fleets (Mahan, 1890). In contrast, Mackinder's theory states that only a land power can have a lead in world affairs. His theory is based on the idea of a world divided into two parts; the World Island, consisting of Eurasian continent and Africa, and Periphery of islands including Americas, Australia, Japan, Great Brittan and Pacific islands. It can be summed up in a statement "Who rules Central and Eastern Europe rules the Heartland. Who rules the Heartland rules the World Island. Who rules the World Island, rules the World." Heartland is the key due to its size and available resources which give it a safe base to develop a superpower. All outside invaders would have a hard time coming to the industrial bases within the Heartland. At the same time the Heartland has the advantage of inner-lines while defending (Huges & Heley, 2015). Nicolas J. Spykman criticized Mackinder that the Heartland is too underdeveloped and inaccessible to play a key role in controlling the world. According to Spykman, the control over Heartland is still important, but to control it one needs to control the Rimland (e.g. Mackinder's Inner crescent). (see Picture 1) Spykman's theory was a base for the US politics of Containment, with which it contained the Soviet influence after the WW II (Gray, 2015). There are a number of other geopolitical theories from Kissinger and Brezinski in US to Ratzel and Haushofer in Germany etc. For our purposes it is also good to know the theories advocating the link on Berlin-Moscow-Tokyo (or today Beijing) axis, which would connect the Eurasian continent into a whole controlling the World island. The latter is of course not in the interest of the US and some other EU players. Without the US, France and UK cannot compete with Germany and Russia, and without the EU, the US are risking of becoming an island off the coast of Eurasia.

Russia is at the core of the Heartland, and as such plays an important role regardless of who rules it or what its current political system is. With that in mind, it is important to know its geopolitical theory. Today, Russia is extremely sensitive to what it considers its "near abroad". The Russia's 'near abroad' is not defined as such, but roughly we can claim it represents all the countries established after the break-up of the Soviet Union. Some of these countries today are members of NATO and others aspire to be one. The central role for Russia and the theory of the World Island plays Ukraine, which among other things represents substantial food reserves for the World Island. Russia is undoubtedly not pleased with NATO's eastward expansion and what it considers interfering in its near abroad (Lukin, 2014). An important role in Russian geopolitical theory is also played by what is referred to as the geopolitics of Islam, which of course Russia is actively opposed to (Dugin, 2015). In combating it, it is considering cooperation with the US, which otherwise are its geopolitical arch enemy (See Picture 1, p. 108).

As already stated, in geopolitics, the geography is not the only important factor. Culture, religion, economy, demographics, climate, natural resources and even history play a role in this respect. And today, we can see the worldwide effects of climate change, driving the migrations and possibly even changing what is referred to as the Pivot region controlling the World Island. In theory, there are many different opinions as to what the Pivot region is. At the same time, Fukuyama warns that it would be unwise to consider Huntington's model of the clash of civilizations without reservations. Reality is far more complicated (Lukin, 2014, p. 5). The players on the geopolitical chessboard are using all the instruments of national power available (regardless of whether they are a nation-state or not) in the form of influence (soft) or coercion (hard), as well as smart power (Kotnik, 2012).

We, however, believe that all this theory lacks certain modern elements, technology being one of the most obvious ones. In the military sense, cruise missiles, long-range rocket artillery, as well as electronic and cyber warfare render the classical strategic depth irrelevant. The industrial and other potentials in strategic depth are no longer safe, and due to the advances in technology, it is no longer necessary to set foot on enemy territory to economically and socially cripple them. However, technology has had influence on other aspects of geopolitics; modern communication links, satellite links and cyber space with instant access to information. All this provides an option to bypass a certain territory, decreases the importance of geographical location, and globally delocalizes human activity (Balažic, 2001). But only at first glance. As Balažic has stated, there are forces actively opposing this. A decade and a half after Balažic had written his article, we can certainly say that the geographical position is still very relevant in geopolitics and/or geoeconomy.

Non-state actors are relatively new to geopolitics, but they interfere with geopolitical interests of great powers and have completely their own views and strategies. Above all, many of them do not recognize state borders or the rules of warfare set up by nation-states in centuries after the peace of Westphalia (1648). With them and hybrid warfare coming onto the stage, the lines between internal and external security have become blurred. As stated by van Creveld, it is the first duty of any civilized society to protect the lives of its members. Nation-states will have to adapt to that and find the solutions for the new forms of low intensity conflicts with non-state actors or they will disappear (van Creveld, 1991). This, however, is nothing new. Prior to the peace of Westphalia (1648), war in Europe was waged by very different actors; families, clans and tribes, as well as ethnic groups, races, religions and cultures, and even business ventures. Legally and illegally. These wars had often many sides, not just two, and alliances changed all the time. Not only different entities were at war, but the means of conducting war were very different as well. Only a few of these non-state actors had armies in today's sense available to them (Lind & Thiele, 2015).

However, we believe it is not important which theory is right and which is wrong. What is important is to realize that the actors on the geopolitical arena use them to identify their own strategic interests. What they have in common is the struggle for supremacy – locally and/or globally. If globalization is a fact, although many would disagree with that, there is still a question under whose leadership it will happen. It is not self-evident that this will be the USA. Other powers such as Brazil, Russia, India and China (BRIC) are actively opposed to that. We believe that a multipolar world with several powerful actors pulling their strings is far more probable. Spykman's Rimland represents an area of the greatest competition between great powers, while at the same time containing several powerful actors of its own. The regions of Central and Eastern Europe and the Middle East within it are the key areas affecting the security position of Slovenia.

At the same time, the climate change could induce some unexpected factors into geopolitical equations. With them, the Pivot land could change – where to, however, still remains uncertain. Access to water could become a major factor. At the same time, the rise of temperature in the Arctic Circle, could drastically change the position of the Heartland (Russia), if it would suddenly gain a permanent and uninterrupted access to world oceans in the North. Climate change may also have a magnifying effect on migrations currently driven largely by globalization and desire for a better life, and, on a smaller scale, the wars in the Middle East and Asia. Migrations could, especially in Central Europe, completely change the demographic picture. Some may consider the current migrant predictions for 500 million EU irrelevant. However, as every organized football supporter will tell you, you need only a small group of a few hundred well-organized supporters on a stadium to have the whole thing of tens of thousands people on their feet and screaming. In this regard, the peaceful majority is irrelevant. This also explains what happened in eastern Ukraine, where the Russian speaking population was minority and peaceful in practically all the regions. However, a few thousand Russian Special Forces and various volunteers have turned things upside down. Having this in mind, it would be ill-advised to underestimate the organizational capabilities and motivation of Islamic fighters fighting in the Middle East for more than a decade, who instinctively understand modern warfare. We believe they will prove to be a huge headache for us.

3 GEOPOLITICAL POSITION OF SLOVENIA

In geopolitical terms, Slovenia lies within the Rimland, i.e. within the area whose control means the control over the World Island. To be more exact, Slovenia lies on the edge of this area, and edges are often more exposed to major earthquakes. Looking at Mackinder's theory, we lie on the edge of Central and Eastern Europe. We are also situated on the edge of the Balkan Peninsula, where, according to Huntington, three major civilizations meet (western Christianity, Orthodoxy and Islam) (Huntington, 1996). The territory of Slovenia also represents the crossroads of the four major geographical features: the Alps, the Balkan Mountains, the Mediterranean and the Pannonian lowlands. Slovenia is also at the crossroads of three major cultures: Romanic, Germanic and Slavic. We can also find influences of both Central and Southern Europe, each with its distinctive functioning patterns. Slovenia also represents the shortest communication link from Central to Southern Europe and across the Balkans to the Middle East. Two pan-European traffic corridors run across

Slovenia, namely the fifth and the tenth (Godec, 2010).[1] The German geopolitical thought has always considered Slovenia to be a part of their "Mittleeuropa", stretching from the Baltic to the Adriatic (Balažic, 2001, p. 235). Italy, on the other hand, is within NATO a strategic partner for Slovenia on the Alliance's southern flank. As stated by Balažic, Slovenia is "geopolitically positioned between the Alps and the Adriatic, and between Pannonia and Padania, which represents an intersection of a relative stability with patches of instability, the latter stretching from the Balkans to the borders of China" (Balažic, 2001, p. 232). Slovenia is in a classical geopolitical sense a midget; however at one point before the outbreak of the great economic crisis in 2007, it had the opportunity to become a geoeconomical regional power (Balažic, 2001). Unfortunately, this status and opportunity was unwisely wasted. Slovenia is also with no strategic resources of its own, with the exception of water and wood (Ponjavič, 2012, p. 44), which have to be protected rather than used and do not represent a viable source form which to finance national-security system.

Slovenia lies in the intersections of many interests. In the European part of NATO, we have several militarily relevant players; three major ones (UK, France and Germany), and Italy together with Poland. While France and UK have not only regional but also global ambitions and Germany is a bit reserved in its global ambitions, Italy and Poland on the other hand represent two different orientations within the Alliance. Italy focuses on the south and the Mediterranean, while Poland focuses on the east and Russia. Considering the current security challenges and their geographical position, this is perfectly normal. All other Alliance members more or less follow one of the two (Keohane in Thränert, 2016). For Slovenia, both Italian and German geopolitical orientations are important, and they are both the result of US geopolitics (Balažic, 2001). Such is our geostrategic position. This, however, means that we are torn between orienting to the south and/or east and we have no easy pick.

Because of this east-south division, our national-security system and the SAF within it need a clear prioritization of threats and geostrategic direction. This can only be given by a responsible and informed politics – statesmanship. Indecision and division in our orientation (east vs. south) are a cause for discomfort, confusion, irrational spending of limited resources and inability to make the right decisions at the right time. The confusion is clearly visible in our contributions to NATO force and command structures. We have a battalion battle group affiliated into the Alliance's southern flank (NRDC-ITA[2]), we are contributing to Italian-led VJTF[3], and together with Italy as a lead nation participate in EU defence capabilities. At the same time, we have affiliated NBC battalion to MNC NE[4], declared that we will participate in the eFP[5] and are exploring options of how to contribute further to the Alliance's

[1] *To this corridors additional two TEN-T corridors are linked; Baltics-Adriatic & Mediteranium corridor.*

[2] *NRDC-ITA – NATO Rapid Deployment Corps Italy*

[3] *VJTF- Very high readiness Joint Task Force*

[4] *MNCE – Multinational Corps Northeast*

[5] *eFP=enhanced Forward Presence*

eastern flank.[6] As these two represent dramatically different operational zones, the confusion in the SAF is complete. Hopefully, everyone can see at first glance that the SAF is not in a position to simultaneously participate in both operational zones. The SAF is in dire need of a clearly defined strategic direction.

4 FOURTH GENERATION WARFARE – WAR WE CAN EXPECT

In the fourth-generation warfare (4GW) nation-states are faced with a broad spectrum of threats from high-intensity conflict to terrorism. To understand why we are speaking of 4GW, we first have to determine how we understand the first three generations of warfare. The first generation is represented by armies fighting in a highly regulated battlefield using the tactic of line and column. It sets the foundation of what we today understand as the military culture – uniforms, drill, saluting. The second generation warfare is represented by armies cultivating the doctrine of firepower and attrition. The French developed such an army during the First World War. This is an army that has an inward focus, stressing the power of orders, rules, processes and procedures. Most of the nation-state armies today, including the US Armed Forces and all NATO countries, fit within this category. The third generation is represented by armies cultivating maneuver warfare, started by the Germans during the First World War, and fully developed during the second. Maneuver warfare is outward focused, on a situation, the enemy and the result. Leaders on all levels are expected to produce results regardless of the details of the orders given to them. The third generation values initiative and self-discipline as opposed to following procedures and imposed discipline. All 4GW armies are free of the first generation culture of order, focused outward not inward as second generation armies, value initiative and self-discipline and are therefore highly decentralized. Second generation armies are largely helpless against them.

We will analyse 4GW in more detail in our next article. For now we have to understand that at the core of 4GW lies not a military evolution but a political, social and moral revolution; crisis of the legitimacy of the state (Lind & Thiele, 2015). The goal in 4GW is the destruction of the moral fibre, which enable the society to exist (Vandergriff, 2006, p. 45). Hybrid warfare is a tool used by actors in 4GW. Hybrid warfare as we understand it combines conventional forces and technologies with non-state actors, criminal groups, Special Forces operations, information operations, cyber-attacks and other sources of asymmetric warfare. In it, we have not only many players at the same time, but also many different sides. The essence of hybrid warfare is not that the asymmetric approach dominates the conventional one, but that the

[6] *At this point one should distinguish cooperation in terms of training and exercises conducted within the framework of RAP (Readiness Action Plan) and it's »Assurance Measures«, and the participation in NCS (NATO Command Structure) and NFS (NATO Force Structure) designated for the NATO eastern flank. Training and exercises regardless of location provide us with enhancing our capabilities and Alliance interoperability, while at the same time sending a clear message of Alliance unity to our adversaries. On the other hand participation in selected NCS and NFS gives a message of a strategic direction, and we should be very careful with assigning our very limited resources to those.*

actors are choosing a method that is best suited for the moment chosen and for which they believe will give them the best results with the minimum of effort required.

In a world as interconnected as ours, nation-states have no economic and political motivation to entangle themselves in classical state-on-state high intensity wars. This, however, does not mean that they would not be ready to use all the instruments of national power (DIME + 6)[7] indirectly or directly through proxies (proxy wars), if they had such a geopolitical or other interest. And more importantly, nation-states have lost their monopoly over the use of force in pursuing their goals. Non-state actors such as various religious movements (e.g. ISIS), terrorist organizations (e.g. Al Kaida) and criminal gangs (e.g. drug cartels) have the resources and the motive to use force and destabilize nation-states (Sokolosky, 2015).

Russian Federation is a threat to Slovenia, because it represents a direct military threat to our allies within its near abroad. This has to be perfectly clear at least to our statesmen if not to the general population and politicians. Not even at the height of its might as Soviet Union, Russia never set foot on our territory (with a small exception of Prekmurje). In the current geostrategic situation and with the current geopolitics of the Russian Federation, the probability of the SAF facing armed units of the Russian Federation on the territory of Slovenia is almost non-existent. However, Slovenia is NATO and EU member, and therefore a potential Russian enemy. It is in our strategic interest that NATO and the EU remain firm and cohesive. Without them, we are extremely vulnerable militarily, politically and economically. Without NATO, Slovenia loses the nuclear umbrella, loses the security of its airspace, and loses the security provided by the large community. As such, it would become susceptible to all kinds of threats from conventional attacks (even from its now Alliance neighbours) to low intensity conflicts. This means that Slovenia has to be ready to carry its fair share of burden in the defence of all members of the Alliance, even those within the Russian near abroad. Even though their security interests at first glance have nothing to do with Slovenia or even actively oppose our security interests, the failure of the Alliance in those states would mean the failure of the Alliance as a whole. And that could lead into the disintegration of the Alliance and Slovenia would all of a sudden have to face all the threats on its own, with the national-security system as it is. A functioning Alliance is an absolute priority for Slovenia, and we have to demonstrate that to our allies. Only actions matter in this regard, and the actions are linked to fulfilling our commitments and obligations towards our allies. This, however, does not mean that by fulfilling them we will meet all our security needs.

For Slovenia (and the SAF), climate changes, migration trends, and demographic and social changes in the region of the western Balkans, at the edge of which we are situated, and along the southern flank of NATO (from Turkey to Libya), represent

[7] *In addition to classic instruments of national power (diplomacy, information, military, economics) Kotnik lists additional six instruments (moral power, socio-cultural and ideological power?, natural resources, geostrategic position, size and quality of population). (Kotnik, 2012, p.19)*

more direct future security challenges. As the violence in the Middle East does not seem to be losing ground, we can expect to see changes along civilization boundaries and in the key regions that will bring more conflicts within some countries on the one hand, and between state and non-state actors (the latter originating within or outside the countries in question) on the other, i.e., more low-intensity conflicts that have represented the bulk of fighting since 1945 (See Picture 2, p. 108).

Slovenia as a transit country could expect to see various aggressive groups with different (even criminal) background. Undoubtedly, they are already operating on our territory despite the formal assessment that the security situation is under control. Slovenia may not be the final destination for these groups. Nevertheless, it does represent a transit and logistical hub, maybe even a safe zone to recuperate and train. However, if they assessed that their interests were significantly endangered, we should expect a violent reaction in terms of taking control over the key locations in all directions in order to continue the transfer of people, money, arms and other resources into what they see as their objectives, or in order to control some of the key resources – e.g. water. These are non-state, even criminal, groups with semi-military or paramilitary formations with strong identity/ideology, a clear goal and a stable source of income. In short, some of the more common actors in 4GW warfare dominated by low-intensity conflicts.

Picture 2 represents the geographical position of Slovenia and its security perspective in terms of key security events in the regions affecting our geopolitical assessment[8]. As stated before, in geopolitics, solely a geographical perspective is not enough even though it represents the base. We believe that the combination of geographical position together with some of the key security events and migration currents gives us a relevant security perspective for Slovenia.

Slovenia cannot have a national-security system designed for an area long gone by. It simply is not reactive enough and it does not provide a sufficient pool of people to guarantee the security of individuals and a society as a whole. Let us again emphasize – at the core of 4GW there lies a crisis of the legitimacy of a state. Citizens denying the legitimacy of a state, from whatever reasons, knowingly or unknowingly destabilize the basic fabric linking the society as a functioning whole, and many of the players in 4GW are more than ready to take advantage of that. A small country like Slovenia has to ensure its own legitimacy and actively take over the responsibility to provide its own security and the security of the citizens. This responsibility cannot be transferred to a one or two subjects within the country (be it Police or the military), let alone to transfer it entirely onto other alliance members.

Slovenian national-security system and the SAF as its integral part are modelled to react to a second generation conflicts, and are totally inappropriate for 4GW hybrid conflicts (in its low- and high-intensity version). The political debates and statements

[8] *The circles represent an approximate distance of 500 km and 1000 km respectively from Slovenian borders.*

during the recent migrant crisis show complete political unawareness of the scope and nature of the problem, when, during such crisis, we could follow a debate on the formal status of the armed forces, on whether or not SAF members can even participate in internal security matters. At the same time, nothing was said about the required system level changes, to ensure appropriate responsiveness to 4GW threats.[9] The existing solutions are inappropriate and do not allow an effective reaction to 4GW threats when required. [10] Even the highly contested powers granted to SAF in Article 37a of the Defence Act are in fact totally irrelevant.[11] SAF members (by law required to be unpunished citizens of the Republic), in spite of Article 37a, do not even have the powers granted to municipally constabulary or department store security guards.[12]

Conclusion

»It takes farsightedness and guts to build an armed force that will only be called to fight *in, say, a decade. One has to guess, as best one can, what resources will be available, what kind of* opponent the forces will be called on to face, and what kind of environment they will have to *operate in*« (van *Creveld, 1991, p. 117).*

In 4GW, there are no clear boundaries between war and peace, or between military and non-military means to conduct wars. The lines between external and internal security are blurred. Countries that choose to wait with the activation of their full security potential until a state of emergency or formal war is declared are doomed to lose. A nation-state must ensure its own legitimacy and must set up a national-security system in which there is no strict division between the actors in peace (police) and the actor in war (military). In 4GW we are faced with warfare that recognizes no clear limits and touches all the segments of a society. That means, there are no more safe zones or protected groups, and no clear limits between peace, crisis and war. Therefore, it is crucial that nation-state's institutions entrusted with security have all the necessary powers to protect the citizens and the whole society in all eventualities that may arise. The national-security system actors in Slovenia need to be uniformly

[9] *We do not consider a parliamentarian »science fiction« debate on National guard to be a relevant debate on system level changes.*

[10] *As already stated, the line between peace and war in 4GW is blurred. Waiting for a state of emergency or war to be declared in order to effectively put the armed forces into use, is putting the latter in an impossible position. The public expects and demands the Army to be used as soon as the problem arises, without waiting for politicians to make up their mind.*

[11] *Defence Act Article 37a. grants the following special powers to the Army: to warn, to direct, to temporarily limit the movement of persons; to participate in controlling groups and masses. Following that, we could find no source detailing these powers and the SAF had a few problems formulating the Rules of Engagement within these powers. SAF members also have no power to identify a person nor do they have any power to use force when necessary.*

[12] *The requirements for municipal constabulary are set in Article 2 of the Policy on conditions to work as a municipal constable, and for Security guards in Article 32 of Private Security Act. Based on these the security guards and constables do not need to be citizens of Slovenia and they can be previously punished for smaller crimes. At the same time they have far bigger powers when dealing with citizens. Article 10 of the Municipal constabulary Act lists the powers of constables: warning; verbal order; establishing identity; security check; confiscation of objects; holding a suspect of a crime; the use of force, handcuffs, and pepper spray. While the security guards have the following powers according to Article 45 of Private Security Act: warning, verbal order, establishing identity, overall check; denying access to or exit from a secured area; holding a person; the use of physical force; the use of handcuffs.*

directed. Not through a single Department/Ministry, as suggested by Podbregar (Podbregar, 2011), but in a way that will allow one institution/department to direct and coordinate all the activities of different institutions/departments in a national-security system. Only this will ensure appropriate coordination and responsiveness. Not as it is now the case in Slovenia where as a matter of principle all the players are equal (with one in the lead) and a consensus is required on principle before anything can move forward. Looking for a consensus takes too much time, time that is not available. With that in mind, a democratic society must not forget that there is a need for civilian control over the uniformed structures [13]. Perhaps in a small country like Slovenia this is even a bit easier, since none of the subsystems is uncontrollably big. We will discuss in more detail the key elements of 4GW and the changes they require in national-security system in our next article.

The decision makers in Slovenia will have to realize the importance of the right balance of the instruments of national power. Neglecting one, in our case military, leaves consequences on all the others. A much broader consensus has to be reached realizing that military instrument of national power is not just about hard power and its ability to conduct wars. It also preforms various other soft functions in support of the other instruments of national power. We cannot deny its great symbolic value in support of diplomatic instruments[14], economic instruments, the moral power and socio-cultural influence on society's consciences. Other small countries like Switzerland and Singapore, can serve as an example in how this is to be done.

We believe that Slovenian national-security system is not ready for 4GW threats, that it is not in control of what is going on and that it is completely inappropriate to effectively face them. In 4GW, we are talking about conflicts that are military by nature, even though they are also being conducted by non-state actors and by instruments that are not strictly military. Slovenian police is not organized, equipped or trained to combat 4GW enemies. The SAF is a bit better organized and equipped for 4GW opponents, but it is at the same time totally untrained to face them.[15] As for the intelligence agencies, we can only guess in what state they are, but we have no reason to assume the conditions are any better than in the uniformed structures. Here, a careful observer can detect a systematic neglect of capabilities.

To be successful in 4GW, the SAF will have to adapt. A change in the organizational culture, which is now a typical second-generation culture focused on the processes, formality and waiting for orders, is of essential importance. This is not to say that processes need not be known, that procedures are not there to ensure security of own

[13] *This is most often done through the authority to allocate resources and controlling their spending.*

[14] *Even a relatively small military contribution goes a long way in diplomatic terms.*

[15] *The statement is impossible to verify through open sources. The information on such level of capabilities is confidential in any country. We, however, do not base our statement on such information, even if it does exist in Slovenia. We base it on a comparative analysis of what we believe is necessary for the success in 4GW as well as on the publicly available reports on the condition of different elements of Slovenian national-security system. We will explain this statement further in our next articles.*

forces or that orders are not important. On the contrary, this only means that they are not the beginning and the end of things, and that initiative, self-discipline and focus on the result are of far bigger importance. For that a leap forward in military education and training will be necessary. It will have to create self-disciplined, thinking and adaptable leaders, capable of reacting to all variations of hybrid warfare in a timely and accurate manner. For this purpose, we would recommend that the "Adaptability Course Model" be examined (Vandergriff, 2006). We will discuss the necessary changes and possible solutions in more detail in the last (third) article of this series.

All this still leaves the question of quality vs. quantity open. Do we need a small professional structure or do we need a larger segment of society involved in national-security system. We believe it is not a question of either-or, but a question of how to have both, as stated by Kotnik in his article (Kotnik, 2015). The legitimacy of a country, in the security sense, can only be ensured if a large enough portion of the population is included in security structures in any of the many possible ways. In addition, 4GW is largely represented by low-intensity conflicts, where the control of territory with soldiers is absolutely essential to ensure the legitimacy of the state. Modern technology can help in the surveillance of the territory, but it cannot be used as a substitute for human presence. On the other end of 4GW spectrum, however, we have conventional high-intensity conflicts. The SAF can only take part in these with highly trained and suitably equipped formations - e.g. battalion battle groups. And the SAF can only enter these as a part of the Alliance in which it will take its fair share of the burden. Slovenia cannot act alone in any kind of global or regional high-intensity conflict. A place at the table when such a conflict is over will only be earned if we carry our fair share of the burden. And this part of the SAF needs to be and needs to stay professional. It also needs to have the absolute priority in terms of capability building. Without the Alliance, the price of security is going to be considerably higher or we will stay without it and without our own country. We also have to realize that Alliances are not forever. And when they are gone, one has to build new ones under new conditions and with new obligations. Or one has to fully rely on its own forces. The latter is usually unavoidable in a short term. And that is why Slovenia's national-security system cannot be based solely on our Alliance contributions, but has to have the capabilities to act independently in defence of the country when and if required.

Bibliography

1. *Balažic, M., 2001. Velika Slovenija: Klasični in novi geopolitični koncepti. V Teorija in Praksa let.38, 2/2001, str. 231–243.*
2. *Bukkvoll, T., 2015. Military inovation under authoritarian goverment – the case of Russian Special Operations Forces. V The jurnal of strategic Studies, str. 602–625. Volume 38, August 2015.*
3. *Dugin, A., 2015. Last War of the World-Island; The Geopolitics of Contemporary Russia. Arktos, London (Kindle book).*
4. *European Commission – Directorate General for Mobility and Transport, 2013. The core network corridors – Trans European transport network 2013. Dostop: http://www.tentdays2013.eu/Doc/b1_2013_brochure_lowres.pdf (21. 2. 2016).*

5. *Godec, A., Jurše, L., 2010. Evropski prometni koridorji preko Republike Slovenije in nova železniška proga Divača – Koper. V zborniku; 10. SLOVENSKI KONGRES O CESTAH IN PROMETU, Portorož, 20.–22. oktobra 2010 (str. 372–385).*
6. *Gray, C.S., 2015. Nicholas John Spykman, the balance of Power, and international order. The jurnal of strategic Studies, str. 873–897. Volume 38, October 2015.*
7. *Hughes, G.R., in Heley, J., 2015. Between man and nature: the enduring wisdom of Sir Halford J. Mackinder. The jurnal of strategic Studies, str. 878–933. Volume 38, October 2015.*
8. *Huntington, S.P., 1996. The Clash of Civilizations and the Remaking of World Order. First Simon & Shuster paperback edition 2003, New York, NY.*
9. *Kotnik, I., 2915. Možni odzivi na migrantsko krizo: Znova je čas za teritorialno obrambo in narodno zaščito! Dnevnik.si, 1. november 2015, dostop na https://www.dnevnik.si/1042723407/slovenija/mozni-odzivi-na-migrantsko-krizo-znova-je-cas-za-teritorialno-obrambo-in-narodno-zascito (3. 2. 2016).*
10. *Lind, W.S., in Thiele, G.A., 2015. 4TH Generation Warfare Handbook. Castilia House. Kouvola, Finland (Kindle book).*
11. *Lukin, A., 2014. Eurasian Integraton and the Clash of Values. Survival global politics and strategy, Volume 56 Number 3, IISS, Washington DC.*
12. *Mahan, A.T., 1890. The Influence of Sea Power Upon History 1660-1783 - Twelfth Edition. Little, Brown and Company, Boston (Kindle book).*
13. *NATO, 2015. Framework for Future Alliance Operations. Supreme Allied Commander Transformation, Norfolk, Virginia.*
14. *Obrambna strategija Republike Slovenije. Vlada RS št. 80000-1/2012/4 z dne 7. 12. 2012.*
15. *Podbregar, I., 2011. Pred reinženiringom nacionalnovarnostnega sistema – Priložnosti za Slovensko vojsko. Sodobni vojaški izzivi, MO RS, Ljubljana.*
16. *Ponjavić, D., 2012. Geopolitika in obveščevalna dejavnost. Univerza v Mariboru, Fakulteta za varnostne vede, magistrsko delo.*
17. *Renz, B., 2014. Russian Military Capabilities after 20 Years of Reform. Survival global politics and strategy, Volume 56 Number 3, IISS, Washington DC.*
18. *Resolucija o strategiji nacionalne varnosti (ReSNV-1). Uradni list RS št. 27/2010 z dne 2. 4. 2010*
19. *Sempa, P. F., 2002. Geopolitics; From the Cold War to the 21st Century. Transaction Publishers, New Brunswick, New Jersey.*
20. *Sokolosky, J. Jr., 2016. The Future of War; How Globalization is Changing the Security Paradigm. Military Review, January-February 2016 str. 8–15, CAC, Fort Leavenworth, Kansas.*
21. *Thränert,O., in Zapfe, M. (ur.), 2016. STRATEGIC TRENDS 2016; Key developments in global affairs. Center for Security Studies, ETH Zurich, Switzerland.*
22. *Van Creveld, M., 1991. The transformation of war. The Free Press, New York.*
23. *Vandergriff D.E., 2006. Rasing the Bar; Creating and Nurturing Adaptability to Deal with the Changing Face of War. Center for Defence Information, Washington, D.C.*
24. *Zakon o obrambi (uradno prečiščeno besedilo) (ZObr-UPB1). Uradni list RS, št. 103/04.*
25. *Zakon o občinskem redarstvu (ZORed). Uradni list RS, št. 136/06.*
26. *Zakon o zasebnem varovanju (ZzasV-1). Uradni list RS, št.17/2011.*
27. *Pravilnik o pogojih za opravljanje nalog občinskega redarja. Ministrstvo za lokalno samoupravo in regionalno politiko, Uradni list RS, št.103/2005.*
28. *37.a člen (izjemna pooblastila vojske) na https://zakonodaja.com/zakon/zobr/37a-clen-izjemna-pooblastila-vojske (27. 2. 2016).*
29. *http://www.businessinsider.com/map-of-the-russia-nato-confrontation-2015-2.*

Staša Novak

NATO IN KIBERNETSKO ODVRAČANJE

NATO AND CYBER DETERRENCE

Povzetek Vpliv kibernetske tehnologije na sodobno družbo je pomemben. Države se morajo prilagoditi spremenjenemu varnostnemu okolju, da bi bile zmožne zagotoviti varnost in stabilnost svojih ozemelj ter prebivalstva. Odvračanje, ki gre po navadi z roko v roki z obrambo, pomeni preprečevanje spopadov z odvračanjem napada morebitnih agresorjev. V kibernetiki so pravila drugačna kot pri tradicionalnem odvračanju zaradi posebnih značilnosti kibernetskega okolja. Zato sta nujna nova miselnost in bolj celosten pristop k odvračanju.

Pristop Nata k odvračanju temelji na ustrezni mešanici konvencionalnih, jedrskih in raketnih zmogljivosti. Kljub temu pa po sprejemu izboljšane politike o kibernetski obrambi (Enhanced NATO Cyber Defence Policy) iz leta 2014 Nato v resnici izvaja nekatere elemente kibernetskega odvračanja, ki temeljijo na močni obrambi, deklaratorni politiki in odzivnih ukrepih. Odzivni ukrepi ne pomenijo Natovih ofenzivnih kibernetskih zmogljivosti, temveč možnost za odzivanje kolektivne obrambe na kibernetski napad, pri čemer se uporabijo vsa sredstva, ki so na voljo. V članku so predstavljeni trenutna Natova kibernetska politika in mogoči prihodnji dogodki, povezani s kibernetskim odvračanjem na ravni zavezništva.

Ključne besede ***NATO, obramba in odvračanje, kibernetsko odvračanje, kibernetska obramba, kolektivna obramba, mednarodno pravo.***

Abstract The impact of cyber technologies on the modern societies is significant. States have to adapt to the changed security environment to be able to ensure the security and stability for their territories and populations. Deterrence, which usually goes hand in hand with defence, is about preventing conflicts by dissuading potential aggressors to attack. With regard to cyber, the rules of deterrence change when compared to traditional deterrence, because of the special characteristics of the cyberspace. What is needed is new way of thinking about deterrence and a more comprehensive approach to it.

The North Atlantic Treaty Organisation's (NATO) approach to deterrence is resting upon the appropriate mix of conventional, nuclear and missile defence capabilities. However, following the 2014 Enhanced NATO Cyber Defence Policy, NATO is *de facto* already pursuing certain elements of cyber deterrence based on strong defence, declaratory policy and responsive measures. Responsive measures are not NATO offensive cyber capabilities, but the possibility of a collective defence response to a cyber attack, which implies a response with all available means. The article is providing an insight into NATO's existing cyber defence policy and possible future developments of cyber deterrence at the level of the Alliance.

Key words ***NATO, defence and deterrence, cyber deterrence, cyber defence, collective defence, international law.***

Introduction

Globalisation and rapid development of technology mark modern society. Almost everything and everyone have become highly dependent on digital information and communication systems. The world has become more interdependent and interconnected. Against this background, the cyberspace, with all its potential opportunities and threats, has become not only a matter of national security, but also a matter of concern for the North Atlantic Treaty Organisation (NATO).

The article explores the implications of the 2014 NATO Enhanced Cyber Defence Policy from the perspective of cyber deterrence. It starts with the contextual background and the analysis of the security environment, and continues with the chapter on deterrence. It provides an overview of the basic concepts of the theory of deterrence, stemming from the Cold War, their possible application to the modern cyber environment and challenges connected to it. It also gives an insight into overall NATO defence and deterrence posture, by aspiring to analyse the cyber elements of it, with a special emphasis on NATO's declaration that cyber defence is part of a collective defence and that cyber attacks can reach a threshold to invoke Article 5.

The attention of the analysis rests only on NATO and not on individual Allies.[1] Although research was limited to the analysis of the secondary literature, relevant documents and other publicly available information, due to its primary focus on NATO's declaratory policy and political and legal implications of linking cyber defence with collective defence, the article provides an insight into some of the questions that might be addressed by NATO in the future.

[1] *The author uses NATO definitions, where available and applicable, or relevant definitions from secondary sources.*

1 CONCEPTUAL FRAMEWORK

1.1 Cyberspace

According to Trujillo (2014, p. 44), cyberspace is comprised of three components: the hardware, the virtual, and the cognitive. The physical element consists of information technology infrastructure (routers, fiber optic and transatlantic cables, cell phone towers, satellites, computers, smartphones, any devices connected to the Internet or local networks). The virtual element encompasses the software and data. And finally, the cognitive component includes its users, which can be anonymous and multiplicative, state or non-state actors. While the physical elements might reside in the sovereign territories of states, the virtual spaces do not.[2]

"Equally important to what cyberspace *is* is what it *does* (Hunker, 2013, p. 173). The information in cyberspace *controls* directly a wide variety of physical and electronic activities (e.g. Supervisory Control and Data Acquisition (SCADA) networks control many industrial processes); cyberspace data also *informs* decisions that people make" (*Ibid.*) Another special feature of cyberspace is its mostly civilian nature. A lot of infrastructure, data, and networks are owned by private entities, which can significantly affect the idea of cyber defence and deterrence, not only by the need to consider public-private cooperation but also to protect civil liberties and privacy.

1.2 Cyber attack

There are several understandings of cyber attacks, ranging from online protests, to cyber frauds, espionage, sabotage or acts of war (Singer and Friedman, 2014, pp. 67-68). NATO Glossary of Terms and Definitions provides the definition of a computer network attack, which is considered as a type of a cyber attack, but there is no specific definition of a cyber attack as such. Computer network attack is defined by NATO as an "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself" (NSA, 2014, p. 2-C-11; definition from 22 January 2010).

The Tallinn Manual on the International Law Applicable to Cyber Warfare (further on: Tallinn Manual),[3] which was published under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), defines cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2013, p. 106). Tallinn Manual is also using the term cyber operation, which can include,

[2] *Despite the fact that cyberspace is usually defined as a borderless domain and compared to the high seas, international airspace or outer space, it has been established that the components of cyberspace, such as cyber infrastructure, are not immune from the territorial sovereignty or national jurisdiction (Heinegg, 2013, p. 126 in Roscini, 2014, p. 23 and UN Doc. A/68/98, 24. June 2013 in Roscini, 2014, p. 23).*

[3] *Tallinn Manual on the International Law Applicable to Cyber Warfare was published in 2013. It was prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE). It does not reflect the NATO doctrine or the official position of any state or organisation (Roscini, 2014, pp. 30-31). Nevertheless, it has developed as an important point of reference on the subject of cyber.*

but is not limited to, cyber attacks, as the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace" (Schmitt, 2013, p. 15, 76).

Additionally, Singer and Friedman (2014, pp. 68-72) describe cyber attack as an attack that uses digital means, a computer action, instead of kinetic force. Unlike a conventional attack, it is not constrained by geography or political boundaries. It can be directed against multiple targets, whereby the first target is always a computer and the information within it, although the intended result might be to achieve a physical damage. Harrison (2012, pp. 65-74) distinguishes cyber attacks from the conventional attacks in terms of their indirectness with regard to finding the actual perpetrator as well as intangibility in terms of methods and consequences.[4]

2 SECURITY ENVIRONMENT

Understanding the security environment and assessing the threats is fundamentally important in order to establish better awareness on the risks individual states or international organizations, such as NATO, are accepting, and on the responses they are adopting.

Rapid technological advancement has lead into increased connectivity between computerized devices, a phenomenon known as the Internet of Things, and into dependence on information and communication technology in our everyday lives (Symantec, 2015, p. 5). We are living in an era of digital globalisation, where cyberspace became a vital enabler of modern society, but also its weak link (Kerschisching, 2012, pp. 5-8). In fact, cyber threats are continuously evolving, and with cheaper and more readily available technologies and communications channels, malicious activities of all kinds can blossom (Symantec, 2015, p. 23). The general rule is that any system can be successfully attacked if sufficient effort is made (Hunker, 2013, p. 164 and Singer and Friedman, 2014, p. 56).[5]

Growing and more complex cyber threats to the governments, public sector and critical infrastructure[6] led many countries to strengthen their cyber defences, and,

[4] *See also Hunker, 2013, pp. 156-157, Heinegg, 2013, p. 125 and Yannakogeorgos and Lowther, 2014, p. 51.*

[5] *Practice is showing great persistence of the attackers and their exploitation of 'zero-day' vulnerabilities, which is known as "advanced persistent threat" and includes a more sophisticated level of planning, organization, intelligence, complexity and patience. Zero day is "An attack that exploits a previously unknown vulnerability" (Singer and Friedman, 2014, pp. 299).*

[6] *Critical infrastructure refers to a system of physical networks and facilities that enable societies to survive. Its protection is of mayor importance for the national security of each state. It includes commercial key assets, government facilities, power plants, dams, sectors such as agriculture and food, chemicals and hazardous materials, banking and finance, defence industrial base, energy, water, transportation, telecommunications. Critical information infrastructure became indispensable for the functioning of most critical infrastructure (Kerschischnig, 2012, p. 41-42).*

in some cases, even develop offensive military capabilities (Symantec, 2015, p. 5).[7] Cyber became regarded as a fifth operational domain, besides land, sea, air and space (Gray, 2013, p. ix).[8] Not only nations, but also international organisations became more aware and are increasingly dealing with cyber threats.[9]

Despite the raising awareness that cyber attacks on the critical infrastructure can potentially lead to substantial physical damage, loss of civilian lives, and country's destabilisation, the extreme or worst potential of cyber operations in terms of damaging and disabling critical infrastructure and inflicting physical harm on the people, has not yet materialised (Kerschisching, 2012, p 17).[10] Gray (2013, pp. x-xi) argues that the effects of cyber are going to be the greatest (or most dangerous) as an enabler of joint military operations, while stand-alone strategic cyber attacks are at this point not so likely.[11] Also, Libicki (2013) is of the view that although the risk of devastating cyber attack is real, the perception of the risk is often greater than it actually is.[12] At the same time, cyber threat assessment cannot totally rule out the possibility that a cyber attack will result in a worst case scenario, which means decision makers, nationally or in the international framework, must take decisions based on assessment of likelihood and consequences (Hunker, 2013, pp. 161). In this regard, deterring cyber attacks and providing for a strong defence becomes even more important in the first place.

[7] *See NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) for the overview of the national cyber security documents at https://ccdcoe.org/strategies-policies.html [Accessed 19 August 2015].*

[8] *Information and communication technology plays an important part with regard to the military equipment, training, logistics, communications, on the battlefield, and as a possible weapon (Kerschischnig, 2012, p. 85). Militarisation of cyberspace can be seen also from the incorporation of cyber operations in military doctrines, and in the creation of cyber units and commands within the armed forces (Roscini, 2014, p. 10).*

[9] *Several international organisations are dealing with matters of cyber security, such as Council of Europe (2001 Budapest Convention on Cybercrime), European Union, Organisation for Economic Cooperation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITA), the Organisation for Security and Cooperation in Europe (OSCE), the World Summit on the Information Society (WSIS), the Internet Governance Forum (IFG) etc.*

[10] *Known cyber attacks offer the insight into what might develop in the future, such as the 2007 attacks against Estonia, 2012 attacks on the company Saudi Aramco, 2010 Stuxnet attack on Iran's Natanz uranium enrichment facility, 2014 Dragonfly attacks of cyber espionage, mainly in the energy sector, or attacks that were carried out as a part of military operations, such as 2008 operation in Georgia, to name just a few (Roscini, 2014, pp. 4-9, Kerschischnig, 2012, pp. 52-56, and Symantec, 2015, p. 65). More recently, cyber threats have evolved further with the attacks on NATO Allies and partners. More recently, the December 2015 cyber attacks on Ukraine power grid represent the first cyber attack taking down the power grid and with this the increased level of sophistication in committing cyber attacks against critical infrastructure, possibly by other states (Sanger, 2. 3. 2016, p.5). This attack came after states agreed in the UN framework norms, rules and principles for the responsible behaviour, which include restraint to intentionally damage critical infrastructure or otherwise impair the use and operation of critical infrastructure to provide services to the public (UN Doc A/70/174, 22 July 2015, para. 13.(f), pp. 7-8).*

[11] *Similar view on the unlikelihood of stand-alone cyber attack or "cyber Pearl Harbor" is expressed also by Gill and Ducheine, 2013, pp. 459-463, Morgan, 2010, p. 58, Waxman, 2013, p. 120 and Harrison, 2012, p. 5, 7.*

[12] *Libicki has been warning against escalation in cyberspace and calling for prudence in managing the cyber crisis. See: Libicki, Martin C., 2013. Cyberwar Fears pose Dangers of Unnecessary Escalation. [Online] Available at: http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cyberwar-fears-pose-dangers-of-unnecessary-escalation.html [Accessed 19 August 2015]. Libicki, Martin C., 2012. Crisis and Escalation in Cyberspace. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf [Accessed 2 November 2014].*

3 NATO AND CYBER DETERRENCE

3.1 Traditional deterrence

While the concept of deterrence, which can be broadly defined as anything that dissuades an attack (Hunker, 2013, p. 174), has been part of military practice for centuries,[13] most of the analysis has focused on the use of conventional and nuclear weapons during the Cold War (Trujillo, 2014, pp. 43-44 and Goodman, 2010, p. 103).[14] Therefore, before going into cyber deterrence and NATO's approach to it, it is important to understand basic presumptions of classical deterrence theory to see if and how they can be applied to cyberspace.

Deterrence is a concept mostly known in traditional security theory and realist views on international relations (Haley, 2013 and Cooper, 2009, pp. 12-20). Usually, it is linked to the concept of mutually assured destruction (MAD), which basically means that an attack is going to be met with an overwhelmingly destructive counter attack. It rests on the assumptions that the world stability can be maintained if the costs and consequences of war far out-weight its benefits; and that strategies that make defence cheaper and offence more expensive decrease the likelihood of the conflict.[15]

Most often deterrence is brought down to deterrence by denial (the ability to discourage the attack; for example with strong defence) and deterrence by punishment (the treat of retaliation) (Libicki, 2009, p. 7).[16] Hunker (2013, p. 162) adds a third, declaratory and diplomatic, element. More broadly, elements of deterrence include everything from an interest, a deterrent declaration ("do not do this, or that will happen"), to capabilities for denial or penalty, credibility (it has to be believable), as well as reassurance (if the interest is not attacked there will be no penalties). To make it work, both parties have to engage in the regular exchange of deterrent messages or a continuous dialogue (Goodman, 2010, pp. 103-108).[17] Deterrence has to be clear and understandable to everyone. Strategic communication is an important aspect in this regard.

[13] *In the History of the Peloponnesian War Thucydides quotes Hermocrates as stating "Nobody is driven into war by ignorance, and no one who thinks that he will gain anything from it is deterred by fear." (Trujillo, 2014, p. 43).*

[14] *In the 1950s the term "nuclear deterrence" was coined by the American military strategist Bernard Brodie. In the 1960s, Thomas Schelling developed theory forward by arguing that the nuclear capacity of a state that possesses nuclear weapons is used as bargaining power, and is most successful when it is held in reserve. See: Brodie, Bernard, 1959. "The Anatomy of Deterrence" as found in Strategy in the Missile Age. Princeton: Princeton University Press, pp. 264–304. Schelling, Thomas, 1966. The Diplomacy of Violence. New Haven: Yale University Press, pp. 1–34.*

[15] *Offense-defence theory argues that there is an offense-defence balance among adversaries, which determines the relative effectiveness of offensive and defensive strategies (the logic of the security dilemma). If the balance shifts to offense than the likelihood of competition and war increases; if the balance shifts towards defence then cooperation among adversaries becomes easier (Shaheen, 2014, p. 78).*

[16] *See also Rühle, 2015, Singer and Friedman, 2014, p. 145 and Haley, 2013.*

[17] *In NATO the idea of deterrence and dialogue, as two concepts that go hand in hand, was introduced in the 1967 Harmel Report ("Report of the Council on the Future Tasks of the Alliance"). This paved the way for the East-West political détente in the 1970 (NATO, 11. 11. 2015).*

In essence, however, deterrence is about the “ability to alter an adversary’s action by changing its cost-benefit calculations” (Singer and Friedman, 2014, p. 145). Deterrence is successful when an actor is convinced that restraint from action is acceptable. It is a state of mind of the adversary and thus a psychological relationship (Morgan, 2010, p. 56). It is the adversary who determines whether deterrence is working (Trujillo, 2014, p. 45). Therefore, for successful deterrence it is important to know who to deter or whose mind we would like to change (Singer and Friedman, 2014, pp. 145-147). Deterrence has to be tailored to potential adversaries. During the Cold War, deterrence theory was based on the assumption of rational state adversaries, while now in the changed security environment, where we are faced with increased variety of state and non-state actors, and new relationships among them, this assumption is under question, which makes deterrence even harder.[18]

3.2 Cyber deterrence

Many authors argue that due to the unique characteristics of cyberspace it is difficult to just translate nuclear and conventional deterrence to cyberspace;[19] nevertheless, the majority of them in principle build on the traditional concept of deterrence by denial and deterrence by punishment (defence and offence).

The analysis has shown that the first element of cyber deterrence is a strong defence (Trujillo, 2014, p. 45; Libicki, 2012, pp. 159-162; Haley 2013; Morgan 2010, pp. 75-76; Singer and Friedman, 2014, p. 137, 155; Shaheen, 2014, pp. 78-79; Rühle, 2015). This includes rather passive defensive measures including the enhancement of security and resilience of computer systems, such as: prevention, protection, detection, mitigation, recovery, awareness raising, policies and legal framework, partnerships, information and intelligence sharing etc. Strong defence prevents most intruders to get access into the network or even keep potential intruders from trying, due to the low probability of success. It requires adequate infrastructure and human capital ranging from governmental to private actors, from the industry and academia, from a national to international level. In addition to this, an important part of cyber defence is also the active promotion of arms control and related management in cyberspace. If states could enhance cooperation at the broader international level by developing common standards, arms control measures, or at least confidence building measures, this would lead to greater transparency and trust among them and would improve the chances for attribution.

[18] *“As long as both sides act “rationally”, i.e. according to a cost-benefit calculus, and if none of them is suicidal, their military potentials will keep each other in check” (Rühle, 2015).*

[19] *Libicki (2009, pp. 41-71) in Trujillo (2014, pp. 47-49) point out some of the challenges: difficult attribution; broad and cheap availability of technology; first-strike advantage cannot be deterred, because in cyberspace many vulnerabilities are unknown; cyberspace actors have a different risk tolerance compared to those operating in strictly physical domain, due to their perceived anonymity, invulnerability, and global flexibility; complexity due to the involvement of third parties (possibly even private companies), unpredictability of consequences etc.*

The second element is active exercise of military influence and threat of retaliation (offensive capabilities). Between the two is a thin line of stronger defence that rests on more advanced capabilities that can already defend against more serious and more sophisticated attacks by applying some initial retaliatory capabilities (Morgan 2010, pp. 75-76).

Successful deterrence by punishment (retaliation) in the cyber domain requires attribution, signalling and credibility. This means the target for deterrence needs to be identifiable, the message needs to be communicated to the intended audience and it has to be believable, which requires a certain level of demonstration of capability (Trujillo, 2014, p. 45). Capabilities for a response can range from cyber, military, economic, political measures and public disclosure (Morgan 2010, pp. 75-76). Even cyberspace deception can fall under this category in a way that cyberspace operations have the ability to manipulate decision-making and thus help to gain advantage and inherently add to deterrence (Trujillo, 2014, p. 47). Most notably, however, deterrence by punishment implies the need for offensive cyber capabilities, which is important to bear in mind with regard to NATO and its cyber capabilities, which, as we are going to see later on, are on the defensive and not offensive side.

The most important element of deterrence is the psychological one. Successful deterrence means affecting the behaviour of potential adversary. For deterrence to work it has to be understood by potential adversaries. It is about dialogue, issuing declarations, warnings and influencing the decisions of potential adversary, including by preserving certain level of ambiguity in policy (Hunker, 2013, pp. 164-165). There are no universal characteristics of adversaries' decision-making that would make deterrence easily effective. There are several factors that need to be considered when preparing the strategy of deterrence, including personal characteristics of a decision-maker, religion, ideology, government structure, culture, geopolitics, broader political context (Payne, 2013, pp. 3-34). Some of these factors are harder to influence than others; even more so in the cyber environment marked by anonymity and multiplicity of actors, ranging from state and non-state, governmental and private, military and civilian actors, each acting in their own specific frameworks; some have a responsibility towards the people, the other can act alone and with nothing to lose. There is a rapid growth of diverse relationships among them, creating multi-dimensional interests and influence and thus demanding new approaches to cyber deterrence, based on social-networks, to affect their perceptions and decision-making calculations (Cooper, 2009, pp. 47-53).[20]

To conclude, it is highly unlikely to eliminate the occurrence of all cyber attacks, but broader and more comprehensive deterrence can help to reduce them (Haley, 2013).

[20] *Cooper (2009, p. 95) argues that modern international system appears to act like a large organism comprised of dynamic networks of relationships. The so called "network deterrence" calls for better understanding of these networks and social relationships between their members – cooperation, competition and conflict (Dr. Lochard in Cooper, 2009, pp. 104-124).*

While cyber deterrence often comes down to strong cyber defence, including also a clear declaratory policy, and responsive capabilities (cyber or other), it needs to go beyond the cyber realm, and how this applies to NATO is going to be seen in the next chapters.

3.3 NATO and Cyber Deterrence

Cyber deterrence as a standalone concept does not exist in NATO; what exists is a classical understanding of deterrence as convincing potential aggressor that the "consequences of coercion or armed conflict would outweigh the potential gains" (NSA, 2014, p. 2-D-6). In 2010 NATO devoted an entire chapter of the Strategic Concept to defence and deterrence and Allies pledged to ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of its populations (*Ibid*., para. 17 and 19). In 2012, NATO reviewed its defence and deterrence posture, which now builds on the mix of nuclear, conventional and missile defence forces (NATO, 20. 5. 2012). In 2014, with the changing security environment, deterrence has re-emerged in the context of NATO (Rühle, 2015). With the crisis in Ukraine, which is seen as an example of hybrid warfare, non-military aspects of deterrence became more important, such as cyber, energy and strategic communications, which demands from NATO to update its concepts and tools of deterrence to fit the 21st century threats.

Specifically on cyber deterrence in NATO, we can see that elements of it are nevertheless already present. Its main focus is on building a strong cyber defence. Deterrence by punishment is mainly framed through Article 4 consultation and Article 5 invocation of collective defence. NATO does not have offensive capabilities, but several nations do, and they could be used as well (Healey and Tothova Jordan, 2014, p. 6). At the same time, there might be a need for NATO itself to consider more responsive cyber capabilities for greater credibility (Hunker, 2013, p. 164). Above all, to increase the success of deterrence, NATO has to provide credible and convincing declaration that it takes cyber threats seriously and is ready to respond with decisive actions, which is to some extent done by the 2014 Enhanced NATO Cyber Defence Policy, as we are going to see in the next chapter.

3.3.1 NATO Cyber Defence Policy

The protection of key Alliance information and communication systems, has always been important for NATO, even more so with the global spread of technology and with growing attempts from the side of adversaries (state and non-state actors) to try to exploit and disrupt the Alliance's increasing reliance on information systems (NATO, 30. 9. 2014 and Strategic Concept, 1999, para. 23). Cyber defence appeared on NATO's political agenda in 2002 after its systems were attacked from activists in Serbia, Russia and China during the Kosovo Conflict (Kerschischnig, 2012, p. 97 and Healey and Tothova Jordan, 2014, p.1). At the 2002 Summit in Prague, NATO Heads of State and Government decided to strengthen the capabilities to defend against cyber attacks (Prague Summit Declaration, 2002, para. 4.f). At the Summit in Riga in 2006 the need to improve the protection of key information systems against cyber attacks was reiterated (Riga Summit Declaration, 2006, para. 24).

After the 2007 cyber attacks on Estonia, Allied Ministers of Defence agreed, in June 2007, to step up the efforts, which led to the adoption of the first Policy on Cyber Defence in 2008 (NATO, 30. 9. 2014 and Kerschischnig, 2012, 97). The policy emphasised that the responsibilities for the protection of key information systems lie with NATO and nations; it further reiterated the importance of developing cyber defence capabilities, and it called for sharing of best practices and providing "a capability to assist Allied nations, upon request, to counter a cyber attack" (Bucharest Summit Declaration, 2008, para. 47). In the same year, the conflict in Georgia revealed the potential of linking cyber attacks to the conventional attacks (NATO, 30. 9. 2014).

In 2010 the Heads of State and Government agreed to enhance cyber defence capabilities, in light of rapidly increasing and more sophisticated cyber threats (Lisbon Summit Declaration, 2010, para. 2, 40). They recognised, in the NATO Strategic Concept (2010, para. 9-15), that cyber attacks are among the threats and challenges that are directly or indirectly affecting the security of the citizens of NATO countries. Strategic Concept (2010, para. 12) also acknowledged that "cyber attacks are becoming more frequent, more organized and more costly in the damage they inflict on government administrations, businesses, economies, and potentially, also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks". Therefore, cyber defence capabilities became part of the whole set of capabilities necessary to deter and defend against any threat to the safety and security of the populations (*Ibid*., para. 19).

In June 2011, NATO Defence Ministers adopted the second Policy on Cyber Defence, which set the framework for more coordinated efforts throughout the Alliance in strengthening cyber defence capabilities (NATO, 30. 9. 2014 and Chicago Summit Declaration, 2012, para. 49). And three years later they adopted the third policy called an Enhanced Cyber Defence Policy (NATO, 30. 9. 2014 and Wales Summit Declaration, 2014, para. 72).

From the comparison of different Summit Declarations, it seems, that the new 2014 policy represents an upgrade from a more technical approach of the protection of communication and information systems, to the higher comprehensive political framework. The policy reaffirms the principles of indivisibility of Allied security, of prevention, detection, resilience, recovery, and defence; it recalls the primary responsibility of NATO to defend its own networks, and of Allies to develop their own cyber defence capabilities for the protection of their networks (Wales Summit Declaration, 2014, para. 72). There is no mentioning of the offensive capabilities, the only focus rests on defence.[21]

The policy also recognises that international law, including international humanitarian law and UN Charter, applies in cyberspace (*Ibid*.). The policy reaffirms that "cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability". And it goes further, by saying that "Their impact could be as harmful to modern societies as a conventional attack", which has led the Heads of State and Government, in Wales, to declare for the first time that cyber defence is part of collective defence (*Ibid*.). They have further specified that a "decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis." (*Ibid*.). Assistance of Allies is addressed in the spirit of solidarity.

It is important to note also that 2014 policy was adopted in the time when the Alliance has started to face significantly changed security environment with Russia's aggressive actions against Ukraine and growing instabilities in NATO's southern neighbourhood, from the Middle East to North Africa, have altered (Wales Summit Declaration, 2014, para. 1). A new quality of threats emerged – hybrid warfare threats, which include a "wide range of overt and covert military, paramilitary, and civilian measures /which/ are employed in a highly integrated design" (*Ibid*., para. 13). Cyber threats are seen as one of the components of hybrid warfare (Blum et all, 2015), as such the need to defend against and deter cyber attacks should become even more important for NATO.

3.3.2 Cyber Defence as part of Collective Defence

As enshrined in the current NATO policy, cyber defence is part of collective defence (Wales Summit Declaration, 2014, para. 72), which is an important declaratory statement with significant deterrence value, but what does this mean in practice.

The principle of collective defence, as enshrined in Article 5 of the North Atlantic Treaty, is at the centrepiece of NATO. Article 5 states that an armed attack against one or more Allies shall be considered an attack against all Allies, which is reflecting the spirit of solidarity and assistance within the Alliance (NATO, 2.

[21] *NATO's approach to cyber threats is defence and not offense. It is, however, not identified, whether it is active or passive defence, whereby both terms are defined in NATO Glossary of Terms and Definitions. Active defence is defined as "Active measures taken against enemy forces to prevent, nullify or reduce the effectiveness of any form of enemy attack" (NSA, 2014, p. 2-A-2; definition from 25 January 2005). And passive defence are "Passive measures taken for the physical defence and protection of personnel, essential installations and equipment in order to minimize the effectiveness of hostile action" (NSA, 2014, p. 2-P-2; definition from 17 January 2005).*

6. 2014).[22] With the invocation of Article 5, Allies can provide assistance they deem necessary in a given situation to restore and maintain the security of the North Atlantic area. So far, Article 5 was invoked as a response to 9/11 attacks in 2001; however, reassurance measures to enhance defences of Allies were applied also more recently as a response to Russian aggressive actions in Ukraine in 2014 (NATO, 2. 6. 2014).

In the future, cyber threats relevant for NATO might come as a component of a larger conflict or as a tool of a major state power used during periods of tension. As in the past, cyber attacks may come as a response to NATO's engagements, its operations and its posture. It is more likely to envision cyber attack on an Ally than a conventional attack. There is also a risk of cyber attacks committed by terrorists or political extremists, even cyber attacks committed by accident or as part of cyber espionage (Hunker, 2013, pp. 159-160).

Response to an actual cyber attack, like a conventional attack on an Ally, would be approached on a case-by-case basis, as it is stated in NATO's policy on cyber defence itself (Wales Summit Declaration, 2014, para. 72). NATO does not respond automatically, but based on a request from an Ally. That Ally decides when it needs assistance from the Alliance. NATO's response is framed by the provisions of the North Atlantic Treaty and requires consensus. Assistance is not automatically collective defence or a military response. It can be any action deemed necessary in order to restore and maintain security. Response also does not have to be mathematically equal to the type and scale of the attack. It could be a political action, declaratory support or, if so decided, even technical assistance.

An Ally could invoke Article 4 consultations or Article 5. While any state could declare that specific cyber attack falls under Article 5 (act of war/use of force), acting upon that declaration is another thing. At the same time, even in the event of a serious and devastating cyber attack, there is no obligation to invoke Article 5. North Atlantic Council (NAC), which has the authority to decide in such a situation, would consider specific political, strategic and other circumstances. Most likely NAC is going to consider the scope (are the effects spreading through wider geographical area or the effects on the critical infrastructure), duration (is it a single attack or part of a longer campaign), intensity/scale (has it caused physical damage or deaths) and external actor (is it foreign or a domestic attacker) (Healey and Tothova Jordan, 2014, p. 7). The actual decision on NATO's reaction to a cyber attack will depend on the perceptions of an attack by Allies and on consensus

[22] *Article 5 is complemented by Article 6 of the North Atlantic Treaty, which stipulates that such armed attack is an attack on NATO territory or on the forces, vessels, or aircraft of any Ally (North Atlantic Treaty, 1949, Article 6). The primary responsibility for the maintenance of international peace and security rests with the UN Security Council (North Atlantic Treaty, 1949, Article 7). Other two important basic principles or the Alliance are encompassed in Article 3, whereby the Allies are pledging to take care of their defences and build, individually and collectively, their resistance to armed attacks; and in Article 4, which offers a basis for consultations, when territorial integrity, political independence or security of any of the Allies is threatened (North Atlantic Treaty, 1949).*

needed to take decisions on the level of the Alliance (Hunker, 2013, p. 161). In the end, it is going to be a political decision.[23]

There is no need to define precisely when a cyber attack might constitute an armed attack and as such a threat to the security, because it is exactly this ambiguity that constitutes certain level of deterrence on potential cyber adversaries. Namely, collective defence response to a cyber attack would mean that there is the whole range of NATO capabilities at its disposal, politically and military, reaching from the conventional to nuclear forces, in the framework of the international law.

Despite declared policy, Healey and Tothova Jordan's (2014, p. 4) assess that it is very unlikely that the NAC would invoke collective defence unless there were significant kinetic effects such as damage and deaths (comparing it with 9/11 response). NATO members have been cautious in the past. When the attacks on Estonia happened in 2007 the discussions on cyber defence were framed in the context of Article 4 of the Washington Treaty calling for political consultations, rather than Article 5, collective defence (Harrison, 2012, p. 39 and 57). Such a response, where NATO would be divided or unable to respond decisively, might negatively affect its credibility and would have a negative effect on deterrence.

3.3.3 International law and its application to responding to cyber attacks

NATO's response to cyber attacks is bound to follow the framework of the international law. What this means in practice and how is this going to affect the decisions taken by the Alliance in the context of possible Article 5 invocation, is going to be the subject of the analysis in this chapter.

Cyber attacks are a new challenge to the international law since they represent a new method of warfare (Harrison, 2012, pp. 279-280). There are no special rules and legal principles for the use of force in cyberspace, but there seems to be an agreement among states that the existing international law, existing treaties and customary norms apply (Gill and Ducheine, 2013, p. 439, Heinegg, 2013, pp. 123-124). This is also the approach NATO is taking with the 2014 policy, which acknowledges that

[23] *The invocation of Article 5 is not necessarily immediate and in the context of cyberspace it could take even more time. When Article 5 was invoked as a response to 9/11 attacks it started with the NAC statement condemning the attacks on 11 September 2001, which was followed by the invocation of the principle of Article 5 on 12 September 2001, with the explanation that Article 5 will apply if it is determined that the attack on the United States was directed from abroad, and finally, the invocation of Article 5 was confirmed on 2 October 2001 with the finding that the attack was directed from abroad (NATO 12. 9. 2001a, NATO 12. 9. 2001b, NATO, 2. 10. 2001). Once Article 5 was invoked, NATO acted in the framework of collective defence. This did not prevent NATO from taking action in the interim nor individual NATO Allies to offer bilateral assistance.*

international law, including international humanitarian law and UN Charter, applies in cyberspace (Wales Summit Declaration, 2014, para. 72).[24]

International law governs the right to wage war and the conduct in warfare through the law of armed conflict, including the rules addressing the legality of war (*jus ad bellum*) and rules regulating the conduct of hostilities (*jus in bello* or international humanitarian law) (Kerschischnig, 2012, 102). The key treaties are 1945 UN Charter, 1899 and 1907 Hague Conventions, four 1949 Geneva Conventions and their two 1977 Additional Protocols (Roscini, 2014, pp. 19-21). The question is how this applies to the concept of cyber attacks.

Threat or use of force in international relations against the territorial integrity or political independence of any state, or in any other way inconsistent with the purposes of the UN, is prohibited (Article 2 (4) UN Charter), with the exception of self-defence (Article 51 UN Charter) and collective measures authorized by the Security Council (Articles 42 and 53 UN Charter) (Kerschischnig, 2012, pp. 105-110). A cyber attack that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other way inconsistent with the purposes of the UN, is thus unlawful (Tallinn Manual, Rule 10 in Schmitt, 2013, p. 42).

The next question is under which conditions can the cyber attacks be classified as a "use of force"? A cyber attack constitutes a use of force when its scale and effects are comparable to non-cyber attacks rising to the level of use of force (Tallinn Manual, Rule 11 in Schmitt, 2013, p. 45). Each attack has to be assessed on its own merits.

So, when does self-defence come into play? The most serious and dangerous form of the illegal use of force and a crime against international peace is the aggression.[25] Armed force is one type of aggression.[26] Element of armed force is important for the establishment of the right to self-defence. Self-defence comes down to the question whether the use of force amounts to an armed attack (Kerschischnig, 2012,

[24] *A certain degree of consensus among the experts on the applicability of international law to cyber attacks can also be found in the Tallinn Manual on the International Law Applicable to Cyber Warfare, which also concludes that general principles of international law apply to cyberspace (Schmitt, 2013, p. 13). Similar conclusion was also reached by the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) (UN Doc A/68/98, 24 June 2013, p. 8 and UN Doc A/70/174, 22 July 2015, pp. 12-13). The Group of Experts identified following principles of the UN Charter and other international law that apply in cyberspace: "sovereign equality; the settlement of international disputes by peaceful means and in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States" (UN Doc A/70/174, 22 July 2015, p. 12, para. 26).*

[25] *UN General Assembly, Definition of Aggression, GA Res. 3314 (XXIX) of 14 December 1974.*

[26] *Article 3 GA Res. 3314 provides examples for acts of aggression, such as: invasion or attack by the armed forces, bombardment by the armed forces of one State against the territory of another State, blockage of ports or coasts by the armed forces of another State, an attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State, one State allowing another State to use its territory for perpetrating an act of aggression against a third State, sending of armed bands, groups, irregulars or mercenaries to another State to carry out acts of armed force (Kerschischnig, 2012, p. 112).*

pp. 112-113).[27] The burden of proof rests with the state exercising the right of self-defence (Kerschischnig, 2012, p. 141 and Harrison, 2012, pp. 99-102).

As a result, the attacked state has an inherent right of individual or collective self-defence,[28] until the UN Security Council has taken measures necessary to maintain international peace and security (Article 51 UN Charter).[29] Whether a cyber attack constitutes an armed attack depends on its scale and effects (Tallinn Manual, Rule 13 in Schmitt, 2013, p. 54).[30] This extends beyond kinetic armed attacks; it is not the weapon that is in the forefront but the effects of an attack or its potential consequences (Schmitt, 2013, pp. 54-55).[31] Based on the analysis of national cyber defence strategies, Gill and Ducheine (2013, p. 444) argue that an armed attack could even include a cyber attack on a critical infrastructure of a state, if it would severely undermine state's ability to carry out essential state functions or severely undermine its economic, political and social stability for a longer period of time.[32]

In situations of an armed conflict, international humanitarian law (jus in bello), usually referring to the conduct of hostilities (Hague Conventions) and minimum protection to individuals involved in armed conflict (Geneva Conventions and their Additional Protocols), applies. Thus far there has been no direct link to cyber attacks. Nevertheless, in accordance with the Martens clause, in the event of new situations

[27] *Article 49 (1) of the Additional Protocol I to the Geneva Conventions defines attacks as "acts of violence against the adversary, whether in offense or in defence". In: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Example of elements that constitute an attack can be found also in Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits) (1986) ICJ 14, International Court of justice.*

[28] *States can also use countermeasures that are close to self-defence, such as retorsions and reprisals to deter an adversary and convince him to return to lawful behaviour. This right belongs only to states victims of wrongful acts and not to the third-states, not even under collective self-defence (Kerschischnig, 2012, pp. 123-124). »A retorsion in international law is an unfriendly – but not illegal – act by a state in response to an unfriendly or unlawful act by another state. On the contrary, a reprisal is an act that per se is illegal under international law, but can be justified as a response to an unlawful act of another state. However, only defensive reprisals can be permissible« (Ibid.).*

[29] *Collective self-defence against a cyber attack amounting to an armed attack may only be exercised at the request of the victim state and within the scope of the request (Tallinn Manual, Rule 16 in Schmitt, 2013, p. 67).*

[30] *On the effects see also: Kerschischnig, 2012, p. 141, Chen, 2013, p. 33.*

[31] *See also: Singer and Friedman, 2014, p. 125; Delibasis, 2009, p. 97 and Kerschischnig, 2012, pp. 110-114 and 178-180.*
At the same time, cyber criminal activity, espionage, other forms of unauthorised penetration, theft of data and sabotage of public or private computer systems that do not fall in the definition of an armed attack are not subject to the law relating to self-defence (Gill and Ducheine, 2013, p. 440). However, even if the cyber attack does not rise to the level of a use of force criteria, it does not mean it is permitted. It is likely, that a cyber attack, which is severe enough to raise this question, might be "considered an unlawful interference in the affairs of a state, and may in all likelihood amount to the threat to the peace" (Harrison, 2012, p. 74).

[32] *For similar arguments see also Tsagourias, 2012, pp. 231-232; Schmitt, 2012, pp. 288-289; Sharp in Harrison, 2012, pp. 81-82; Singer and Friedman, 2014, pp. 122-124; and NATO Parliamentary Assembly, Annual Session 2009, Committee Report 173, paras 58-61, available at: http://www.nato-pa.int/Default.asp?SHORTCUT=1782 [Accessed 20 August 2015].*
While the attacks in Estonia in 2007 and in Georgia in 2008 did not reach this level (no loss of life, physical injury or destruction of property as a result of cyber attacks), the 2010 Stuxnet worm would amount to a use of force, but its scale and effects did not appear to have sufficient gravity to amount to an armed attack (Harrison, 2012, pp. 81-82).

or new forms of warfare, customary international law applies (Kerschischnig, 2012, pp. 175-177, Harrison, 2012, pp.127-128 and Schmitt, 2013, pp. 77-78). Cyber attacks executed in the context of an armed conflict are thus subject to the law of armed conflict; in both international and non-international armed conflicts (Tallinn Manual, Rule 20 in Schmitt, 2013, p. 75).[33]

The response to the attack has to be in accordance with the principles of necessity and proportionality (Tallinn Manual, Rule 14 in Schmitt, 2013, p. 61). A state victim may resort to proportionate countermeasures against the offending state, with intention to induce compliance with the international law by the offending state (Tallinn Manual, Rule 9 in Schmitt, 2013, pp. 36-37). Proportionality does not require mathematical equivalence nor does it define the modalities of self-defence (Gill and Ducheine, 2013, pp. 449-450). In essence, states are not restricted only to cyber responses; however, there is a danger of cyber attacks escalating into conventional attacks (Harrison, 2012, pp. 102-104).

Necessity requires an armed attack that is ongoing or imminent (Tallinn Manual, Rule 15 in Schmitt, 2013, p. 63). The principle of necessity is linked to the question of timely response; immediacy requires that self-defence measures must not be duly delayed (see also Tallinn Manual, Rule 15 in Schmitt, 2013, p. 63). This implies reasonable action within a reasonable timeframe in response to an ongoing attack or a clear threat of the attack in the future (Gill and Ducheine, 2013, p. 451).

This opens a question of legality of response in the event of anticipatory or pre-emptive self-defence in case of a manifest and unequivocal threat of attack in the near future or preventive self-defence to a potential attack at some indeterminate point in the future (*Ibid*., pp. 452-458). Gill and Ducheine (2013, pp. 453) argue that there is no universal consensus on either, but while the first is being more or less accepted by the international law and state practice, the second is more controversial. Nevertheless, many nations claim that bona-fides self-defensive actions can only come after an armed attack and not before (Dunlap, 2014, pp. 217). The Group of Experts from the Tallinn Manual took the "last feasible window of opportunity" approach, whereby they agreed that state might act in anticipatory self-defence, cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim state will lose its opportunity to effectively defend itself unless it acts (Schmitt, 2013, pp. 64-65).

Moreover, there is also the question of attribution; the importance of knowing the attacker and obtaining reasonably credible and convincing evidence. This is not only the question of identifying the source, a computer, but also the person operating the computer and the 'mastermind' behind the attack. It is very difficult to establish

[33] *Similarly, the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) noted that the established legal principles, including the principles of humanity, necessity, proportionality and distinction apply in cyberspace (UN Doc A/70/174, 22 July 2015, p. 13)).*

with any certainty who is actual perpetrator of the attack, due to the anonymity of the cyberspace, the possibility of launching multi-stage cyber attacks (for example due to IP spoofing or proliferation of botnets)[34] and/or speed with which cyber attack can materialize (Tsagourias, 2012, p. 233). In the end, attribution is a technical, legal and political process. Technical attribution has to be complemented with intelligence and information analysis on the profile, capabilities, intent and affiliations of the authors of the attack, as well as on the political context in which the attack took place (Tsagourias, 2012, pp. 233-234).

A state bears international legal responsibility for a cyber attack attributable to it and which constitutes a breach of an international obligation in a form of an act or omission (Tallinn Manual, Rule 6 in Schmitt, 2013, p. 29). When the actions of non-state actors (private companies, private citizens etc.) can be attributable to the states, in terms of support and control, their actions can qualify as an armed attack subject to the UN Charter (Kerschischnig, 2012, pp. 110-114 and Schmitt, 2013, pp. 26-29).[35]

At the same time we cannot but recognise the possibility that some groups might act on their own, without a state control and influence, and commit an armed attack comparable in scale and effect to an armed attack by states, which would still fall under the law on self-defence and non-state actor could become a direct target of self-defensive action (Gill and Ducheine, 2013, p. 446 and Tsagourias, 2012, pp. 236). In such a case, if the state, where the non-state actor is located, consented, such consent would form a legal basis in addition to or in place of self-defence for taking action by the target state (Gill and Ducheine, 2013, p. 450).[36]

To conclude, besides the legal perspective we need to consider also strategic perspective, linking the right of armed self-defence to the long-term policy interests including security and stability, as well as a political perspective, which is taking into account the situational context of decision making (Waxman, 2013, pp. 110-120). In the end legal analysis comes down to politics. A decision whether cyber attack reaches the threshold of war will be political and a matter of judgement and not automaticity (Singer and Friedman, 2014, p. 126). State practice is still evolving, therefore, it is going to be difficult to build a legal consensus on the question, especially as it seems that major actors in this field have divergent strategic interests (Waxman, 2011, pp. 425-426 and Dunlap, 2014, pp. 213-214).

[34] *For example, DDoS Attack in Estonia in 2007 involved a large botnet of approximately 85 000 hijacked computers from around 178 countries (Tsagourias, 2012, p. 233).*

[35] *International Court of Justice uses the term "effective control", which goes beyond mere financing and equipping, and involves also participation in planning and supervision (Schmitt, 2013, pp. 32-33). The mere fact that cyber attack has been launched from governmental cyber infrastructure or was routed through a state is not sufficient evidence for attributing the operation to that state (Tallinn Manual, Rules 7 and 8 in Schmitt, 2013, pp. 34-36). On this see also: Tsagourias, 2012, pp. 236 and Gill and Ducheine, 2013, p. 445.*

[36] *Yannakogeorgos and Lowther (2014, p. 51) have a bit more radical approach in this regard, saying that "rather than individual accountability, nation-states should be held culpable for the malicious actions and other cyber threats originating in or transiting information systems within their borders, or owned by registered corporate entities therein". They are also of the opinion that a global culture of cyber security would help in mitigating the risk of a country being used as a transit or origin point for a cyber attack (Ibid., pp. 51-52).*

Conclusion

Growing and more complex cyber threats are leading many countries and NATO into strengthening their cyber defences and adopting more proactive approaches to cyber security. Even though it is assessed that a strategic standalone cyber attack on NATO or Allies is, at this point, not so likely, it is the perceived risk or potential devastation, in the form of physical damage, disabling of critical infrastructure, loss of civilian lives and destabilisation of states that is the driving force of the decisions taken by the states, nationally and internationally. The states are the ones bearing responsibility for the security of their territories and populations; therefore, it is in their interest to ensure the security in cyberspace and dissuade potential adversaries from attacking them. This cannot be done just by transferring the experiences and approaches from the nuclear and conventional deterrence of the Cold War. Cyberspace is different and demands new ways of thinking and acting.

Cyber deterrence seems to come down to the following elements: strong cyber defence, clear messaging that some actions are unacceptable and will thus have consequences, and credible responsive capabilities, cyber and other. In essence, however, it is a very psychological and behavioural question, which refers to adversary's state of the mind. It is about perceptions; the adversary calculating that the attack is not worth it and that restraint is more acceptable. Each adversary has its own characteristics and deterrence strategy has to be tailored according to them. Cyber deterrence is thus never going to be one hundred percent successful. There is always going to be a risk of a cyber attack. To prevent as many attacks as possible, deterrence has to go beyond cyber and beyond traditional concepts. It has to be broader and more comprehensive.

NATO's defence and deterrence posture rests on the mix of nuclear, conventional and missile defence forces. In the changed security environment, defined also through the hybrid warfare, non-traditional aspects are becoming more important, such as cyber and strategic communications. NATO has made an important step forward in terms of cyber deterrence in 2014 when it declared that cyber defence is part of collective defence. Another important element was ambiguity in its policy, with regard to the activation of Article 5 and possible responses to a cyber attack, which has put all options on the table.

But the question is, if such an approach, resting only on cyber defence and leaving offensive cyber capabilities to individual member states, is enough to successfully deter, to the highest extent possible, future cyber attacks. Allies could offer their offensive capabilities as assistance to other Allies or NATO, if required. However, in the future, following further developments in the cyberspace, NATO, as a military Alliance, could also consider adding such capabilities to its own repertoire. However, just adding offensive cyber capabilities on the list of NATO capabilities is not so simple. NATO has been cautious in the past. Its response to 2007 cyber attacks on Estonia is a case in point. Nevertheless, Estonian experience has pushed forward the development of cyber defence within the Alliance, and possible new cyber attacks on NATO and its Allies or even partners may bring the matter even further.

By developing only defensive capabilities, NATO is portraying itself as a defensive Alliance, which, in itself, is an important political message. Too much emphasis on the offensive cyber responses can lead to an arms race, unpredictable spill-over effects, or even into making the matters worse when applied under the conditions of blurred circumstances of hybrid warfare, where attribution and evidences will not be totally clear. Besides, an important element of constraint is also NATO's adherence to the international law in cyberspace, which is providing a legal framework for its response to a cyber attack. A decision to invoke Article 5 as a response to a cyber attack is always going to be a political one, done on a case-by-case basis, and it will include broader political and strategic considerations, but it has to be legal and legitimate. However, decision might take time and time is not always in abundance when dealing with matters of urgency in a cyber crisis situations. Building consensus within an Alliance is not going to be easy. The future will tell how NATO is actually going to react in a given situation. And this in turn will also going to send an important message for the credibility of the Alliance and will greatly affect the success of its cyber deterrence.

To conclude, effective cyber deterrence goes hand in hand with the overall credible and strong defence and deterrence posture of NATO. A posture that corresponds to the new and emerging security challenges in the ever changing security environment. It is the broader picture that matters. This includes the ability of NATO and its Allies to stand united, be willing and able to respond in a timely manner and act coherently, as well as to generate the required resources (human, financial and technological), invest in defence by developing and maintaining appropriate capabilities and forces. Moreover, it is about the people and new ways of working together. What is needed is greater cooperation and greater sharing of information on every possible level, nationally and internationally, with partner nations, international organisations, industry and academia. A new quality of trust has to be forged to enable such modus operandi. And lastly, this has to be communicated to the public. It is a matter of transparency, generating legitimacy, but also a matter of warnings towards the adversary and thus, a matter of the general success of deterrence.

Bibliography

1. *Blum, R., Evelina, Z., Sadia, R., Soliman, E., 2015. The Future of NATO in the Face of Hybrid Threats. [Online]. Available at: http://www.academia.edu/11044703/THE_FUTURE_OF_NATO_IN_THE_FACE_OF_HYBRID_THREATS [Accessed 29 August 2015].*
2. *Chen, T. M., 2013. An Assessment of the Department of Defence Strategy for Operating in Cyberspace. The Letort Papers. [pdf] Strategic Studies Institute, US Army War College, Carlisle, PA. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1170.pdf [Accessed 2 November 2014].*
3. *Cooper, J. R., 2009. New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework. Prepared under contract number N65236-08-D-6805, Under Secretary of Defence for Intelligence, Joint & Coalition Warfighter Support, Cyber, Information Operations and Strategic Studies Task Order, DWAM80950, 29. 12. 2009. [Online] Available at: http://www.americanbar.org/content/dam/(aba/mitigate/2011_build/law_national_security/new_approaches_to_cyber_deterrence.authcheckdam.pdf [Accessed 16 November 2015].*

4. *Delibasis, D., 2009. Information warfare operations with the concept of individual self-defence. In: Karatzogianni, Athina ed., 2009. Cyber Conflict and Global Politics. Abingdon, UK: Routledge. Ch.7, pp. 95-111.*
5. *Dunlap, C. J., Jr., 2014. Pespectives for Cyberstrategists on Cyberlaw for Cyberwar. In Yannakogeorgos, Panayotis A. & Lowter, Adams B. eds., 2014. Conflict and Cooperation in Cyberspace: The Challenge to National Security. Boca Raton, FL: Taylor & Francis, pp. 211-226.*
6. *Gartner, Int., 2014. Gartner says 4.9 billion connected "things" will be in use in 2015. Press release, Barcelona, Spain, 11 November 2014. [Online] Available at: http://www.gartner.com/newsroom/id/2905717 [Accessed 13 July 2015].*
7. *Gill, T. D., Duchein, P. A. L., 2013. Anticipatory Self-Defense in the Cyber Context. International Law Studies, U.S. Naval War College, Vol. 89, pp. 438-471.*
8. *Goodman, W., 2010. Cyber Deterrence: Tougher in Theory than in Practice? [pdf] Strategic Studies Quarterly, Fall, pp. 102-135. Available at: http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf [Accessed 2 November 2014].*
9. *Gray, C. S., 2013. Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling. [pdf] Carlisle, PA: US Army War College. Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf [Accessed 2 November 2014].*
10. *Haley, C., 6. 2. 2013. A theory of cyber deterrence. Available at: http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ [Accessed 20 August 2015].*
11. *Harrison D. H., 2012. Cyber Warfare and the Laws of War. Cambridge University Press, Cambridge, UK.*
12. *Healey, J., Tothova, J, K., September 2014. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. [pdf] Issue Brief. Atlantic Council. Available at: http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf [Accessed 2 November 2014].*
13. *Heinegg, W. H., 2013. Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, U.S. Naval War College, Vol. 89, pp. 123-156.*
14. *Hunker, J., 2013. NATO and Cyber Security. In: Herd, Graeme P. and Kriendler eds., 2013. Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance. Abingdon, UK: Routledge. Ch. 10, pp. 154-175.*
15. *Kerschischnig, G., 2012. Cyberthreats and International Law. The Hague: Eleven International Publishing.*
16. *Libicki, M. C., 2009. Cyberdeterrence and Cyberwar. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [Accessed 2 November 2014].*
17. *Libicki, M. C., 2012. Crisis and Escalation in Cyberspace. [pdf] Santa Monica, CA: Rand Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf [Accessed 2 November 2014].*
18. *Libicki, M. C., 2013. Don't Buy the Cyberhype. Foreign Affairs, [Online] 14 August. Available at: http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype [Accessed 2 November 2014].*
19. *Morgan, P. M., 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. [pdf] Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press. Available at: http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059436.pdf [Accessed 2 November 2014].*
20. *NATO, 20. 5. 2012. Deterrence and Defence Posture Review. [Online] (Updated 21 May 2012). Available at: http://www.nato.int/cps/en/natolive/official_texts_87597.htm [Accessed 15 July 2015].*

21. *NATO, 30. 9. 2014. Cyber defence. [Online] (Updated 30 September 2014). Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 2 November 2014].*
22. *NATO, 11. 11. 2014. The Harmel Report. [Online] (Updated 11 November 2014). Available at: http://www.nato.int/cps/en/natohq/topics_67927.htm [Accessed 1 December 2015].*
23. *NATO, 2. 6. 2014. Collective defence. [Online] (Updated 2 June 2014). Available at: http://www.nato.int/cps/en/natohq/topics_110496.htm [Accessed 5 November 2014].*
24. *NATO, 12. 9. 2001a. A moment of great tragedy and mourning. NATO Update. [Online] (Updated 14 September 2001). Available at: http://www.nato.int/docu/update/2001/1001/e1002a.htm [Accessed 20 August 2015].*
25. *NATO, 12. 9. 2001b. NATO reaffirms Treaty commitments in dealing with terrorists attacks against the US. NATO Update. [Online] (Updated 15 September 2001). Available at: http://www.nato.int/docu/update/2001/0910/e0912a.htm [Accessed 20 August 2015].*
26. *NATO, 2. 10. 2001. Invocation of Article 5 confirmed. NATO Update. [Online] (Updated 3 October 2001). Available at: http://www.nato.int/docu/update/2001/0910/e0911a.htm [Accessed 20 August 2015].*
27. *NSA (NATO Standardisation Agency), 2014. NATO Glossary of Terms and Definitions.. [pdf] NATO standard AAP-06(2014). Available at: http://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf [Accessed 10 July 2015].*
28. *Payne, K. B., ed., 2013. Understanding Deterrence. New York: Rutledge.*
29. *Roscini, M., 2014. Cyber Operations and the Use of Force in International Law. Oxford, UK: Oxford University Press.*
30. *Rühle, M., 20. 4. 2015. Deterrence: what it can (and cannot) do. NATO Review. [Online]. Available at: http://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/ [Accessed 15 July 2015].*
31. *Sanger, D. E, 2016. After cyberattack in Ukraine, U.S. tells utilities to be on alert. In International New York Times, 2. 3. 2016, p. 5.*
32. *Schmitt, M. N., ed., 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, UK: Cambridge University Press. Available at: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [Accessed 20 August 2015].*
33. *Schmitt, M. N., 2012. "Attack" as a Term of Art in International Law: The Cyber Operations Context. [pdf] 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn. Available at: http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf [Accessed 2 November 2014].*
34. *Singer, P.W., Friedman, A., 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.*
35. *Symantec, 2015. Internet Security Threat Report. Government. April 2015, Volume 20.*
36. *Trujillo, C., 2014. The Limits of Cyberspace Deterrence. [pdf] JFQ/Joint Force Quarterly, 75, 4th Quarter, pp. 43-52. Available at: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_43-52_Trujillo.pdf [Accessed 2 November 2014].*
37. *Tsagourias, N., 2012. Cyber Attacks, Self-Defence and the Problem of Attribution. Journal of Conflict and Security Law, 17(2), pp. 229-244.*
38. *UN Doc A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013. Available at: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf [Accessed 20 August 2015].*
39. *UN Doc A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Accessed 20 September 2015].*

40. *Waxman, M. C., 2011. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). [pdf] The Yale Journal of International Law, 36(2). Available at: http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf [Accessed 2 November 2014].*
41. *Waxman, M. C., 2013. Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies, U.S. Naval War College, Vol. 89, pp. 109-122.*
42. *Yannakogeorgos, P. A., Lowter, A. B., 2014. The prospects for Cyber Deterrence. American Sponsorship of Global Norms. In Yannakogeorgos, Panayotis, A., Lowter, A. B. (eds.), 2014. Conflict and Cooperation in Cyberspace: The Challenge to National Security. Boca Raton, FL: Taylor & Francis, pp. 49-77.*
43. **NATO documents**
44. *Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest, 3 April 2008. [Online] (Updated 8 May 2014). Available at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm [Accessed 3 July 2015].*
45. *Chicago Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, 20 May 2012. [Online] (Updated 1 August 2012). Available at: http://www.nato.int/cps/en/natohq/official_texts_87593.htm?mode=pressrelease [Accessed 3 July 2015].*
46. *Lisbon Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 November 2010. [Online] (Updated 31 July 2012). Available at:*
47. *http://www.nato.int/cps/en/natolive/official_texts_68828.htm [Accessed 3 July 2015].*
48. *North Atlantic Treaty. Washington D.C., 4 April 1949. [Online] (Updated 9 December 2008). Available at: http://www.nato.int/cps/en/natolive/official_texts_17120.htm [Accessed 5 November 2014].*
49. *Prague Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, 21 November 2002. [Online] (Updated 18 January 2008). Available at: http://www.nato.int/docu/pr/2002/p02-127e.htm [Accessed 3 July 2015].*
50. *Riga Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga, 29 November 2006. [Online] (Updated 27 February 2009). Available at: http://www.nato.int/docu/pr/2006/p06-150e.htm [Accessed 3 July 2015].*
51. *Strategic Concept: Active Engagement, Modern Defence. Adopted by the Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010. Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf [Accessed 2 November 2014].*
52. *The Alliance's Strategic Concept. Adopted by the Heads of State and Government at the NATO Summit in Washington, 24 April 1999. [Online] (Updated 25 June 2009). Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm [Accessed 3 July 2015].*
53. *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014. [Online] (Updated 29 September 2014). Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed 2 November 2014].*

József Padányi
László Földi

IZKUŠNJE MADŽARSKIH OBRAMBNIH SIL, PRIDOBLJENE PRI RAZMESTITVI INŽENIRSKIH OVIR MED VSEEVROPSKO MIGRANTSKO KRIZO LETA 2015

LESSONS LEARNED FOR THE HUNGARIAN DEFENCE FORCES FROM THE DEPLOYMENT OF ENGINEER OBSTACLES DURING THE 2015 EUROPE-WIDE MASS-MIGRATION EMERGENCY

Povzetek Leta 2015 se je v Evropo zateklo izjemno veliko število beguncev, kar se ni zgodilo še nikoli prej. Da bi preprečila nenadzorovan in nezakonit prestop državne meje, je Madžarska začela postavljati ograjo vzdolž svoje južne meje.

V članku so najprej opisane vrste vojaških inženirskih ovir in nato izbruh dogodkov, povezanih z migracijami leta 2015 na Madžarskem. Predstavljeni so »krizne razmere«, ki so jih povzročile množične migracije in jih je razglasila vlada, ter sodelovanje madžarskih oboroženih sil pri njihovem reševanju.

Povzete so do zdaj opravljene vojaške naloge ter z njimi povezane težave in izkušnje. Članek se konča z nekaj komentarji in predlogi avtorjev.

Ključne besede Inženirske ovire, begunci, migracije, madžarske obrambne sile.

Abstract A serious mass of refugees, which has never been seen before, arrived to Europe In 2015. Hungary started to build fences along its southern borders to stop uncontrolled and illegal border crossings.

In our paper, we start with the description of the types of military engineering barriers, then we describe the escalation of the 2015 migration events in Hungary. We present the “crisis situation caused by mass migration” announced by the Government and the involvement of the Hungarian Defence Forces.

We summarize the related military tasks completed so far and the emanated problems and experiences. In the end of our paper we make some comments and proposals.

Key words ***Engineering barriers, refugees, migration, Hungarian Defence Forces.***

Introduction

One of the most important categories of military engineering barriers is the so called non-explosive obstacle where you can find the fences among others. Soldiers of the Hungarian Defence Forces built a lot of them, combined with other defensive elements in the 1990's during the Southern Slavic conflict to protect borders of Hungary. These obstacles are suitable to block or limit movements, to direct movements of crowds or to reinforce protection of camps or depots. Defence wirings, the so called "concertinas" are primarily made for close of important directions or territories applied in combination with other defensive tools. They are widely used on routes to military installations, at the gates, along the fences and also in the inner parts of military camps. Concertinas can be installed on the top of existing fences or they can be used individually. They can be built in several forms or patterns, in rows or on top of each other.

Fences are brought into the limelight because they became one of the most considerable elements for handling of masses of migrants along the borders. In the followings we present various types of fences and other obstacles, practice and experiences of their possible applications from professional point of view, especially their utilization for protection against uncontrolled flow of masses of people. The present situation at Hungary's Southern borders gives special actuality to our research where fences play a key role in protection against the crisis.

Someone may ask why the use of the Hungarian military was necessary for the task of building fences along the border of our country. Decision makers assessed the situation and the possibilities and chose such an option that already proved its suitability a lot of times. Emergency situations are quite common in Hungary, when quickness and professionalism are the key factors to solve the problem by the use of specific preparedness together with special equipment, such as fighting against floods, extreme snowfall or industrial disasters like "Red Sludge Catastrophe" was back in 2010. In our country only the military is suitable for this, because it is a unique human and technical resource, which is capable to deploy a mass of skilled experts with special equipment in a very short time with complete logistic an communication systems. Authors of this paper are already published about these military activities in details (Padányi et al., 2015).

Participation of military power such as the Hungarian Defence Forces is not extraordinary in building and maintenance of fences and other border obstacles. It is one of the major and undisputable tasks of military engineering units during wartime or peace support operations. And this was not the only task dedicated to military forces during mass migration emergencies. Slovenia made it possible for its military to assist the police driving refugees along its border (www.dehir.hu).

Croatia (http://kitekinto.hu), Serbia (www.portfolio.hu), Bulgaria (www.ma.hu), Greece (www.ekathimerini.com), Italy (444.hu) and the Czech Republic (www.lokal.hu) also use their military in handling the mass migration emergency.

Tasks of the Hungarian Defence Forces in handling mass migration are limited to the deployment and maintenance of border fences and common patrolling together with the police forces. Building and maintenance of fences along the borders mean billions of costs, which exceed 6 billion HUF only at the Serbian-Hungarian border.

1 MILITARY ENGINEERING BARRIERS

Wirings in military practice are the major group of non-explosive obstacles used against enemy infantry. There are two types of them: fix (stationary) and deployable (mobile).

Stationary wirings, as they name shows are deployed to certain places or routes to make obstacles. Their main subgroups are wire fences and wire networks. The most commonly used type of obstacles is the wire fence (simple or multiplied) that can be built easily and quickly in comparison with the available resources.

Most important types of deployable wirings are: Spanish rider (or "Cheval de fries"), hedgehog barrier, wire rolls (or rapidly deployable concertinas) and wire networks. These barriers are easily removable, can be used multiple times and redeployable. They can be made previously or on site, sometimes from improvised materials in case of need. They are perfect tools for quick and reliable closing of the desired territories, routes or installations (Kovács, 2012).

Properties of wires used for certain types of barriers basically determine the kind of obstacle that can be formed from them and the task that it will be suitable for. Wires used against enemy infantry are mainly made of steel with average tearing strength and smaller diameter (1.5-3.5 mm), while types that are used against vehicles have much higher tearing strength and diameter (3.5-5.5 mm). All the wires can be made of steel or sometimes copper (very rarely) with smooth surface or some kind of piercing or cutting edge, applied weaved or expanded separately.

Fences used as military engineering barriers vary in a wide range concerning their height, but mostly in the range of 1.8-4.0 metres (but sometimes we can meet a height of 7 metres, too). The fences' definite advantage is that to cross them is a time-consuming task (especially in case of their application in several rows together with other obstacle elements), so they can provide a comprehensive protection against foot-soldiers and foot-passengers. Meanwhile, their disadvantages are the reasonable time, manpower and materials necessary for their planting, in addition with the difficulties caused by harsh terrain. However, combined with wire rolls, electric locks and signal devices they can provide effective holding and deflection power.

Wire rolls are very useful against persons and vehicles depending on the thickness and quality of the wire. One of their most important property, that they are made of steel wires with different cutting edges (see Picture 1, p. 109).

Wire rolls are the most commonly used wire-based obstacles. They can be made in different sizes concerning their diameter (20-150 cm) and length (10-30 m), and can be used in several forms: in one or in multiple rows, one or multilevel forms, as individual obstacles or as reinforce elements to other engineering barriers (see Picure 2, p. 109).

Some deployment forms can be seen in Picture 3 (p. 110), where wire rolls are used individually or in combination with fences.

Possible packing of wire rolls, in other words formation of a multi-level engineering obstacle depends on the stability of the instrument that can be improved by vertical reinforcement. This system is well applicable in rural areas for the protection of friendly forces or to close roads, squares, buildings.

In addition to make movements difficult, an important task of the use of non-explosive engineering obstacles during peace support operations is the definitive demonstration of the purpose. While in combat operations the obstacles, barriers on the battlefield are often camouflaged, in peace support operations their presence is greatly emphasized. In general, the elements are placed on the surface easily perceptible to the naked eye. Lifetime of deployed wires can be increased with the prevention of problems emanating from undergrowth: the elements are often placed onto gravel layer over geotextile rug (Kovács, 2004).

Effectivity of these demonstrated barriers can be further improved whether they are completed with cameras and movement sensors, or patrols to be ordered along them. In this case they provide reliable closing, their undetected utilization is almost impossible. They are used in many areas all over the world.

2 FENCES ALONG THE BORDERS OF HUNGARY

In the followings, we would like to present the formation of the military engineering barrier along the Southern borders of Hungary in 2015. Its official name is “Temporary security border closing for border guarding” (Act 213/2015). In July 2015, the Hungarian Parliament modified the law concerning state borders and gave public utility right to the Government in the outer Schengen border areas, in 10 metres from the border line. The Government rearranged 6.6 billion Forints, so the construction works could be started.

Building of the fence at the border started on 13th July, at Mórahalom. First, a 150 m pilot stage was built, than based upon the experiences from this, the construction of the elements of the border closing started at the full length of the Serbian-Hungarian border. The fence has been built with columns extruded into the ground in 1 m depth, connected with wire network to each other, and two additional layers of wire rolls: one on the top of the fence and the other at the bottom of it. The only exception is the most difficult terrain in 30-40 km, where only wire rolls were used. There are information tables along the fence indicating the nearest border crossings and stating that illegal border crossing is considered as a crime in Hungary.

The full length of the fence has been built by the soldiers of the Hungarian Defence Forces, on 10-12 sites and with several hundreds of persons at a time. The original deadline of the construction was 30th November, but the Prime Minister modified it to 31st August at the end of July. To speed up the works military subunits were reinforced with additional 100-250 public workers and 6 pile-drivers were also used. Because of the modified deadline a lighter version of the primarily determined type was built, the so-called rapidly deployable wired fence, which were 3 lines of wired rolls expanded between steel pales on top of each other with a total height of 1.5-2 metres (see Picture 4, p. 110).

The newly appointed Minister of Defence, István Simicskó announced on 11th September, that 3800 soldiers built 10 kilometres of fence every day. On 14th September, the last free passage was closed with the use of a railway wagon reinforced with cutting edge wires at the Szeged-Horgos stage. With this step, closing of the Serbian-Hungarian "green" border became complete.

On 15th September, the Minister of Foreign Affairs announced, that the Government decided to prepare the construction of a fence along the Romanian-Hungarian border as well. So the engineering barrier is decided to be extended from the Romanian-Serbian-Hungarian border point to the River Maros and further in some kilometres. Three days later, on 18th September the Prime Minister announced, that an engineering border closing is to be built along the Croatian-Hungarian border in 41 kilometres. The construction was started immediately.

On 21st September Governmental Act 1665/2015 came out ordering the construction of the security border closing along the outer Schengen borders of Hungary in the counties affected by the crisis situation caused by mass migration. On 15th October it was officially announced that the engineering border closing was ready on the full length of the Croatian-Hungarian border.

On 16th October the same system came into force along the Croatian-Hungarian border, as it was already created one month earlier along the Serbian-Hungarian border. The "green" border was totally closed with combined use of physical devices and manpower, and entering into the territory of Hungary only at the official border crossing points became possible.

The Governmental Act 1665/2015 defines the "temporary security border closing" and its territory, but it does not describe its proper form, only says, that "an installation built and deployed for the protection of the state border's order in property of the state". This way it gives some flexibility to the constructors and the developers. It is very important because of the requirements derived from different terrains along the border. A lot of water-courses cross the border, roads and railways also can be found at the frontier, too. These points sometimes need special solutions, just remember the "reinforced wagon" used for the closure of the railway line as the last element of the border defence along the Serbian-Hungarian border.

The one and only purpose of the fence along the Croatian-Hungarian and Serbian-Hungarian borders is the restraint of the mass migration. This engineering barrier with the closure of previously open passages directs migrants towards the designated border crossing points, where the guarded and protected gates decrease security risk. For this purpose, this barrier is clearly visible, with gates and information signs written in several languages. It is suitable for safe deflection of people making the terms for controlled motions.

Deployment of the engineering obstacle, especially along the border needs specific attention. On one hand, the respect of the border is important. On the other hand the configuration of the proper trace is substantial. On harsh terrain, dense vegetation and changing ground properties are retarding the progress. Extreme weather (hot, rain, dust, cold or snow) can also detain the construction. Extreme press interest, frequent visits of the superiors or lack of necessary materials and assets can also be problems.

Concerning the efficient organization of this type of "linear" construction, one of the most important points is the determination of the "weakest link". You can have unlimited manpower in vein in the absence of the necessary machines and materials, and vice versa. Effectiveness can be raised with aligned working on many points at a time.

Other important factor that must be taken into consideration is the professionalism of the workers. And in most cases the problem is not the knowledge of machine-operators, but the unskilled labour. As the former experts and experiences left the Army years before, soldiers had to learn the fence construction skills again. In case of a disciplined organization like the military, it is not a serious problem, but the proper drill of the public workers is not an easy task. It means risk both for preparation and for safe and disciplined work.

The installation for the border protection was completed in time (see Picture 5, p. 111). In first stage, assessment and designation of the trace were made, than the settlement of the terrain, laying of wire rolls and finally building and signing of the fence. The task of the military is not finished, soldiers keep taking part in guarding and patrolling as well. This is just as important as the construction was. Participation means serious surplus work for the involved military units and personnel, so the reservist system and use of voluntary reservists can have great importance (Simicskó, 2011).

Because of the rapid construction some problems have remained unsolved, such as proper preparation of the ground along the fence so we can count with the introduction of some undergrowth and their consequences during the forthcoming months.

By the data of Frontex[1] there are 1.5 million migrants arrived to Europe in 2015, while 391 thousands of them vent through the territory of Hungary, coming from 104 different countries (frontex.europa.eu). 177 thousands of "Request for a Refugee Profile" were passed to the Hungarian authorities during last year, 508 of them was accepted, a lot of them was refused, but majority of the migrants were disappeared before the decision of the immigration bureau.

By the data of the Hungarian Police the number of illegal migrants greatly decreased after the completion of border fences, from 4-8 thousands to dozens, daily. From this time migrants preferred to choose Croatia and Slovenia to reach Austria and further Germany (www.police.hu).

This year already 18 thousands of refugee requests were passed till June, 4300 of them in the dedicated transit zones. There are 100-120 daily attempt to illegally crossing the borders of Hungary, so the continuous pressure is still exists (www.kormany.hu).

Conclusion

We can draw several lessons from the completed tasks in handling the mass migration emergency. The authors of this paper wanted to focus on the professional military engineering aspects, political and economical lessons are not our responsibilities. During the building of fences on our borders it was proved, that a work with these extents can be carried out only by the use of a well organized and equipped force with excellent logistic capabilities. Hungarian Defence Forces could meet this challenge with good capability assessment, task prioritization and deployment of appropriate forces and equipment.

Building fences is an accepted way for closing borders, obstruction of illegal migration, direction of masses of people and enhancing state security all over the world. But fences individually are useless without continuous supervision using technical and manpower assets. Only these can guarantee that fences will fulfil their task that they were built for. Another important issue, while the time of their cessation cannot be seen, their proper and responsible maintenance is also necessary in addition to the previously summarized tasks. Our prior experiences from peace support operations show that even one year without maintenance can cause serious damages and the effectiveness of the fences can drastically decrease.

One of the most important conclusions is that fences along the borders could reach the goal they had been built for. The migration pressure on our borders significantly decreased, which can be clearly seen from the statistical numbers. As the number of illegal migrants decreases, the feeling of safeness increases among our citizens.

[1] *Frontex: Management of Operational Cooperation at the External Borders of the Member States of the European Union (EU agency)*

However we know that fences are guarding the borders on several areas of the world for decades, this can not be a long term solution in Central Europe. The mass migration emergency problem has to be solved all along the borders of the European Union in a peaceful manner. The complete solution can come only with elimination of the reasons of mass migration in Africa and the Middle East. The efforts of the European countries should be focused on peaceful assistance to the developing countries in the crisis area to stabilize their governments to provide acceptable living standards to their people.

Bibliography

1. *Frayer, J. L., 2015. The Fences Where Spain And Africa Meet,10. March 2016.*
2. *Governmental Act, HUNGARY, 213/2015. (31 July) for modification of 211/2015. (23 July) Governmental Act for protection of workers involved into the construction of the temporary security border closing for border guarding and compensation because of the state expropriation.*
3. *Kovács, Z., 2004. A műszaki zárak alkalmazási lehetőségei a nem háborús katonai műveletekben, Hadtudomány, 2004. 3-4. Budapest http://www.zmne.hu/kulso/mhtt/hadtudomany/2004/3_4/2004_3_4_7.html.*
4. *Kovács, Z. 2001. Műszaki zárak a békefenntartó műveletekben, http://193.224.76.2/downloads/konyvtar/digitgy/20012/eloadas/kovacsz.html.*
5. *Nenov, S., 2016. Bulgaria's fence to stop migrants on Turkey border nears completion, 12 March 2016.Nielsen, N., 2012.: Fortress Europe: a Greek wall close up, 09 March 2016.*
6. *Padányi, J., Földi, L., 2015. Tasks and Experiences of the Hungarian Defence Forces in Crisis Management. CONTEMPORARY MILITARY CHALLENGES/SODOBNI VOJASKI IZZIVI (ISSN: 1580-1993) 17. 1., pp. 29-46. http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/vojaski_izzivi/2015/svi_17_1.pdf.*
7. *Sarkadi, Z., 2016. Az olasz hadsereg kész beavatkozni Líbiában, http://444.hu/2016/03/03/az-olasz-hadsereg-kesz-beavatkozni-libiaban, 13 March 2016.*
8. *Simicskó, I., 2011. A tartalékos rendszer fejlesztésének kiemelt kérdései. Hadtudomány 2011, 4 p. 78.*

Metodi Hadji-Janev
Marija Jankuloska

IZZIVI UPORABE DRONOV V DRŽAVAH JUGOVZHODNE EVROPE

THE CHALLENGES OF DRONE USAGE BY SOUTHEAST EUROPEAN COUNTRIES

Povzetek V članku so predstavljeni vidiki in izzivi uporabe tehnologije dronov v državah Jugovzhodne Evrope v luči izzivov, ki jih pomeni prisotnost terorizma in radikalnega ekstremizma v Jugovzhodni Evropi. Teza članka je, da bi vlade v tej regiji morale razmisliti o spremembah v zakonodaji in o posebnih zakonodajnih postopkih na nacionalni ravni, pri čemer je treba ustrezno upoštevati mednarodna načela in standarde, da ne pride do morebitne zlorabe tehnologije dronov.

Ključne besede ***Droni, brezpilotna letala, ciljno ubijanje, jus ad bellum, samoobramba.***

Abstract The article seeks to explore the perspectives and challenges of employing drone technology by the Southeast European countries (SEE countries) in the light of the challenges imposed by the presence of terrorism and radical extremism in the region of Southeast Europe. The article argues that SEE governments should consider legislative changes and special legislative procedures on domestic level with a due diligence of international principles and standards in order to inhibit any possible abuse of drone technology.

Key words ***Drones, UAVs, targeted killings, jus ad bellum, self-defense.***

Introduction

Modern terrorism which is practiced by radical religious groups and individuals affiliated to Al Qaeda and group known as Islamic State (IS) is a serious threat to the global peace and security. At the same time these groups' affiliates represent a serious security challenge to the region of South East Europe (SEE)[1] too. Many

[1] *The region of South Eastern Europe consists of countries predominantly of Balkan Peninsula including the Albania, Kosovo, Serbia, Bosnia and Herzegovina, Croatia, Greece, Romania, Bulgaria, Macedonia and Montenegro and some parts of Turkey, Italy and Slovenia.*

anecdotal and empirical evidences confirm that the threat posed by radical Islam and terrorism in the region of SEE is real. In addition to the anecdotal evidences (views and analyses by the experts, media and academia), three cases of terrorist attacks all related to radical Islam practice, were conducted in the region of SEE. The attack to the US Embassy in Bosnia (2011), terrorist attack at Smilkovci Lake in Macedonia (2012) and the suicide terrorist attack on the Israeli tourists in Bulgaria (2012), all of them point to the danger of spreading the radical Islam in the Region.

At the same time, the so-called "foreign fighters" trend is also present in the region. Although the exact number of the individuals who have joined Al Nusra in Syria or IS in Syria and Iraq is not clear SEE media have heavily reported about the deaths of the SEE citizens in these conflicts. Thus, global security trends in the context of threats from terrorism and countering these threats have seriously affected SEE countries in two ways.

On one hand the threat dynamics are similar as to the rest of the world. The strategic advantage that violent religious groups and individuals that use terrorism and threaten SEE security have, among others, is a direct result of the modern technology. Relying on modern technology (especially information technology) and by (ab)using modern processes, radical religious terrorists pose asymmetric and unconventional threats to SEE countries. Some of them are locals and some have migrated during the bloody conflicts in the Balkans.

On the other hand globally, the modern technology has directly affected the means and methods used in countering terrorists threats. One such example comes from the usage of the unmanned aerial vehicles (UAVs). Although earlier used as a tool for surveillance and reconnaissance in the contemporary counter-terrorist operations UAVs equipped with missiles are most frequently used as a weapon platform by some of the leading counter-terrorist nations (These UAVs are generally known as drones and therefore further in the article we will also use the term: drone/s when referring to the UAVs as a weapon platform). Giving that SEE countries, so far have followed the trends in counter-terrorist operations and efforts generally, and that most of the SEE countries have purchased or produce UAVs, the debate over their potential employment in the future counter-terrorist efforts as a weapon systems is of a great importance for several reasons.

First, use of the drones in the so-called "targeted killing" counter-terrorist operations is not generally supported, among others, for legal challenges that these operations produce. Related to former, it is true that global threat requires global response, however, different legal tradition has already "burned" some of the SEE countries, like Macedonia for example, in the so-called "*El Masri vs Macedonia case*". Third, although almost all SEE countries have or produce UAVs their usage is vaguely, if not, unregulated at all. Fourth, recent counter-terrorist measures in some of the SEE countries have been employed without serious analyses. Finally, the global counter-terrorist efforts have so far arguably felt the burden of "legitimacy deficiency" heavily due to the discrepancy in the legal approach among the coalition partners (European vs. US).

Therefore, the article by exploring both analytical and empirical evidences will briefly explain why and how terrorism represents a serious threat to the SEE security and will address the SEE experience in countering these threats. Then via legal analyses relying on the international-legal methodology, the article will explore whether use of drones in the future counter-terrorist operations by the SEE coalition partners could hurt the global counter-terrorist efforts. Finally, the article will provide some recommendations that SEE countries should consider to avoid challenges to their and the global counter-terrorist coalition efforts by using drones. Giving that other coalition partners from different regions in the global counter-terrorist efforts may face the same paradigm this article's finding hold potential to provide incentives wider than the region of South East Europe.

1 UNDERSTANDING THE THREAT FROM TERRORISM TO THE REGION OF SOUTH EAST EUROPE

Modern terrorism practiced by radical religious groups and individuals affiliated to Al Qaeda and associated movements and the group known as Islamic State (IS) is a serious security challenge to the region of South East Europe (SEE). Despite of the mismatched opinions, as already noted, both anecdotal and empirical evidences point to the genuine presence of radicalism and violent extremism in the region of SEE.

In spite of the conflicting views concerning the anecdotal evidences, two empirical indicators show that the South East Region has been swept by the radical wave. On one hand, the attack on the U.S. Embassy in Bosnia and Herzegovina (BBC, 2011), the murder of five civilians in Republic of Macedonia (Marusic, 2012) and the attack on the Israeli tourists in Bulgaria (BBC, 2012) and the multitude of reported attempts to attack clearly indicate that the threat is present in the Region and that the SEE countries like the rest of the world are vulnerable to the terrorist threat. Also, many reported attacks in Europe allude to some connections with radicalized groups from the region of SEE. Despite that, the Region has also become a source of radicalized individuals that take part in Syrian and Iraqi resistance movements as foreign fighters (Samardziski, 2015). The media reports and statistics about the radicalized individuals that have left their homeland in SEE to join the military and paramilitary groups in Syria and Iraq, as well as the numerous reported deaths of SEE foreign fighters attest that the Region has been subject of radicalization practices.

The unstable post-conflict societies of SEE overburdened by the turbulent past are perfect ground for the spread of radical Islam in the Region (Hadji-Janev, 2012). The ones that radicalize rely on technological progress and utilize flexible approaches to spread their agenda and to attract many followers and usually target weak and fragile societies. The complex environment is largely driven by the countries' turbulent past, history of inter-ethnic conflicts, economic challenges and social inequalities, division of the populace among ethnic and religious lines, ill-managed transition processes accompanied with corruption practices and the low reputation of the security services. All of these issues along with the rapid development of technology in the Region make SEE countries susceptible to the spread of the violent extremism.

2 SOUTH EAST EUROPEAN COUNTRIES' EXPERIENCE IN COUNTERING TERRORIST THREATS

SEE governments have seriously considered the threat from global terrorism posed by radical religious groups and individuals. Understanding that global threat requires global response, they have undertaken serious measures to strengthen domestic and global counter-terrorist efforts. (Caleta & Shemella, 2012). In this context there are serious evidences that SEE' intelligence community cooperation has also been enhanced and intensified (Pavlevski, 2013).

Almost all SEE countries have actively participated in the global counter-terrorist efforts with their strategic coalition partners. Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Macedonia, Montenegro and Slovenia have participated in ISAF and Albania, Bosnia and Herzegovina Bulgaria and Macedonia have been part of the coalition of willing in the so called: "Iraqi Freedom" mission. Nevertheless, different legal tradition entrenched by the European Convention for Human Rights (ECHR) and the European Court for Human Rights' practice (ECtHR) have raised serious challenges for SEE countries' counter-terrorist efforts.

For example, as a support to strategic partners' interest (i.e. the U.S.), Macedonian intelligence community has supported special intelligence gathering on suspected terrorist called Khaled El Masri. However, after he was released without charges the victim initiated legal case in front of the European Court of Human Rights. During the process called "El Masri vs. Macedonia", the Court found Macedonia guilty of violating the applicant's human rights in accordance with the European Convention for Human Rights (Hadji-Janev, 2013, pp. 55-69).

This example raises serious concerns in the context of SEE countries counter-terrorist efforts for two reasons. First, it signals to the potential adversaries (terrorists) the institutional limits that SEE governments have to confront them more aggressively regarding the European legal tradition. This is not to be understood that this article supports illegal interrogation techniques or any illegal counter-terrorist measures. This argument's intention is to illuminate the complexity and uncertainty that intelligence and security pundits face in their global counter terrorist efforts. Second, giving that acquisition of modern technology is important to keep up with coalition partners' tempo in the global counter-terrorist efforts use of specific technology such as drones, might be a serious problem for SEE governments.

Like the enhanced interrogation practice many have questioned the so-called "targeted killing operations" with drones. Most of the critics to these counter-terrorist operations have legal prefix too. At the same time almost all SEE countries have already purchased or produced UAVs (Radaljac, 2014; Šoštarić, 2007) or they are already in a process of acquiring UAV technology (*Đaković*, 2010). The recent drone incident that happened during the European Championship qualifications in Belgrade between Albania and Serbia set the urgency for legal regulation of the use of drone technology in the region of SEE. Considering that legality of counter-terrorist operations is tightly connected to the legitimacy we will continue our debate in the context of legal aspects of use of drones in the counter-terrorist operations.

This analysis should help SEE and global counter-terrorist coalition's strategists and leaders to understand whether, and if yes, under what conditions SEE countries can conduct targeted killing operations with drones. Understanding these conditions should further help in avoiding odd situations that could create uncertainty inside the counter-terrorist coalition (as it was the case with the so-called rules of engagement crisis during the Afghan counter-terrorist campaign). Namely, due to the different legal tradition and arguably different threat perceptions during the early phases in the counter-terrorist efforts in Afghanistan European coalition partners had strict rules of engagement. Most of them were reluctant to conduct robust combat operations and had therefore implemented a lot of caveats. This has created frustrations on the ground and has raised doubts among the coalition partners. Eventually, as the most severe critics of the global counter-terrorist efforts argue these dynamics have undermined coalitions' legitimacy.

3 UAV OPERATIONS FOR TARGETED KILLINGS AS A PART OF COUNTER-TERRORISM EFFORTS

Traditional direct approach (direct actions) means and methods in countering global terrorist threats practiced by Al Qaeda's and IS's affiliates have so far proven unreliable. As a result, states that feel most affected by these threats such as USA, UK and Israel significantly rely on drone technology for conducting offensive operations. Their use by the USA as a means for carrying out attacks in the name of the fight against terrorism, to date, have been reported in the territory of Afghanistan (Drew, February 19, 2010), Iraq (Rubin, August 8, 2014), Pakistan (Khan, January 6, 2010), Yemen (Black, 22 April 2014), Somalia (BBC News, 9 January 2007) and the small number of cases in Libya (Raddatz, April 23, 2011) and Syria. (NBC News, Nov 6, 2014). Besides the U.S., only Israel and UK use unmanned aircraft in combat operations (Cook, 2013; MacAskill, 2015), even though larger group of countries are developing or have already developed UAV technology (Wan and Finn, 2011).

This practice that was intensified after the arrival of Obama to the head of the United States is not spared from criticism regarding its correctness and legality. The views toward these attacks are divided. For many, they represent a successful and effective means for disruption of terrorist networks. Authors who hold this view also emphasize the precision of these weapons, the low cost for their production and, most importantly, the completely eliminated risk on the US armed personnel.

However, there are views that despite of the many advantages and the effectiveness of such attacks they are counterproductive and represent illegitimate means in the war on terror. Despite of the political and ethical concerns, these attacks have also raised serious legal issues. Considering the international-legal aspects, the use of unmanned aerial systems in cross-border operations touches upon the both legal regimes that govern the use of force (jus ad bellum and jus in bello), as well as the human rights law.

The main argument of the countries that utilize the unmanned aerial vehicles in counter-terrorist operations is that the drone capabilities offer more advantages compared to other options available to them. The use of drones for combat operations is politically justified because they do not pose a risk to the armed forces; they can be easily operated (Brooks, 2012) and they do not differ much from the traditional fighter jets and other conventional means of warfare in terms of their ability to cause collateral damage (Anderson, 2013). Another advantage is that they are equipped with sensors that increases their accuracy at large allowing the operators to have a clear picture of the target and the environment (Brennan, 2012). Moreover, they can easily penetrate into unavailable terrains and fly over targets for hours before targeting them. Additionally, these actions are preceded by a long process of intelligence and information gathering about the potential targets (Coll, 2014). All of this contributes for better identifications of the targets and reduced possibility of causing collateral damage.

But they are also problematic taking into consideration several aspects. Firstly, they are usually conducted by a civil agency (i.e. CIA) instead of the US armed forces (Mayer, 2009). CIA as a civil agency do not hold the status of a combatant under international law which means that they are not obliged to respect the laws and customs of war. The drone operators are distant thousands of miles from the target and they are not part of conventional combat operations. There is also a difficulty to locate responsibility in circumstances where there is no conventional movement of forces. Second, another problem is the lack of transparency and publicly uncovered information how many people are killed and how the targets are selected. There has been no specific figure about the number of victims although according to Guardian (assessment of the American Civil Liberties Union of 2002) so far there are about 4000 people killed by the attacks (Bowcott, 2012). According to another study, only in Pakistan the number of civilian deaths in the period from 2008 to 2013 ranged from 400 to 900 people (Bureau of Investigative Journalism, 2013). Peter Bergen and Katherine Tiedman in their analysis of drone attacks in Pakistan, estimated that the mortality rate of civilians as a result of the attacks in 2004 is 32% (Bergen and Tiedman, 2010). However, details about the overall policy of targeted killings remain shrouded in secrecy, making it impossible to get a clear and objective picture. This fact raises concerns of numerous human rights organizations and human rights activists who continuously call for greater transparency. Third, according to some authors the use of drones for execution attacks is a dangerous precedent that could encourage other countries to resort to such technology for future combat operations (Williams, 2013). Also, some claim that it is a matter of time before terrorists themselves will begin to use them (Kelley, 2013). Forth, some highlight the side effects arising from their use and the negative impact that they may have on the local population in the countries where they are carried out. According to such views, the attacks could easily generate anger and hatred that could further contribute to the emergence of new radicalized groups. This may in the future adversely affect and seriously harm the counter-terrorist efforts (Kilcullen & McDonald, 2009; Raghavan, 2009).

4 INTERNATIONAL-LEGAL ASPECTS OF THE UAV TARGETED KILLINGS

Another problem which, perhaps, the biggest differences between the scholars revolve around, is the issue of the legality of the UAVs targeted killings. The different views are partly resulting from different perceptions when it comes to the modern threats of terrorism and the right to life. The views which are mostly dominant in the European legal tradition emphasize that for the targeted killings carried out in countries where there is no declared state of war, their use should be governed by the rules and standards prescribed by the International Human Rights Law (IHRL). Contrary to this view, the US position is that the UAV target killings are part of an armed conflict which is global in character and where the geographical boundaries are irrelevant. Subsequently, according to the US view, the UAV targeted killings, no matter where they are conducted, they are governed by the law applicable in armed conflict (ILAC).

Legal criticism regarding this matter, which is currently dominant in the international community, is based on several reasons. Part of the criticism concerns the potential violation of sovereignty in countries where there is no armed conflict. Other humanistic-oriented critics indicate violations of human rights (especially the right to life). Reports of some NGOs often attest their view that these weapons (some claim they are non-discriminatory weapons) cause death of innocent civilians. Others claim that such attacks create implications in the field of international law of armed conflict, in particular that they affect the principles of proportionality and distinction. However, what is most evident for now is that there is a lack of a proper legal framework to regulate this matter.

From jus ad bellum perspective, these attacks are problematic, mostly, regarding the explanations brought forward to justify their use in countries not engaged in armed conflict with USA and their coalition partners. According to U.S. representatives these attacks are lawful judging on two independent grounds (Koh, 2010). The first is the highly contested “global war” argument, an assertion that USA is engaged in armed conflict with Al Qaeda and its affiliated groups. The second explanation according to which USA tries to build legitimacy for their operations refers to self-defense justification specifically employed to give grounds for the targeted killings conducted outside of the recognized theatre of war.

To determine whether the drone attacks were an act of legitimate self-defense or aggression they must be analyzed from the perspective of jus ad bellum. The legal regime of jus ad bellum regulates the conditions when and under what terms and circumstances the States may resort to the use of force against another State.

This legal regime consists of rules and standards that can be found in the UN Charter, customary law, and in certain decisions of international courts and tribunals. The ban of the use of force is stipulated in Article 2 of the UN Charter which requires States in their international relations to refrain from the threat or use of force against the territorial integrity or political independence of any State. The first exception of the general prohibition is set forth in Article 42 of the UN Charter, which authorizes the Security Council to use force in cases when there is an urgency to maintain or restore the international peace and security. The second exception is Article 51 which codifies States' inherent right of self-defense. The UN Charter reads as follows: "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security*". The right of self-defense under Article 51 consists of three components that have to be met in order to acknowledge that this right has been legally practiced. Namely, there must be an armed attack of sufficient gravity, the attack (according to the traditional view) to be attributable to certain State and the self-defensive act to satisfy the customary principles of necessity, proportionality and immediacy.

In terms of jus ad bellum, the targeted killings are often contested for two reasons: their use against non-state actors and continuous cross-border raids into countries outside of war zones. From the jus ad bellum perspective, U.S. justifies the attacks with their inherent right of self-defense which is guaranteed in article 51 of the UN Charter. Several dilemmas concerning the use of armed drones in cross-border operations arise as a result of this claim: (1) whether the right of self-defense is operable against non-state actors, in this case the use of drones for targeted killings against the suspected terrorists in foreign countries; (2) whether the exercise of this right challenges the generally accepted principles for the use of force in self-defense; and (3) whether this right can be a legitimate justification for carrying out drone attacks in sovereign States not involved in armed conflict or not responsible for armed attack against the territorial integrity of another State.

Besides all the dilemmas arising from jus ad bellum, the massive use of UAVs targeted killings in cross-border operations raises the question of sovereignty as an additional problem, especially since the attacks are carried out in sovereign countries which are not formally at war with USA. That is the case with Yemen, Pakistan and Somalia which over the years have demonstrated failure in dealing with terrorists who operate from their territory.

The USA offers two rationales as jus ad bellum justifications for UAVs attacks carried out in these countries. The first is that in most of the cases of drone attacks in Pakistan, Yemen and Somalia are carried out as a result of a consent provided by their governments. Second, in the absence of a required consent they employ the "unwilling and unable" doctrine to justify the attacks.

In this regard, Philip Alston (in his highly influential report on targeted killings) has outlined two circumstances when a targeted killing conducted in the territory of a sovereign state does not violate its sovereignty. The first is when the sovereign state has consented with the action and the second is when the conditions for lawful invocation of the right of self-defense under Article 51 of the UN Charter are met. According to the report, the latter is possible if the state on which territory the targeted killings have been conducted is not just responsible for an armed attack against the state which carries out the targeted killings, but also when the respective state is "*unwilling or unable to stop armed attacks against the first State launched from its territory*" (Alston, 2010, pp 11-12). Several authors including Michael Schmidt and Sean D. Murphy and few others are in the same line with Philip Alston citing the consent and the right of self-defense as legitimate grounds for justification for the use of drones in countries where there is no armed conflict. For instance, Michael Schmidt enumerates the circumstances under which the territorial state can express consent to other state's action on its territory. According to him, the consent can be issued either when the territorial state agrees other state to take action in self-defense on its territory or when the territorial state *itself* seeks assistance from another state (Schmidt, 2010, pp. 6). According to Sean D. Murphy, the the legality of the drone operations under international law is not questioned as long as the State that conducts the attacks on foreign territory have previously acquired consent from the territorial country (Murphy, 2008, pp. 118). Other scholars just emphasize the irrelevance of invoking self-defense justification in cases where there is already provided consent from the territorial State (Milanovic, 2010). Although the scholars are unanimous that the consent can preclude the wrongfulness of the employment of force in the territory of another State, there are some constraints that should be considered. Namely, the States by no means are allowed to consent to other States' action if such action has potential to endanger or violate applicable human rights and the peremptory norms.

Regarding the second justification, there are more or less three main sources for controversies over this issue. Firstly, in countries such as Pakistan, Yemen and Somalia there is no armed conflict or situation of occupation. The current terrorist activities are often qualified as isolated attacks rather than attacks which are sufficient enough to activate the right of self-defense. Secondly, even if we accept the fact that the attacks are carried out in accordance with the right of self-defense, there are certain conditions that must be met in order to consider that this right has been legally practiced. The Charter guarantees the right to self-defense only if the states that exercise the right of self-defense without any delay notify the Security Council for their action. Till now, there has been no notification sent to the Security Council for any of the drone attacks carried out in these countries. And lastly, none of these countries is directly or indirectly responsible for 9/11 attacks, or in any case involved in the preparation or planning future terrorist activities.

Irrespective of whether or not the drone strikes are lawful or not in respect of jus ad bellum, there particular use would fall under other applicable rules and is not dependent upon their legality in jus ad bellum. Till now, it is indisputable that the legality of the UAV targeted killings is largely determined by the context in which they are implemented (in time of peace or in time of war) and the rules applicable in a given situation. In fact, in international law there is a double standard when it comes of protecting human rights in times of armed conflict or during peacetime. The circumstances under which IHRL allows individuals to be deprived of their lives are strictly limited. According to the IHRL standards, the use of force can be considered legal only in exceptional circumstances where it is absolutely necessary and intended to prevent imminent threat to life and in circumstances where less extreme measures cannot be applied. Contrary to the IHRL standards, during armed conflict the legality of the use of force depends directly of the status of the persons against whom it is directed.

5 PERSPECTIVES ON DRONE USAGE BY SEE COUNTRIES

Drones (as the mostly utilized means for conducting targeted killings) were originally used as a platform for surveillance and reconnaissance in the war in Vietnam and furthermore, during the conflicts in Bosnia and Kosovo. However, a distinction should be underlined between armed and law enforcement drones utilized domestically. Till now, there are two generations of drones developed and used by the majority of countries. Ones still used for surveillance and reconnaissance, while the other group (equipped with weapons) is widely utilized in counter-terrorist operations for conducting counter-terrorist attacks and targeted killings against persons suspected of being part of the modern terrorism. In this regard, despite of the military purposes of the UAVs, they are also used for domestic law-enforcement aims such as border control and protection, intelligence gathering, reconnaissance and surveillance missions. Unlike the armed drones which primary affect the right to life, the law enforcement drones pose predominantly implications to privacy rights.

In respect of the region of SEE, another issue of concern is the easy accessibility of UAVs by private individuals for non-military purposes which represent a serious concern for SEE countries given the under-regulation and uncontrolled proliferation of unmanned aircraft. As already noted, many SEE countries have developed or are in the process of acquiring drone technology which can be easily owned by private individuals. The urgency for regulation of the proliferation of drone technology is perfectly reflected in the recent drone incident at the football match between Serbia and Albania. Despite that, this issue is equally important for SEE countries in circumstances when the majority of SEE countries are part of the counter-terrorism coalition. In this regard, firstly, acting in counter-terrorism coalition environment should require keeping the track with the new technological dynamics and the coalition partners' tempo in employing new types of weapons. Second, the rise of terrorism has become an increasing and imminent threat in the SEE region respectively which creates a possibility for future joint platform for cooperation in respect of the use and development of unmanned aircraft in order to ensure the effectiveness of employment of such advanced technology.

6 RECOMMENDATIONS FOR SEE COUNTRIES

In the light of the ongoing debate on the potential usage of drone technology for combat operations by the SEE countries, the SEE governments should take into consideration the following recommendations:

First, at domestic level the drone usage is still under-regulated. The SEE states should implement legislative changes that will lay down the circumstances under which the employment of drones in counter-terrorist operations would be considered as lawful. In order to evade any public opposition and condemnation domestically, the proliferation of drones should be limited only to situations strictly regulated under domestic laws. In addition, the SEE governments should establish special legislative procedures for the employment of drones in foreign countries along with investigation and accountability mechanisms incorporated in their legislatures in order to prevent possible abuses of drone technology.

Second, any possible usage of drones for offensive operations should be carried out in compliance with international law and more precisely, with a due diligence to the existing jus ad bellum rules, principles and standards. In this regard, the SEE governments should make a rigorous consideration of alternative opportunities before resorting to UAVs targeted killings.

Third, a well-articulated position and political dialogue should precede any possible employment of combat drones by the SEE countries. And lastly, the cooperation between SEE governments and coordination with their coalition partners should be prioritized in order to develop common approach toward the employment of cross-border lethal force against individuals who pose imminent threat to their security.

Conclusion

The threats of terrorism and Islamic extremism have become a serious threat to the countries of Southeast Europe. As indicated, both anecdotal and empirical evidences confirm this claim. At the same time the impact of modern technology has not bypassed the region of SEE. The acquisition of modern technology by the SEE governments has raised serious concerns. The tendency to purchasing and developing their own unmanned aircraft opens the question about the possible use of these aircraft in joint action or combat operations by the SEE countries, but also the urgency of their effective regulation. This question poses implications to both international law and domestic legislation.

Although under international law there is no explicit prohibition of introducing new and sophisticated weapons, their use must by strictly regulated in order not to be utilized in non-discriminatory and perfidious manner. Despite that, their use in combat operations must be in accordance with fundamental principles of international law applicable in armed conflict.

The effects of the new technological dynamics that have also affected the Region of SEE have also urged for domestic regulations of the utilization of unmanned aircraft.

Relative to these tendencies, the SEE governments should consider legislative changes and special legislative procedures, as well as tightening restrictions on domestic level with a due diligence of international principles and standards in order to inhibit any possible abuse of such technology.

Bibliography

1. *Anderson, K., 2013. The Case for Drones, Commentary, Vol. 135, No. 6, pp. 14-23, available at http://www.commentarymagazine.com/article/the-case-for-drones.*
2. *BBC, 19 July 2012. Bulgaria blast: 'Suicide bomber' killed Israelis, BBC News, available at http://www.bbc.com/news/world-europe-18897772.*
3. *BBC, 28 October 2011. Sarajevo gunman fires at US embassy in Bosnia capital, BBC News, available at http://www.bbc.com/news/world-europe-15499143.*
4. *BBC, 9 January 2007. US 'targets al-Qaeda' in Somalia, BBC News, available at http://news.bbc.co.uk/2/hi/africa/6245943.stm.*
5. *Bergen, P., Tiedemann, K., 2010. The Year of the Drone, available at http://www.newamerica.net/sites/newamerica.net/files/policydocs/bergentiedemann2.pdf.*
6. *Black, I., 22 April 2014. Yemen conflict highlighted after 55 killed in air raids and drone strikes, The Guardian, available at http://www.theguardian.com/world/2014/apr/22/yemen-conflict-in-spotlight-after-drone-strikes-air-raids.*
7. *Bowcott, O., 21 June 2012. Drone strikes threaten 50 years of international law, says UN rapporteur, The Guardian, available at http://www.theguardian.com/world/2012/jun/21/drone-strikes-international-law-un.*
8. *Brennan, J., 30 April 2012. The Ethics and Efficacy of the President's Counterterrorism Strategy, Transcript of Remarks by John O. Brennan, available at http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy.*
9. *Brooks, M., 13 June 2012. If you can play a video game, you can fly a drone, available at http://www.newstatesman.com/sci-tech/sci-tech/2012/06/play-video-game-fly-drone.*
10. *Caleta, D., & Shemella, P., (Eds.). Managing the Consequences of Terrorist Acts - Efficiency and Coordination Challenges, 2012, ISBN: 978-961-92860-5-0, available at: http://www.ics-institut.com/research/books/4.*
11. *Coll, S., (November 24, 2014). The Unblinking Stare, The New Yorker, available at http://www.newyorker.com/magazine/2014/11/24/unblinking-stare.*
12. *Cook, J., 2013. Gaza: Life and death under Israel's drones, Al Jazeera, available at, http://www.aljazeera.com/indepth/features/2013/11/gaza-life-death-under-israel-drones-html.*
13. *Đaković, T. N., 2010. Prva srpska bespilotna letelica/The first Serbian unmanned vehicle, Blic, available at http://www.blic.rs/Vesti/Tema-Dana/187488/Prva-srpska-bespilotna-letelica.*
14. *Drew, C., 2010. Drones Are Playing a Growing Role in Afghanistan, The New York Times, available at http://www.nytimes.com/2010/02/20/world/asia/20drones.html?_r=0.*
15. *Hadji-Janev, M., 2014. Solving the counter-terrorist puzzle after the El Masri verdict and Smilkovci terrorist attack: legal and strategic considerations for the South East European intelligence communit. In: Intelligence and Combating Terrorism: New Paradigm and Future Challenges, Center for Civil Military Relations Monterey, USA, Ljubljana, pp. 207-221. ISBN 978-961-92860-8-1.*
16. *Hadji-Janev, M., 2013. Legal Aspects of Intelligence Gathering through Extraordinary rendition Operations, in Stephen R. Di Rienzo, Ferdinand Odzakov, (Eds.) Shaping The Security Environment Western Balkans and Beyond, Ministry of defense Republic of Macedonia, pp 55-69, 04/2013; ISBN: ISBN 978-9989-2851-4-1, COBBIS.MK-ID 93727498 In book.*
17. *Kelley, M., 2013. America Is Setting A Dangerous Precedent For The Drone Age, Business Insider, available at http://www.businessinsider.com/america-is-setting-a-dangerous-precedent-for-the-drone-age-2013-1.*

18. *Khan, I., 2010. Drone Strikes Reported in Pakistan, The New York Times, available at http://www.nytimes.com/2010/01/07/world/asia/07drones.html*
19. *Kilcullen, D., McDonald, A., 2009. Death From Above, Outrage Down Below, N.Y. Times, available at http://www.nytimes.com/2009/05/17/opinion/17exum.html?pagewanted=all&_r=0.*
20. *Koh, H., 2010. The Obama Administration and International Law remarks to the American Society of International Law (25 March 2010), available at http://www.state.gov/s/l/releases/remarks/139119.htm.*
21. *MacAskill, E., 2015. Drone killing of British citizens in Syria marks major departure for UK, The Guardian, available at http://www.theguardian.com/world/2015/sep/07/drone-british-citizens-syria-uk-david-cameron.*
22. *Marusic, S.J., 2012. Unsolved Killings Raise Fears of Macedonian Turmoil, Balkan Insight, available at http://www.balkaninsight.com/en/article/unsolved-killings-raise-fears-of-macedonian-turmoil/btj-topic-justice-and-politics-latest-headlines-right-column/26.*
23. *Mayer, J., 2009. The Predator War, The New Yorker, available at http://www.newyorker.com/reporting/2009/10/26/091026fa_fact_mayer.*
24. *Milanovic, M., 2010. More on Drones, Self-Defense, and the Alston Report on Targeted Killings, EJIL: Talk!, http://www.ejiltalk.org/more-on-drones-self-defense-andthe-alston-report-on-targeted-killings/.*
25. *Murphy, S. D., 2008. The International Legality of US Military Cross-Border Operations from Afghanistan into Pakistan, Int. Law Studies, volume 85, pp. 109-139.*
26. *NBC, 2014. U.S. Drone Strike in Syria Takes Out Khorasan Bomb-Maker: Officials, NBC News, available at http://www.nbcnews.com/news/world/u-s-drone-strike-syria-takes-out-khorasan-bomb-maker-n242626.*
27. *Pavlevski, A., 2013. Western Balkans intensify military, intelligence co-operation, SETimes.com, available at http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2013/05/27/feature-02.*
28. *Radaljac, D., 2014. Hrvatska obvezna nabaviti 30-ak bespilotnih letjelica, available at http://www.novilist.hr/Vijesti/Hrvatska/Hrvatska-obvezna-nabaviti-30-ak-bespilotnih-letjelica?meta_refresh=true.*
29. *Raddatz, M., 2011. Pentagon Confirms First Predator Drone Strike in Libya, ABC News, available at http://abcnews.go.com/International/pentagon-confirms-predator-drone-strike-libya/story?id=13442570.*
30. *Raghavan, S., 2012. In Yemen, U.S. airstrikes breed anger, and sympathy for al-Qaeda, The Washington Post, available at http://articles.washingtonpost.com/2012-05-29/world/35456187_1_aqap-drone-strikes-qaeda.*
31. *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, 2010. Study on targeted killings Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6.*
32. *Rubin, A. J., August 8, 2014. U.S. Jets and Drones Attack Militants in Iraq, The New York Times, available at http://www.nytimes.com/2014/08/09/world/middleeast/iraq.html.*
33. *Samardziski, A., 2015. Стотина македонски државјани војуваат за паравоени формации во Сирија и во Ирак / Hundreds of Macedonian citizens fight for paramilitary formations in Syria and Iraq, Nova Makedonija, available at http://www.novamakedonija.com.mk/NewsDetal.asp?vest=4291517766&id=12&setIzdanie=23457.*
34. *Šoštarić, E., 2007. Na Udbini tvornica špijunskih letjelica/Factory for spy aircraft in Udbina, Nacional.hr, available at http://arhiva.nacional.hr/clanak/40777/na-udbini-tvornica-spijunskih-letjelica.*
35. *Summary of the International Law Discussion Group meeting held at Chatham House, International Law and the Use of Drones, 2010, available at http://www.chathamhouse.org/publications/papers/view/109506.*

36. *The Bureau of Investigative Journalism, Covert Drone War, available at http://www.thebureauinvestigates.com/category/projects/drones/drones-pakistan/.*
37. *Wan, W., Finn, P., 2011. Global race on to match U.S. drone capabilities, The Washington Post, available at http://www.washingtonpost.com/world/national-security/global-race-on-to-match-us-drone-capabilities/2011/06/30/gHQACWdmxH_story.html*
38. *Williams, C., J., 2013. U.S. drone use could set dangerous example for rogue powers, L.A.Times, available at http://articles.latimes.com/2013/feb/07/world/la-fg-wn-us-drones-global-precedent-20130206.*

József Kis-Benedek

ISLAMSKA DRŽAVA IRAKA IN LEVANTA TER MEDNARODNI BOJ PROTI NJEJ

ISLAMIC STATE OF IRAQ AND THE LEVANT AND THE INTERNATIONAL FIGHT AGAINST IT

Povzetek Kriza v Iraku in Siriji bo še nekaj let v središču mednarodne in evropske pozornosti. Cilji glavnih velesil in koalicijskih partnerjev se razlikujejo, sedanje mednarodne institucije pa sploh niso učinkovite pri obvladovanju konfliktov, saj se po svetu širijo versko pogojena ekstremistična gibanja. V članku analiziramo okoliščine in vzroke za vzpon organizacije ISIL/DAESH, vlogo glavnih akterjev pri obvladovanju krize, sodelovanje tujih borcev in boj proti tej teroristični organizaciji.

Ključne besede *ISIL/DAESH, Sirija, Irak, Bližnji vzhod, terorizem.*

Abstract The Iraqi and Syrian crisis will dominate international and European agendas for several years. The aims of great powers and coalition partners are different; the existing international institutions are not at all effective in the handling of the conflict, while religiously-motivated extremist movements has been spreading in the world. This article analyses the causes and circumstances of the rising of ISIL/DAESH, the role of the main participants in the handling of the crisis, the participation of foreign fighters, and the fight against the terrorist organisation.

Key words *ISIL/DAESH, Syria, Iraq, Middle East, terrorism.*

Introduction

"The Middle East influenced by the conception of Sykes-Picot began to disintegrate. Sir Mark Sykes and Francois Georges-Picot were British and French diplomats who redrew the map of the region between the Mediterranean Sea and Persia after World War I" (Friedman, 2014, p. 4). The Sykes-Picot agreement was signed in 1916 and determined the political situation of the region for many years by dividing the Arab lands between France and Great Britain. Today, as we witness the disintegration of

Iraq and Syria, there are many more political and economical interests (American, Russian, Kurdish, Iranian, Turkish and so on) so the Sykes-Picot agreement cannot hold for long.

The question is how far the collapse of the post World War I system will go. Will the national governments reassert themselves in a decisive way, or will the fragmentation continue? Will this process of disintegration spread to the other heirs of Sykes and Picot? This question is perhaps more important than the emergence of ISIL/DAESH[1]. Religiously-motivated extremist movements are a factor in the region, and will assert themselves in various organizational forms. What is significant is that while it is a force, ISIL/DAESH is in no position to overwhelm other factions, just as they cannot overwhelm it. Thus it is not ISIL/DAESH, but the fragmentation and the crippling of national governments that matters. More than 300,000 Syrians have lost their lives in these five years of armed conflict, which began with anti-government protests before escalating into a full-scale civil war. More than 11 million others have been forced from their homes as forces loyal to President Bashar al-Assad and those opposed to his rule battle each other – as well as Extremists Claiming Affiliation with Islam (ECAI).

I am convinced that the book of Samuel P. Huntington on The Clash of Civilization (written 20 years ago) is also very relevant in 2016. “The religious revival has in part involved expansion by some religions, which gained new recruits in societies where they had previously not had them. To a much larger extent, however, the religious resurgence involved people returning to, reinvigorating and giving new meaning to the traditional religions of their communities.” (Huntington, 1997, p. 96).

1 THE SHORT HISTORY OF ISIL/DAESH

1.1 The Iraqi line

“ISIL/DAESH can trace its roots back to 2002, when Abu Musab al-Zarqawi – a Jordanian who was to gain notoriety in the Iraqi insurgency from 2003-2006 – founded a so-called jihadist organisation called *Tawhid wal-Jihad* in the north of Iraq. Zarqawi had been linked with al-Qaeda while in Afghanistan in the late ‘90s, but was not a member of the group and disagreed with the tactic of focusing on the ‘far enemy’ (the West) as opposed to the ‘near enemy’ (rulers in the Islamic world). Following the 2003 invasion of Iraq, Zarqawi’s organisation grew more active and affiliated itself to al-Qaeda in 2004, becoming al-Qaeda in Iraq (AQI). Despite the tactical differences, this made a useful alliance. Zarqawi’s organisation gained the recruiting and resourcing benefits of being part of a global and credible so-called jihadist organisation, while al-Qaeda gained an affiliate in Iraq, already by that stage the global centre of jihad.” (Welby, 2015).

[1] *DAESH: Dawla al-Islamiya al-Iraq al-Sham (Islamic State of Iraq and the Levant- ISIL).*

Zarqawi's AQI was an influential actor in Iraq's descent into chaos between 2003 and 2007. It had the explicit policy of stoking sectarian violence with the aim of rallying the Sunni community around Sunni so-called jihadist groups, a tactic that ISIL/DAESH is replicating now. This gained criticism from al-Qaeda's leaders, who felt that the indiscriminate and brutal violence risked alienating their supporters. However, it continued to support Zarqawi in public until he was killed in an airstrike in 2006.

In late 2006 AQI joined with eight other so-called Islamist insurgent groups to form the Islamic State of Iraq (ISI), without permission from the al-Qaeda leadership. The name chosen for this new group indicated its ambitions: it was more than a mere jihadist group, but an embryonic caliphate, governed by Islamic law, to which all Muslims within its territory owed allegiance.

The alliance between al-Qaeda and ISIL/DAESH was no longer convenient. ISIL/DAESH could now claim a history and a support base that established its credibility, and al-Qaeda's central leadership was weak. An ISIL/DAESH spokesman declared that al-Qaeda's leader, Ayman al-Zawahiri, was sinful, and Jolani nothing less than a traitor. Shortly afterwards, Zawahiri announced that ISIL/DAESH had nothing to do with al-Qaeda.

The political and military successes of ISIL/DAESH in the summer of 2014 were shocking. Cities fell to ISIL/DAESH forces a fraction of the size of their defenders; soldiers were ordered to abandon their posts; and those soldiers who were captured were massacred. Based on its advance, the group declared a caliphate, a move that has split the so-called jihadist world despite long being the aspiration of such organizations.

"In September 2014, the US began a military campaign against ISIL/DAESH in Iraq and Syria, supported by more than a dozen European and Arab states. Extensive airstrikes have supported the operations of the Iraqi Kurdish ground troops in making strategic gains." (McInnis, 2014). In Iraq, the Peshmerga forces were able to dislodge ISIL/DAESH from key areas around Mount Sinjar in December 2014. Furthermore, in March 2015 Iraqi security forces, aided by Shia militias supported by Iran, launched the first major government offensive against ISIL/DAESH since June 2014, in Tikrit. However, 2015 brought setbacks for the group, including the Iraqi Kurdish forces. A hard-fought four-month battle for the city of Kobane, on the Syrian-Turkish border, culminated in victory for the YPG (Popular Protection Units) in January 2015 – although ISIL/DAESH has maintained a presence nearby. We have to note that NATO countries recognized both the Kurdish Democratic Union Party (PYD) and its military division YPG as terrorist organizations.

By claiming responsibility for the November 2015 attacks in Paris and the downing of a Russian plane in Egypt, ISIL/DAESH gives the impression that the group, ordinarily focused on targeting the near enemy, is keen to convey a broadening of its operational strategy and the pursuit of targets further afield.

Regardless of these defeats, the development of ISIL/DAESH since 2013 has changed the nature of the group. It is no longer a mere terrorist group, but an army that can hold and administer territory. It governs according to harshly interpreted principles of Islamic law, including the imposition of *dhimmi* pacts on minorities – guaranteeing protection in exchange for the payment of a tax and the acceptance of second-class citizenship. Minorities, including Shia Muslims, have been subject to severe human rights abuses, including massacres and forced conversion, and the persecution of minorities in northern Iraq has been particularly brutal. ISIL/DAESH has also provoked shock and condemnation worldwide for its brutal execution of foreign journalists and humanitarian aid workers, as well as captured combatants from opposing forces. While the quality of its governance is questionable, it can broadly coerce the consent of the people it governs.

"At the end of 2015 the Iraqi army, with coalition air support, succeeded in gaining significant territories from ISIL/DEASH, including the reoccupation of Ramadi." (Glenn, 2014).

1.2 The Syrian line

Pro-democracy protests erupted in March 2011 in the southern city of Deraa, after the arrest and torture of some teenagers who had painted revolutionary slogans on a school wall. After security forces opened fire on demonstrators, killing several, more took to the streets.

The unrest triggered nationwide protests demanding President Assad's resignation. The government's use of force to crush the dissent merely hardened the protesters' resolve. By July 2011, hundreds of thousands were taking to the streets across the country.

Opposition supporters eventually began to take up arms, first to defend themselves and later to expel security forces from their local areas.

The violence escalated and the country descended into civil war as rebel brigades were formed to battle government forces for the control of cities, towns and the countryside. Fighting reached the capital Damascus and the second city of Aleppo in 2012.

"By June 2013, the UN said 90,000 people had been killed in the conflict. However, by August 2014 that figure had more than doubled to 191,000 – and continued to climb to 250,000 by August 2015, according to activists and the UN." (UNHCR MUNIC VII, 2016, p. 6).

The conflict is now more than just a battle between those for or against President Assad. It has acquired sectarian overtones, pitching the country's Sunni majority against the President's Shia Alawite sect, and drawn in neighbouring countries and world powers. The rise of the so-called jihadist groups, including ISIL/DAESH, has added a further dimension.

"More than four million people have fled Syria since the start of the conflict, most of them women and children. It is one of the largest refugee exoduses in recent history. The neighbouring countries have borne the brunt of the refugee crisis, with Lebanon, Jordan and Turkey struggling to accommodate the flood of new arrivals. The exodus accelerated dramatically in 2013, as conditions in Syria deteriorated." (Rodgers, BBC News, 11 March 2016, p. 1).

A further 7.6 million Syrians have been internally displaced within the country, bringing the total number forced to flee their homes to more than 11 million – half the country's pre-crisis population. Overall, an estimated 12.2 million are in need of humanitarian assistance inside Syria, including 5.6 million children, according to UN reports.

"In December 2014, the UN launched an appeal for $8.4bn (£5.6bn) to provide help to 18 million Syrians, after only securing about half the funding it asked for in 2014. By a year later, it was less than half funded. This is one of the causes of the refugee crisis into Europe." (Rodgers, Gritten, Offer, Asare, 2016, p. 1).

"A report published by the UN in March 2015 estimated the total economic loss since the start of the conflict was $202bn and that four in every five Syrians were now living in poverty – 30% of them in abject poverty. Syria's education, health and social welfare systems are also in a state of collapse." (Conflict background I am Syria, 2016, p. 1).

The armed rebellion has evolved significantly since its beginning. Secular moderates are now outnumbered by jihadists, whose brutal tactics have caused widespread concern and triggered rebel infighting.

The Syrian war also facilitated ISIL/DAESH's final break with al-Qaeda. Since 2006, the group's relationship with al-Qaeda had been ambiguous, possibly deliberately so; the mutual benefits that had first prompted Zarqawi to affiliate to the organisation remained. In 2011, Baghdadi created a Syrian subsidiary, Jabhat al-Nusra (JN), under Abu Mohammad al-Jolani. In 2013, with JN showing unwelcome signs of independence, Jolani announced their re-absorption into the expanded Islamic State of Iraq and al-Sham – 'al-Sham' being the Arabic name for Greater Syria, with connotations of earlier caliphates. However, Jolani appealed to al-Qaeda's central command, which ruled in his favour, ordering Baghdadi to confine his group to Iraq. Jabhat al Nusra split from al Qaeda in July 2016. The new name is Jabhat Fateh al-Sham (Front for the Conquest of Syria). "The director of US National Intelligence described the split as a PR move." (Sly, DeJoung, 2016, p. 2).

In subsequent fighting in Syria, much of it with other rebels including JN and other jihadist groups, ISIL/DAESH has gained and held significant amounts of territory. It captured the city of Raqqa from other rebels in early 2014, using it since as a base to launch attacks in Syria and Iraq. In Iraq, the group exploited botched Iraqi military operations in Fallujah in January 2014 to gain control of the city. Control of sparsely populated transport corridors allowed them to advance rapidly in the kind of surprise attacks that delivered them Mosul, among other cities, in June of the same year. Profiting from the chaos in the region, ISIL/DAESH has taken control of huge swathes of territory across northern and eastern Syria, as well as in neighbouring Iraq. Its many foreign fighters in Syria are now involved in a "war within a war", battling rebels and jihadists from the al-Qaeda-affiliated Nusra Front, who object to their tactics, as well as Kurdish and government forces.

"ISIL/DAESH has been forced out of about 56 places where it once had control, including five major cities. This process has not yet finished. Unfortunately there are signs that the group has been shifting its focus from controlling territories to executing terror attacks in Iraq, Syria and abroad." (Sly, DeJoung, 2016, p. 1).

The following maps show the territorial gains and losses in 2015 and 2016. I would like to remark that the size of territories and population has been changing day by day. When the Islamic State of Iraq (ISI) was established in 2006, ISIL claimed seven Iraqi and 9 Syrian provinces, covering most of the countries. In autumn 2016 ISIL/DAESH lost about 45% of its former occupied territories (see Picture 1 and 2, p. 112).

2 ISIL/DAESH AFFILIATES AND ADHERENTS

Since 2014, some armed groups have recognized the ISIL/DAESH caliphate and pledged loyalty to Baghdadi. Groups in Yemen, Egypt, Algeria, Saudi Arabia, Libya, Afghanistan, and Nigeria have used the Arabic word "*wilayah*" (state/province) to describe themselves as constituent members of a broader IS-led caliphate (Blanchard, Humud, 2016, p. 3).

Why is it important to detail the ISIL/DAESH affiliates in 2016? Since the autumn of 2015, with the military actions of Russia and the other international coalitions, ISIL began to lose territories (up to August 2016 it has lost about 45% of its former territory). This does not mean the end of ISIL/DAESH, as some of its affiliate organisations are able to take over the task of ISIL.

In 2016, the following ISIL/DAESH adherents are the most significant and capable of terrorist actions:

2.1 ISIL/DAESH affiliates in Egypt (Sinai Province, Wilayah Sinai)

ISIL/DAESH's local affiliate in the northern Sinai Peninsula was formerly known as *Ansar Bayt al Maqdis* (Supporters of the Holy House or Partisans of Jerusalem). It emerged after the Egyptian revolution of 2011 and affiliated with ISIL/DAESH in 2014.

Estimates of its membership range from 500 to 1,000, and it is comprised of radicalized indigenous Bedouin Arabs, foreign fighters, and Palestinian militants.

Among their armaments are man-portable air defence systems (MANPADS), such as the 9K338 Igla-S, and Kornet anti-tank guided missile (ATGM) systems. The organization has claimed credit for destroying Metrojet Flight 9268, which exploded in mid-air over the Sinai Peninsula on October 31, killing all 224 passengers aboard.

2.2 ISIL/DAESH affiliates in Saudi Arabia (Wilayah Najd/Haramayn/Hijaz)

IS leaders have threatened the kingdom's rulers directly and called on the group's supporters there to attack Shiites, Saudi security forces, and foreigners. ISIL/DEASH supporters have claimed responsibility for several attacks e.g. suicide bombing attacks on Shia mosques in different parts of Saudi Arabia, and in a Kuwaiti mosque, killing more than two dozen people and wounding hundreds. Saudi officials have arrested more than 1,600 suspected ISIL/DAESH supporters (including more than 400 in July 2015) and claim to have foiled several planned attacks.

ISIL/DAESH poses a unique political threat to Saudi Arabia, in addition to the tangible security threats demonstrated by a series of deadly attacks inside the kingdom since late 2014. IS leaders claim to have established a caliphate to which all religious Sunni Muslims owe allegiance, directly challenging the legitimacy of Saudi leaders who have long claimed a unique role as Sunni leaders and supporters of particular Salafist interpretations of Sunni Islam. ISIL/DAESH critiques of Saudi leaders may have resonance among some Saudis who have volunteered to fight for or contributed on behalf of Muslims in several conflicts involving other Muslims over the last three decades.

2.3 ISIL/DAESH affiliates in Libya (Wilayah Tarabalus/Barqa/Fezzan)

Supporters of ISIL/DAESH in Libya have announced *three* affiliated wilayah (provinces), corresponding to the country's three historic regions – *Wilayah Tarabalus* in the west, *Wilayah Barqa* in the east, and *Wilayah Fezzan* in the south-west. Some observers put the group's strength in Libya at several hundred to a few thousand fighters among a much larger community of so called Salafi-jihadist activists and fighters. Since late 2014, ISIL/DAESH supporters have taken control of Muammar al Qadhafi's hometown, Sirte, and committed a series of atrocities against Christians and Libyan Muslim opponents. They also have launched attacks against forces from Misrata and neighbouring towns in an effort to push westward and southward. ISIL/DAESH backers sought to impose their control on the eastern city of Darnah. There is no concrete data, but we can suppose that this organization can train people who could appear in Europe.

2.4 ISIL/DAESH affiliates in Nigeria (West Africa Province [Wilayah Gharb Afriqiyyah])

Two of the most significant African insurgent groups – Boko Haram in Nigeria and al-Shabaab in Somalia – are looking to ISIL/DAESH, possibly to gain momentum, as both groups are facing the increased pressure of successful military operations against them. The Islamist group Boko Haram pledged its allegiance to ISIL/DAESH in early March 2015, more specifically to the 'Caliph of Muslims', Abu Bakr al-Baghdadi. The pledge coincided with successful operations against Boko Haram carried out by a coalition of Nigerian forces and neighbouring countries affected by Boko Haram violence (Neill, 2015, p. 8). This north-eastern Nigeria based Sunni insurgent terrorist group is widely known by the name *Boko Haram* ("western education is forbidden"). In 2014 alone, 5,500 have been killed and more than 1.5 million people have been displaced by related violence, which increasingly spread into neighbouring Cameroon, Chad and Niger in 2015. The group threatens civilian, state and international targets, including Western citizens in the region. Boko Haram's announcement of allegiance to ISIS coincides with its ousting from key towns in north-eastern Nigeria. Meanwhile, Somalia's al-Shabaab also appears to be flirting with the idea of associating itself with ISIL/DAESH, having been seriously weakened by the African Union-led *Operation Indian Ocean* and US airstrikes targeting its leaders.

2.5 ISIL/DAESH affiliate in Yemen (Wilayah al Yemen, Wilayah Al Bayda, Wilayah Aden-Abyan, Wilayah Shabwah)

In Yemen, militants who claim allegiance to ISIL/DAESH have taken advantage of ongoing war to repeatedly bomb mosques known for attracting worshippers of Zaydi Islam, an offshoot of Shia Islam (with legal traditions and religious practices which are similar to Sunni Islam). ISIL/DAESH terrorists have targeted supporters of the Houthi Movement, a predominately Zaydi armed militia and political group that aims to rule wide swathes of northern Yemen and restore the "Imamate."

2.6 ISIL/DAESH affiliate in Afghanistan and Pakistan (Wilayah Khorasan)

ISIL/DAESH is attempting to expand its reach in both Afghanistan and Pakistan. ISIL/DAESH presence in Afghanistan and Pakistan appears to consist of certain individuals of more mainstream insurgent groups, particularly the Afghan Taliban, showing themselves as members of "ISIL/DAESH of Khorasan Province," or *Wilayah Khorasan*. This group differs from the Khorasan Group identified by U.S. officials as being an Al Qaeda affiliated cell seeking to conduct transnational terrorist attacks. It does not appear that the ISIL/DAESH leadership has sent substantial numbers of fighters from Iraq and Syria into Afghanistan or Pakistan. ISIL/DAESH's presence and influence in Afghanistan remains in the exploratory stage. It is known that there is growing competition and conflict between the Taliban and ISIL/DAESH fighters.

3 THE AIMS AND INTERESTS OF THE MOST IMPORTANT PARTICIPANT COUNTRIES

3.1 United States

The United States lost its credibility in the Middle East because of the wars in Afghanistan and Iraq. Its support in Iraq, but mainly in Syria, is very low from both the leadership and the general population.

“The US has accused President Assad of responsibility for widespread atrocities and says he must go. But it agrees on the need for a negotiated settlement to end the war and the formation of a transitional administration.” (Syria crisis BBC News, 30 October 2015, p. 1).

The US supports Syria's main opposition alliance, the National Coalition, and provides limited military assistance to "moderate" rebels. The question is, who are the moderate and who are the radical rebels?

Since September 2014, the US has been conducting air strikes on ISIL/DAESH and other jihadist groups in Syria and Iraq as part of an international coalition against the so-called jihadist group. But it has avoided attacks that may benefit Assad’s forces or intervening in battles between them and the rebels.

A programme to train and arm 5,000 Syrian rebels to take the fight to ISIL/DAESH on the ground has suffered embarrassing setbacks, with few having even reached the frontline (nobody knows how many fighters have joined ISIL/DAESH after the training).

Assessing the role of the United States in Iraq and Syria, we cannot forget the current election campaign and the unsuccessful policy towards Iraq (and also Afghanistan). After the transfer of the focal point to the Far East in 2012, a new hybrid war began in 2014 in Ukraine against Russia. In the Middle East in summer 2016, the USA faced tremendous difficulties from Egypt to Yemen, not to mention Turkey. To tell the truth concerning the Iraqi and Syrian war, the US is satisfied with the proxy war. I really hope that after January 2017 the US policy toward Iraq and Syria will change, and they do more to diminish (and maybe to end) the war in these countries, reducing the refugee problem in Europe.

3.2 Russia

In the new multipolar world, Russia is attempting to establish its own place. First Crimea (with its special meaning for Russia and no hint of irredentism) and then Syria (where Russia fights against the arbitrary change of regimes and not for the current President of Syria Bashar al-Assad) indicate the global ambitions of Moscow, which no longer wants to be confined to the status of a rank-and-file regional power. Moscow has managed to mitigate some of the worst impacts of the post-Ukrainian adventure, such as isolation, and proved that to a certain extent it is a regional and global player. Putin has demonstrated a capacity to play his weak hand very well and has, at least, made the case that you cannot ignore Moscow.

Russia is one of Syrian President Bashar al-Assad's most important international backers and the survival of the regime is critical to maintaining Russian interests in the country.

It has blocked resolutions critical of President Assad at the UN Security Council and has continued to supply weapons to the Syrian military despite international criticism.

Moscow wants to protect a key naval facility which it leases at the Syrian port of Tartous, which serves as Russia's sole Mediterranean base for its Black Sea fleet, and also has forces at an air base in Latakia, President Assad's Shia Alawite heartland.

In September 2015 Russia began launching air strikes against rebels, saying Islamic State (IS) and "all terrorists" were targets. However, Western-backed groups were reported to have been hit.

President Vladimir Putin has said that only a political solution can end the conflict. No doubt he is right, but while there is no political agreement, unfortunately the situation on the battlefield influences the events.

“Three factors made the Kremlin’s policies in 2015 quite different from routine political, diplomatic and economic dialogue.” (Polikanov, Utkin, Smirnova, Kornilov, 2015; Russia Direct Report: Russia and the World: Foreign Policy Outlook 2016, p1). Firstly, the ominous shadow of ISIL/DAESH changed the dynamic of Russia’s Middle East foreign policy. The rise of ISIL/DAESH gave impetus to all sides concerned to do as much as they could to join Russia’s efforts to establish an international anti-terrorist coalition.

Secondly, 2015 witnessed an obvious shift from an exclusively Ukrainian focus in international politics to Syria as the topic most discussed by the key players in the region and beyond.

Thirdly, a strategic shift in Russia’s Middle East policy took place on September 30 2015, when the Russian Air Force started to bomb ISIL/DAESH positions in Syria.

The three pillars of Russian foreign policy in Syria:

First, it is necessary to unite and coordinate the efforts of those who can make a real contribution to the fight against terror. It would be useful to coordinate the efforts on the basis of Security Council resolutions in accordance with the United Nations Charter. Whatever we say about some progress in international anti-terrorist efforts, this idea continues to be current. The anti-terrorist coalition is still going to emerge.

Second, all the concerned parties should facilitate the internal Syrian dialogue on the basis of the Geneva Communiqué of June 30, 2012.

Third, it is important to ensure an inclusive and balanced external support of the political process with the participation of Russia, the United States, Saudi Arabia, Iran, Turkey, Egypt, the United Arab Emirates, Jordan and Qatar. The European Union, according to Minister Lavrov, could also play a useful role, as well as China.

Unfortunately, clear misunderstandings between the concerned parties are quite evident. Saudi Arabia, Qatar and some other partners in the Syrian dialogue do not agree with the Russian proposals for the settlement of the crisis.

3.3 Turkey

The Turkish government has been a staunch critic of Assad since the start of the uprising in Syria. President Recep Tayyip Erdogan has said it was impossible for Syrians to "accept a dictator who has led to the deaths of up to 350,000 people". Turkey is a key supporter of the Syrian opposition and has faced the burden of hosting almost two million refugees. But its policy of allowing refugees and humanitarian aid to pass through its territory has caused foreign terrorists to use this territory to reach Syria and Iraq in order to join ISIL/DAESH. However, Turkey has made great progress in preventing FTFs from passing through its borders. “Several hundred suspected terrorists have been captured and sent back to their countries of origin, and also hundreds of terrorists have been arrested.” (Capelouto, 2015, p. 1).

In addition to this information it is important to note that Turkey agreed to let the US-led coalition against ISIL/DAESH use its air bases for strikes on Syria.

The role of Turkey is extremely important, not only in the fight against ISIL/DAESH, but also in the fight against the radicalization of refugees. The possible radicalization of refugees is a problem of the near future. “The term ‘radicalization’ is used widely, but a consensus on its definition and drivers have yet to be achieved, and past research has proved of little explanatory value.” (Dawson, Edwards, Jeffray, 2014, p. 10).

Turkey has, though, been critical of coalition support for the Syrian Kurdish Popular Protection Units (YPG) – an affiliate of the banned Turkish Kurdistan Workers' Party (PKK), recognized as a terrorist group by Turkey, the EU and the US.

The reconciliation between Turkey and Russia on 9 August 2016 significantly contributed to the fight against ISIL/DAESH, future regional developments and also the future of President Bashar al Assad. It is too early to assess the impact of this agreement, but we can establish it may also have an effect on the future of NATO.

3.4 The Kurdish problem

While speaking of the region we cannot neglect the situation of the Kurds. Because of its complexity this topic should be the theme of a separate study. This nation (about 30 million people mainly in four countries) merits an independent country, but the religious and civil war did not help this process at all. The position of the Kurds is “best” in Iraq, thanks to oil and the Iraqi history. They were able to defend themselves against the move of ISIS into the Kurd Autonomous area. The future of Iraq cannot be realised without Kurdish autonomy (more autonomies than they currently have). The western alliance helps the Peshmerga forces in fighting against ISIL, and the Kurds have an important role in fighting against ISIL in Iraq. In Syria the situation for the Kurds is much worse than in Iraq, since they are attacked not only by the Assad forces but also by the Turkish army.

A huge problem is the political division in the population. In Iraq the Kurds have a strong relationship with Turkey. In Syria the biggest Kurdish party, the PYD, is an enemy of Turkey and is in close contact with the PKK, which is in war with the government. The basic question is whether the Kurds can have territory and independence after the reconciliation or not. The role of Turkey is indispensable in a future Kurdistan. I think that the establishment of a Kurdish state is a question of the distant future.

3.5 Iran

Iran as a Shia power is believed to help the Assad regime by providing billions of dollars for military advisers and weapons.

Assad is Iran's closest Arab ally, and Syria is the main transit point for Iranian weapon shipments to the Lebanese Shia Islamist movement, Hezbollah. Iran is also believed to have been influential in Hezbollah's decision to send fighters to western Syria to assist pro-Assad forces.

Militiamen from Iran and Iraq who say they are protecting Shia holy sites are also fighting alongside Syrian troops.

Iran has proposed a peaceful transition in Syria that would culminate in free, multi-party elections. It was involved in peace talks over Syria's future for the first time when world powers met in Vienna. The Russian-Iranian military cooperation in the fight against ISIL/DAESH (use of an Iranian airbase by Russian bombers) may open a new chapter in the relationship between the two countries.

3.6 Saudi Arabia

The Sunni-ruled Gulf kingdom says President Assad cannot be part of a solution to the conflict, and must hand over power to a transitional administration or be removed by force.

Riyadh is a major provider of military and financial assistance to several rebel groups, including those with religiously-motivated ideologies, and has called for a no-fly zone to be imposed to protect civilians from bombardment by Syrian government forces.

Saudi leaders were angered by the Obama administration's decision not to intervene militarily in Syria after a 2013 chemical attack blamed on Assad's forces.

They later agreed to take part in the US-led coalition air campaign against ISIL/DAESH, concerned by the group's advances and its popularity among a minority of Saudis.

The Syrian crisis happens to be the pivot of both the current European refugee challenge and the terrorist threat.

3.7 The role of international organizations

The ongoing crises in Europe and in the Middle East and North Africa demonstrate that the existing institutions (the UN, NATO, and the EU) are largely impotent and cannot provide a universal remedy for the resolution of these crises. Without going into detail I think that the international organizations have made a lot of declarations and decisions, but in the field there are few effects of these decisions. The UN has a clear position in the fight against ISIL/DAESH, but unfortunately the organization was not able to mediate between the belligerents. The result of the activities of NATO and the EU cannot be seen in the region.

4 PARTICIPATION OF FOREIGN FIGHTERS IN IRAQ AND SYRIA

“According to U.S. intelligence officials more than 18,000 foreign fighters have now flocked to the region -- up from about 16,000 at the start of November 2014. An estimate by The National Counter Terrorism Center in September had put the number of foreign fighters at more than 15,000.” (Seldin, 2014, p. 1).

“The number of Western passport holders joining the fight has also grown to at least 3,000. Earlier estimates had put the number of Westerners fighting in Iraq and Syria at about 2,700.” (Besenyő, 2015, p. 5).

However, officials caution that the higher estimates do not necessarily mean that there are more fighters on the battlefield. U.S. intelligence officials say most of the foreign fighters heading to Iraq or Syria seem to be intent on joining ISIL/DAESH, although many are still fighting with the al-Qaida-affiliated Nusra Front or with other groups. There is also hope that the flow of foreign fighters to the region will begin to subside.

It is important to analyze whether ISIL/DAESH is indeed a rising Islamic jihadist force about to seize control of several countries in this region as part of its plan to establish an Islamic caliphate, or whether it is an organization with limited means and abilities, whose pretensions exceed its real strength and are derived from the world view of its leader. “Without minimizing the achievements of ISIL/DAESH, it appears that the secret of its power rests primarily on the weakness of its enemies. So far, ISIL/DAESH states are those whose central governments suffer from a lack of legitimacy among their citizens and ineffective control of large parts of their territory.” (Schweizer, 2014, p. 1). Most Sunni Muslims are not interested in the extreme interpretations of ISIS/DAESH, but at this stage they have no choice but to obey the organization, if only for the sake of appearances. Should ISIL/DAESH try to extend its conquests to areas of Iraq where there is an established Shiite population, such as the capital Baghdad or the holy cities of Najaf and Karbala, it may well encounter a fighting population protected by an Iranian military force and the deeper involvement of Western countries, as happened when it threatened to penetrate the heart of the Kurdish region of Iraq. A similar response can be expected if ISIL/DAESH dares to confront Jordan or Turkey. For that reason, its threats to make similar advances against other countries of the region – Jordan, Lebanon, and certainly Iran and Turkey – are weak.

When starting a war it is important to clarify who is the enemy. The basic question is: who is the main enemy in Iraq and Syria? Unfortunately the belligerents have different goals and enemies. The main target is ISIL/DAESH, but the means of defeating it are different. This chapter attempts to perceive how complicated the situation is in Syria.

What began as another Arab Spring uprising against an autocratic ruler has mushroomed into a brutal proxy war that has drawn in regional and world powers.

ISIL/DAESH is an organization built around an idea. It is the latest, most competent and brutal perception of a way of thinking that is around a century old. It was not ISIL/DAESH that attacked New York in 2001, Madrid in 2003 or London in 2005, but those responsible were part of the same movement. That movement is extremism. At its core is a belief that all social, political and economic activity must be governed by a single interpretation of Islamic law, and violent jihad is a just way to achieve this.

In September 2014, a US-led coalition launched air strikes inside Syria in an effort to "degrade and ultimately destroy" ISIL/DAESH, helping the Kurds repel a major assault on the northern town of Kobane. But the coalition has avoided attacks that might benefit Assad's forces or intervening in battles between them and the rebels.

In the political arena, opposition groups are also deeply divided, with rival alliances battling for supremacy. The most prominent is the moderate National Coalition for Syrian Revolutionary and Opposition Forces, backed by several Western and Gulf Arab states. However, this coalition has little influence on the ground in Syria and its primacy is rejected by other groups, leaving the country without a convincing alternative to the Assad government.

Iran and Russia have helped the Alawite-led government of President Assad and have gradually increased their support.

In September 2015, Russia launched an air campaign against Assad's opponents. Moscow said it was targeting "all terrorists", above all members of ISIL/DAESH, but many of the strikes hit Western-backed rebels and civilians.

The Syrian government has also enjoyed the support of Lebanon's Shia Hezbollah movement, whose fighters have provided important battlefield support since 2013.

Moderate opposition has, meanwhile, attracted varying degrees of support from its main backers – Turkey, Saudi Arabia, Qatar and other Arab states, along with the US, the UK and France. However, the rise of radical rebels and the arrival of so called jihadists from across the world have led to a marked cooling of Western backing. A programme to train and arm 5,000 Syrian rebels to take the fight to ISIL/DAESH on the ground has suffered embarrassing setbacks.

“The US-led campaign against ISIL/DAESH, known as Operation Inherent Resolve, has launched over 6,000 airstrikes against ISIL/DAESH and is killing about 1,000 militants every month, roughly the same number believed to be joining the group, leaving the group's manpower strength effectively capped at 30,000 to 40,000. ISIL/DAESH has had to adopt a different strategy since the beginning of aerial attacks on the group in Iraq and Syria, no longer having the freedom of movement it once enjoyed. With Russia entering the war and carrying out airstrikes against ISIL/DAESH targets, the group's capabilities will be further diminished.” (Welby, 2015, p. 1).

The December 2015 decisions on French, German and British air force engagement will probably have a limited effect on the developments in Syria, but they will play a significant role in the intra-European debates on foreign policy.

The disagreements on Syria will not disappear overnight, but they could take a milder form as the practical military-to-military communication in battling the radical groups, and the slow progress in political talks, could change the atmosphere. Military events will dictate many things in the diplomatic process.

As for Syria, it would be extremely problematic to preserve the integrity of the country when so many actors prefer to see sectarian cantons in Syria.

Conclusion

The Syrian crisis will dominate international and European agendas for several years. The unresolved conflict has a direct effect on both the European refugee crisis and on terrorism. With regard to the solution of the Iraqi-Syrian crisis, I am convinced that it will not happen in the short term; it will take many years. The coalitions are constantly transforming, and countries like Turkey are members of different coalitions. After the coup d'état in Turkey the Turkish armed forces became weaker, and this has had an effect on its participation in the Syrian-Iraqi conflict. The reconciliation of Russia and Turkey is also encouraging for the future of Syria. The participation of Russia in the political processes is indispensable. Russian-Iranian military ties are important, but raise a lot of security concerns in the region (it is enough to think of Israel and Saudi-Arabia). Referring to the policy of the United States, we cannot disregard the election campaign, but this is a temporary event. I am convinced that the new administration will participate more actively in the settlement. The common Russian-US actions against ISIS are also encouraging.

As for ISIL/DAESH, the military operations carried out since the end of 2015 by the Iraqi Army, helped by the coalition forces, have been a significant blow to the terrorist organisation.

The loss of territory, equipment and supporters are all good news, but based on previous experience, organizations like this follow an asymmetrical warfare which means more terrorism in the region and beyond. Religiously-motivated radicalism is spreading not only in the Middle East and Africa, but also in Europe.

References

1. *Almukhtar, S., Wallace, T.; Watkins, D., 2016. ISIS has Lost Many of the Key Places It Once Controlled. The New York Times. http://www.nytimes.com/interactive/2016/06/18/world/middleeast/isis-control-places-cities.html?_r=0, 21.08.2016.*
2. *Besenyő, J., 2015. Not the invention of ISIS: Terrorists among immigrants. Journal of Security and Sustainability Issues, Volume 5, Number 1, pp. 5–20.*
3. *Glenn, C. Timeline: Rise and Spread of the Islamic State https://www.wilsoncenter.org/article/timeline-rise-and-spread-the-islamic-state (last visited:21.08.2016.)*
4. *Blanchard, C. M.; Humud, C. E., 2016. The Islamic State and U.S. policy. https://fas.org/sgp/crs/mideast/R43612.pdf, 06.12.2015.*

5. *Capelouto, S.; Gul, T., 2015. Turkey arrests hundreds of suspected terrorists, Prime Minister says. CNN. http://edition.cnn.com/2015/07/25/middleeast/turkey-syria-isis-attacks/, 07.02.2016.*
6. *Conflict background I am Syria. http://www.iamsyria.org/conflict-background.html, 07.02.2016.*
7. *Dawson, L., Edwards, C.; Jeffray, C., 2014. Learning and adapting: The Use of Monitoring and Evaluation in Countering Violent Extremism. In: Royal United Services Institute for Defence and Security Studies (RUSI) Whitehall, London SW1A 2ET, ISBN 978-0-85516-124-8. p10.*
8. *Friedman, G., 2014. The Top Five Events in 2014. Stratfor Geopolitical Weekly. http://www.stratfor.com/weekly/top-five-events-2014#axzz3NJ1tsbwB, 30.12.2014.*
9. *Huntington, S. P., 1997. The Clash of Civilizations. Touchstone, Rockefeller Center. ISBN-0684-81164-2 p96.*
10. *McInnis, K. J., Coalition Contributions to Countering the Islamic State. https://www.fas.org/sgp/crs/natsec/R44135.pdf (Last visited 23.08.2016.)*
11. *Neill, H. U., 2015. African insurgent groups look to ISIS as they face increasing pressure. https://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2015-dda3/march-a921/african-insurgent-groups-look-to-isis-as-they-face-increasing-pressure-262b, 06.12.2015.*
12. *Polikanov, D., Utkin, S., Smirnova, L., Kornilov, A., 2015. Russia Direct Report: Russia and the World: Foreign Policy Outlook 2016. http://www.russia-direct.org/archive/russia-direct-brief-russia-and-world-foreign-policy-outlook-2016, 25.12.2015.*
13. *Rodgers, L., Gritten, D., Offer, J., Asare, P., 2016. Syria: the story of the conflict. BBC News. http://www.bbc.com/news/world-middle-east-26116868, 21.08.2016.*
14. *Schweitzer, Y., 2014. ISIS: The Real Threat. INSS Insight No. 596. http://www.inss.org.il/index.aspx?id=4538&articleid=7572, 31.12.2014.*
15. *Seldin, J., 2014. Estimates Rising of Foreign Fighters in Iraq, Syria. http://www.globalsecurity.org/security/library/news/2014/12/sec-141224-voa02.htm?_m=3n.002a.1299.qi0ao00qad.16wb, 31.12.2014.*
16. *Sly, L., DeJoung, K., 2016. Syria's Jabhat al-Nusra splits from al-Qaeda and changes its name. The Washington Post. https://www.washingtonpost.com/world/middle_east/syrias-jabhat-al-nusra-splits-from-al-qaeda-and-changes-its-name/2016/07/28/5b89ad22-54e6-11e6-b652-315ae5d4d4dd_story.html, 21.08.2016.*
17. *Syria crisis: Where key countries stand. BBC News, 30 October 2015. http://www.bbc.com/news/world-middle-east-23849587, 21.08.2016.*
18. *UNHCR MUNIC VII. http://munik.iba.edu.pk/VII/wp-content/uploads/2015/12/UNHCR.pdf, 06.02.2016.*
19. *Upreti, P., 2015. The summary of crises in Damascus. The Times of Israel. http://blogs.timesofisrael.com/a-summary-of-crises-in-damascus/, 07.02.2016.*
20. *Welby, P., 2015. What is ISIS? http://tonyblairfaithfoundation.org/religion-geopolitics/commentaries/backgrounder/what-isis, 24.12.2015.*

Aleš Avsec

CIKEL USPOSABLJANJA BATALJONSKE BOJNE SKUPINE

BATTLE GROUP TRAINING CYCLE

Povzetek Bataljonska bojna skupina (v kopenski vojski ZDA angl. *Task Force, NATO – Battle Group)* je orodje za izboljšanje bojnih zmogljivosti celotne Slovenske vojske, saj ne gre le za pehotni bataljon, temveč za enoto, ki vključuje vse zvrsti in nujno podporo. Cikel usposabljanja kot del operativnega cikla pomeni poslanstvo bataljonske bojne skupine, kar je skladno z določili Zakona o obrambi, Vojaške doktrine in drugih strateških dokumentov – ohranjanje pripravljenosti za zagotavljanje vojaške obrambe. Čeprav je ameriška kopenska vojska veliko večja, mora skozi enake stopnje kolektivnega usposabljanja bataljona kot bataljon SV, kar je tudi eden izmed vzrokov, da smo za primerjavo izbrali cikel bataljonskega usposabljanja kopenske vojske ZDA. Po drugi strani imajo ameriške enote več izkušenj z usposabljanjem in bojevanjem, SV pa veliko izkušenj z usposabljanji kopenske vojske ZDA. Za zagotovitev uspeha je treba jasno določiti seznam bistvenih nalog (SBN) za izvedbo poslanstva (Mission Essential Task List – METL), ki daje ustrezne usmeritve in podlago za razvoj načrta za usposabljanje enot (Unit Training Plan – UTP). Usposabljanje brez evalvacije je brez pomena, zato je evalvacija sklepna faza vsakega usposabljanja. Na podlagi predpisanega poslanstva, SBN in UTP ter jasnih evalvacijskih standardov smo usposabljanje bataljonske skupine SV primerjali s kopensko vojsko ZDA, da bi tako izboljšali cikel usposabljanja bataljonske skupine SV.

Ključne besede ***Bojna skupina, cikel usposabljanja, poslanstvo enote, seznam bistvenih nalog za izvedbo poslanstva (METL), kolektivno usposabljanje.***

Abstract Battalion Battle Group (Bn BG) (U.S. Army term Task Force) is a tool to improve combat capabilities of the entire Slovenian Armed Forces, since it is not just an Infantry battalion, but it includes all the branches and support that comes with it. The main mission of the Bn BG is the training cycle as part of the operation cycle, which is in line with what Defence Law, Military Doctrine and other strategic documents stipulate – "maintaining readiness to execute military defence". Even though U.S. Army is a much larger force, it still has to go through the same stages of battalion collective training as SAF battalion, which is one of the reasons why U.S. Army battalion cycle was used as comparison. On the other hand it has much more training and war experience, and the SAF has a lot of experience with U.S. Army training. In order to be successful, it is necessary to have a clear Mission Essential Task List (METL), which gives guidance and constitutes a basis for the development of the Unit Training Plan (UTP). It is a waste to perform any training without evaluation, which is why BG evaluation is the final stage of every training. With the assigned mission and METL, developed UTP and clear evaluation standards, SAF Battalion BG training cycles were compared with the U.S. Army in order to improve SAF Bn BG training cycle.

Key words ***Battle Group (BG), Task Force (TF), training cycle, unit mission, mission essential task list, collective training***

Introduction

After the breakup of Yugoslavia in 1991, Slovenia initially adopted a conscript army, since that was the concept of the Yugoslav army, well known to the SAF. That was suspended completely in 2003, even though by 1997 the first professional battalion (Bn) was established. Another important event for the SAF was joining NATO in 2004, which gave the defence forces a new approach and a lot of things to be improved. The training of a professional force developed through the years and is still developing. The transition from hourly prescribed training for coscript soldiers, to a "mission command" type training is still underway. Currently, commanders of the units do not receive much guidance, except mission and organization, and since doctrine is evolving, it is hard to come up with a training plan that would match the available resources. This is critical today when the Slovenian Armed Forces (SAF) is facing drastic budget cuts.

Even though the SAF is composed of two manoeuvre Brigade Combat Teams (BCT's) in reality half of the size of a U.S. Army BCT, complemented with army aviation units, a naval detachment, Special Operations Forces unit and a Logistic Support Brigade with roughly 7,500 active and 1,500 reserve soldiers, training one Battle Group (BG) at a time is the main goal. BGs rotate between the two manoeuvres BCTs, which also provide direction, guidance, support and combat support elements for the battalion that they are developing. The BCT has a goal to both develop and train the BG or to have an operationally ready BG normally partly deployed to NATO operations like International Security Assistance Force (ISAF) or Kosovo Force (KFOR) or others. So while one of the Bn BG is training within one of the BCTs, the other one is operational in the other BCT. This rotation between BCTs is normally done within an 18-month cycle.

The Bn BG is not just the SAF's main training mechanism; it is also a tool to develop the whole Slovenian Armed Forces. Since there are all branches included in the multifunctional BG, this also provides a chance to develop their capabilities. It is a development concept for organizational, training, doctrine, equipment and other perspectives. However, for the purpose of this research, only the training part was examined. Interoperability within the NATO structure is also one of the aspects that can be tested throughout the training and deployment cycle.

Within this concept of multifunctional BG, armies like the SAF can develop doctrine, organization, training, equipment, leadership, education, infrastructure, and interoperability. We can use this concept to develop all the elements of the SAF. Multifunctional BG also allow the SAF to execute a combined arms operations, like U.S. Marines do with the Marine Expeditionary Unit (MEU), or the US Army does with BCTs. We can train for a joint fight with all the combat support multipliers all together with other services as well. Combat service support also has to be employed and developed as necessary.

Beside the manoeuvre infantry battalions, which are normally motorized with 6x6 or 8x8 Armoured Personal Carriers (APC), there are other elements such as; an artillery battery, combat engineer platoon, air defence platoon, reconnaissance -intelligence element, civil-military cooperation (CIMIC) and psychological operations (PSYOPS) group, nuclear biological and chemical (NBC) element and a Forward Support Company (FSC) logistic element. All of this is to be part of the multifunctional BG concept, not just to provide capabilities but also to provide a development basis for all different elements within the SAF.

The main question concerns training of the multifunctional BG from a qualitative perspective. Even though U.S. Army is a much larger force than the SAF, battalion training cycle still goes through similar stages in most of the armies in the Alliance. SAF training cycle can thus be compared with a US Army Infantry Bn/BCT. On the other hand, we have Infantry and Stryker BCTs. Even though they are larger in size, these units still execute the same stages of training and use an 8 x 8 Stryker APC like the SAF. Therefore, the main research question for this paper was: what improvements can be made to the training cycle or concept for training a multifunctional BG for the SAF?

The other research questions are: how can we improve the SAF's BG training cycle as part of the Army Force Generation Cycle (AFORGEN) comparing it with the US Army? What are the best situated missions and METLs to drive training and how to develop them? How to develop a Unit Training plan? How to evaluate BG readiness?

This research is significant for the whole SAF since it develops not just the multifunctional BG, but also all other elements. Addressing doctrine, organization, training, material, people, leadership, facilities (DOTMPLF), for each element of the BG drives the development for the whole SAF. Slovenia could build larger armed forces in case of emergency using multifunctional BGs with reintroducing conscription, which would provide an additional 25,000 troops. On the basis of the BG training cycle, the SAF would be able to generate and develop a force within relatively short period, if resourced properly.

Along with most of the armies of the Western countries, the SAF is also facing drastic budget cuts. Optimizing our training cycle with a common goal and understanding what drives our army as a whole, should make available resource use more efficient. Another assumption is that Slovenia as part of the NATO will not have all the capabilities of a larger army. That is one of the main reasons why we are part of the Alliance, and with this said it will develop what is needed with the resources that are currently available. Even though there are some thoughts to reduce the army, events like the ongoing refugee crisis in Europe prove again that small countries need a capable army to not only do its primary mission of national defence, but also to assist police and other agencies when security challenges are raised, or when natural disasters occur.

The scope of this paper is limited to the training of the multifunctional BG, since organization, doctrine, and other elements of DOTMPLF would be too extensive for this study. The SAF has conducted BG training cycles for almost ten years and is constantly changing and developing the cycle focusing predominantly on SAF experience.

1 METHODOLOGY

A qualitative research methodology was used to examine NATO and U.S. Army training doctrine and management systems in light of the requirements of the SAF, to determine improvements that should be made to the SAF multifunctional BG training cycle. This research will add to the literature on the topic, which is necessary to improve military readiness and leadership preparedness within the SAF and Slovenia's defence system.

The research process consisted of three main phases. The first phase consisted of the collection and selection of data and information. The second phase was identification of key areas of difference between current SAF multifunctional BG training cycles and U.S. Army and NATO training management systems and doctrine. These areas of difference provide substance for the assessment process. In the final phase, collected data and information were analysed and a clear and concise conclusion is proposed.

The ability to understand training quality and efficiency of resources was gained using doctrinal literature and documented empirical examples. Data was collected from the different training models and training examples. Qualitative analysis, first of doctrinal data and also of executive documents (different examples of BG training models), as well as training orders, BCT and Bn Commanders guidances and SOPs were included.

Documentation review was the first step to actually examine all available doctrinal publications and materials. It was first necessary to study in depth all the available documents regarding NATO training, SAF Bn training and then US Army Bn /BCT training. After that it was necessary to study BG cycles for the US Army IBCT and

Bn. All available U.S. Army publications were used, together with prior research that covered some aspects of training cycles. A part of this step was also a review of how to develop a mission, how we develop our training goals, and what tasks the SAF is supposed to train for. Both of the armies use Mission Essential Task List (METL), but the level of detail and the approach used to develop them is different. It was also important to study how the NATO Universal Task List (UTL) and Army Task List (ATL) impact certain METL.

In order to answer other research questions of "how to develop a Unit Training Plan," part of the research was a review of how to plan battalion training in detail and provide resources. There are different models that are being followed for successful training plans. The U.S. Army and the SAF both have guidelines. The question is how can SAF improve or learn from the U.S. Army and improve SAF multifunctional battalion training cycles. Resources are another challenge, especially for smaller militaries like the SAF during an economic crisis. Different approaches with a common goal, to be better, and especially to be more efficient are even more important for smaller militaries. In the SAF, there is no standard model of resourcing the training cycle; a lot depends on the BG commander and his ability to influence decision makers. Resourcing training also depends on our NATO allies, mostly the US Army in Europe. Since the SAF does not have a BG training area and capabilities to develop an environment (HICON, role players, OC-T, etc.) to conduct a BDE seize exercise, the SAF tries to utilize U.S. BCT size exercises and align SAF training goals with theirs in order to maximize SAF training opportunities. The US Army is not dealing with those issues to such an extent, so finding better ways to improve SAF resourcing of the training cycle was another part of the subject of this research.

To address the main research question, this research focused on training cycles that are the most relevant to the needs of the SAF. Since Slovenia is a NATO member, NATO requirements must be met. According to NATO Bi-SC Capability codes and capability statements from Jan 2016 (NATO, Supreme Headquarters allied powers Europe, *BI-SC Capability codes and capability statements* (Mons, 2016), 65.), a Light infantry battalion should be able to:

Capstone capability statement: Capable of employing organic motorized infantry at battalion level (predominantly dismounted) in land tactical activities to deliver operational and strategic agility by exploiting light Protected Patrol Vehicles (PPV), which will provide basic protected mobility to ensure operational and strategic mobility.

Even though the concept of military training cycles has been around for a long time, there were significant changes through time. A long time ago for U.S. forces, and 15 years for SAF, military training was for conscript soldiers, which requires a completely different approach than with the training of professional soldiers. While conscript armies conduct training for a limited time, normally from 6 to 12 months which limits the level of professionalism and readiness, professional soldiers stay in the SAF for at least 5 years (minimum contract for the SAF). This allows individuals and units to be better trained, not so much for individual skills, but definitely much better trained in collective tasks from platoon to brigade level.

The next step of this methodology was to examine the training cycle. The SAF multifunctional BG training cycle was examined and then the training cycle of a U.S. Army infantry battalion. It is necessary to determine the initial status of the unit entering the training cycle. All the individual training should be done and units should be from at least 90% to 100% in personnel and equipment. This screening criteria is necessary to ensure a valid evaluation between units and prevent making judgements based on units that are dissimilar. The examination of different kinds of training elements such as shooting, simulation training, situational and command post exercises (STX, CPX), provided a good basis for evaluation. The unit's training calendar for the whole training cycle, with all important training events, allows for examination of the differences between current SAF multifunctional battalion training cycles and U.S. Army and NATO training management systems and doctrine. The differences between SAF training cycle examples were based on different Unit Training Plans (UTP), where it is obvious which events including repetitions had been conducted.

The next important step is how to evaluate the readiness of a certain unit. This is tied to the secondary research question of "How to evaluate BG readiness." Training is all about achieving standards, so how do we determine if the units are trained to a certain standard? In the past, the US Army used the Army Training Evaluation Programs (ARTEP), which were exact measures for either confirming or denying readiness of certain units. Those were adopted also in the SAF, and were especially used at the SAF Combat Training Centre (CTC). So there is an institution in the SAF that it is in charge of training and more importantly certifying units within the SAF, either when achieving final readiness capabilities or as part of pre-deployment training. Most of the observer controller - trainers (OC-T) are trained by the US Army; however they can process just one company at a time. The U.S. Army can process at least BCT size element through its collective training programs at the NTC or JRTC at one time, together with all the combat multipliers. On the other hand, U.S. forces abandoned ARTEPs and are using just official reports from CATS, the so-called Training Evaluations and Objectives (TE&O). Within NATO, there are also different approaches to evaluation, as for example the Combat Readiness Evaluation (CREVAL) method, which is focused on higher headquarters such as corps and divisions. To determine what a better solution is for the SAF, it was necessary to study in depth and examine different examples to establish results of the different training cycles.

The third step of this methodology was to review the differences produced by different training cycles and the reasons behind them. This way the results produced by different armies, which conduct parts of the training cycle differently, can be examined. It provided some results with which the SAF multifunctional Bn training cycle could be improved.

The end result of this analysis was a set of recommendations to improve the SAF's multifunctional BG training cycle. It provided concrete solutions for certain challenges. This produced an optimum training cycle with a variation of possible sets of training events that make it better, possibly cheaper and more effective. This research methodology at the end presents a broad review of different factors affecting training cycles of the SAF, and US Army training cycles. A complete and thorough research of published publications and articles helped produce a comprehensive analysis, which provided several recommendations for improvement.

2 ANALYSIS

The first glance at the doctrine and documentation review in chapter two reveals that it is obvious that U.S. Army doctrine is much more prescriptive than SAF doctrine. This is understandable, since U.S. Army has significantly more resources and can afford more of them being dedicated for doctrine development. Another argument is also that the U.S. Army has much more experience in training a professional force, with the best evaluation – combat, which forces militaries to train better. The SAF on the other hand cannot afford a robust TRADOC element. It has had a professional force for only a good decade, and combat experience is very limited. Part of the SAF doctrine relies on the NATO alliance doctrine.

2.1 Assigning Mission and METL

The basis of the whole Bn training cycle is development of the mission statement. According to the SAF Manual for education and training, unit training has to be aligned with mission, METL and operational training cycle. For the battalion training cycle, the General Staff of the SAF is responsible for mission, organization and training standards according to the battalion Battle Group Directive. In the same above-mentioned directive, there are basically two missions: one is an "independent, self-sufficient, purposed built capability, which conducts joint combat of all the branches in full-spectrum operations for a certain period, and is capable of integration in the higher unit within the Alliance", and the other (which is stated in Annex A of the same document), is national defence within the Alliance. This could easily be confused with the mission statement. However, it is just an extract of the SAF Doctrine (the highest doctrinal document of the SAF). The same directive also states that the mission will be provided by the SAF General Staff.

On the other hand, the U.S. Army uses three kinds of mission types, which allow training to focus on certain areas and can be used simultaneously for one unit. First of all, there is the core mission, which guides the overall training or the unit's primary task. The next one is the training mission, which guides short-term training; and there is the deployment mission, which is obviously used as guidance while training for deployment. They are all scoped by higher headquarters one level up, but are normally prepared by the unit itself. The core mission statement is used as an overarching statement. It provides a broad focus for training and is based upon the unit design. It is important to stress that units are equipped, organized and skilled to provide capability for the entire army. For example, an infantry unit is primarily built for offensive, defensive and stability operations. So, normally, its mission would be to conduct decisive action as part of the land force operations to win the nation's war. The units could also change their mission from one phase to another, and thereby focus their training on certain areas. For example, in the first phase, units could focus on offense, while in the next on defence. According to the focus of the training, units could also have temporary short-term missions. Tasks or capabilities for a certain type of the unit can be found in the CATS. There is a long list of tasks, and since all of the tasks cannot be performed by every unit, the army uses METL to focus the training.

While SAF units have great flexibility with assigning METL to certain units, the U.S. Army has developed METL all the way from BDE down to the company level. Before 2005, U.S. Army units could develop their own METLs according to the mission, but that caused issues with tracking readiness and the use of different resources. Therefore, the U.S. Army assigned METL tasks to BCTs. However, this proved so much better that the U.S. Army assigned METL tasks all the way down to the company level. Again, similar as with the mission, units could have three sets of METLs. The base one that supports the core mission is the core METL (CMETL), which normally supports overall training. When a certain unit would be assigned with a concrete deployment, that unit could shift its training with a new METL, called the deployment METL (DMETL).

BN METL	A/B/C Company METL
Conduct Mission Command (ART 5.0)	Conduct Mission Command (ART 5.0)
Conduct an Attack (07-6-1092)	Conduct an Attack (07-TS-2112)
Conduct a Defense (71-8-7222)	Conduct a Defense (07-TS-2113)
Conduct Area Security (07-6-1272)	Conduct Area Security (07-TS-2114)
Conduct Stability Operations (07-TS-1004)	Conduct Stability Operations (71-TS-2115)
HHC (Headquarters Co) METL	FSC (Forward Support Co) METL
Establish the Battalion Command Post (71-TS-1205)	Perform Company HQ Functions (T63-S-2098)
Execute the Operations Process (71-TS-1201)	Conduct Maintenance Platoon Operations (63-TS-3398)
Conduct PLT Zone Reconnaissance (17-TS-3103)	Conduct Distribution Platoon Operations (63-TS-3392)
Conduct PLT Screen (17-TS-3604)	Establish Unit Area (63-TS-2094)
Employ Fires (71-TS-1077)	Conduct Air Delivery Operations (63-TS-2096)
Conduct Medical PLT Operations (71-TS-2124)	
Conduct BN FM Retransmission Communication Support (71-TS-1211) Example of the U.S. Army infantry Bn METL (SAF examples are used and explained in text)	

The SAF Manual for education and training reads that the METL should support the war-time mission. When studying previous training cycles in the SAF, this was frequently not the case. For example, we can find tasks such as Humanitarian Assistance, which is obviously not a war-time mission. Another example is force protection. Even if it is a very important task that the unit has to perform, it is an activity in every unit, not a task, and as such it does not focus its training. On the other hand, warfighting tasks such as occupying an assembly area, alarming and movement, and tactical movement are basic and lower level tactical tasks and again do not scope the BG training which they should.

Even though the CREVAL determines the areas of evaluations, it cannot be confused or used as a METL, which should drive the training. The same goes for the ARTEPs in U.S. Army. ARTEPs too are not used as METLs, even though their tasks can be used for evaluation purposes. In one of the examples of the training cycles in the SAF, CREVAL was used as a base for assigning METL. It is clear that the unit did not train according to their METL, but according to the evaluation, which is wrong. One of the examples of the METL is Plan and Conduct education, training, and exercises. This is obviously what a unit has to do, but it is not guiding or focusing training in any direction or area.

“Resources cannot limit the METL,” says the same manual. Even though this is annoying to every commander, units should conduct battle-focused training and the higher unit should assign resources. It is hard nowadays to follow this training principle, but it is important that commanders do not hinder their unit’s training. Resources are critical; they should not be in question. The SAF should estimate how much money is spent for the training cycle, and that amount should be provided for every Bn in the training cycle. This principle can be used as an argument to get the needed resources and conduct training.

Another important METL fact is that a unit’s METL has to be aligned with the higher unit’s METL. This sometimes causes problems in the SAF, since the BDEs normally do not participate as part of the training cycles, and their METL focuses on their peacetime mission, which is again wrong according to the doctrine. Nowadays, the SAF BCT headquarters assumes an “admin” role. They focus on day-to-day business, and training is their last concern. Excuses, such as that they have to write reports for higher; that they do not have time to deploy out to the field, since they have to deal with regular day-to-day business, are obviously shallow. If they were deployed in the field for exercises they would be able to perform their core job, and reports and day-to-day business would disappear, or those that are necessary would be done in the field since they would have more time. So it is important to stress that not only admin but also training of the higher HQ of the BG, should be conducted. At the end of the day, the superior commander is the one that signs and approves the METL for a subordinate unit. In this case, the BCT commander has to make sure that the BCT and BG METL are aligned.

Even though the SAF has no aircraft to deploy soldiers with parachutes or helicopters to conduct airborne operations, units like to assign such tasks to their METLs. In U.S. Army, this is impossible, since tasks and METLs follow the organization and Table of Organization and Equipment) TOE. So, if you do not have that equipment you cannot have that task. On the other hand, the SAF also does not have an establishment to train instructors, which would then train units. Again, equipment is completely different if you are jumping from an aircraft or marching or using an APC on the battle field. It is interesting that the SAF realized that our helmets were not suited for parachute jumps, since that was not the requirement when the SAF ordered them. So, how can one of the METL tasks be air assault, if the SAF does not have this ability, equipment or transport aircraft? On the other hand, it is important to stress that this kind of operation also changes the whole concept of the unit; support has to be air dropped too and logistical supplies as well.

A lot of times, the SAF battalion training cycles forget to establish a METL for the headquarters. Even though company units are the focus of the training and the battle, headquarters elements also have to have METLs that will focus their training. In this case, mission command or command and control would be one of the main tasks for headquarters. Integrating all the elements of the unit, not just companies, but combat support elements and service support elements as well must be a key function of the training cycle.

METL is just another step in the training development. It should be followed by supporting tasks development, battle drills that support collective tasks, crew drills and individual skills. This together with other trainings such as shooting, key leader training and others should develop a unit training plan, which is basically a training calendar. In the SAF, developing the METL is the last step when developing collective training; it should be followed by development of supporting tasks, battle drills, crew drills, and individual training.

According to this analysis SAF should prescribe METL not just down to companies as the U.S. Army does, but all the way down to platoons, since platoons are elements of the BG. This should be done by the General Staff, since the BG is the SAF primary manoeuvre capability and not the BCT. The SAF BCT has to be part of the Bn training cycle, even if the other two battalions and other support elements are not fully capable. It is still necessary to develop BCT capabilities especially within BCT headquarters, since they became "admin" instead of fighting headquarters, because the BCT may be called to support a national defence mission.

2.2 Developing Unit training Plan

When mission and METL are assigned to specific units, it is time to develop Unit Training Plan (UTP). UTP will include cascade key training events, mainly including tactical training and shooting activities. Other training events such as key-leader development, staff rides, NCO time are part of the training as well. Units will produce a long-term plan, but the focus with all the details will be for the next quarter. As soon as the brief to the superior commander is done and he approves the training calendar, it is time for the execution phase.

The handbook for training headquarters and units in the SAF does not prescribe; it only recommends roughly how the training should be conducted. Since it is only a recommendation, the majority of the units will not follow it; they will produce their own training cycle, which causes confusion. Additionally, the BCT HQ and the General Staff as superior authorities do not have an oversight of how the training is conducted. The end result is training, and the use of resources is not very efficient. Even though we have a simulation centre and a CTC, they are rarely part of the training cycle, and even when they are, it is more individual effort than a part of the concept (see Picure 1, p. 113).

When analysing two SAF Bn BG cycles and comparing them to U.S. Army, it is clear that one cycle is very different from another. This is a proof that there are no major prescribed directions on how to conduct the SAF Bn BG training cycle, what the key events are and how to progress from one level of collective training to another. It is also obvious that the amount of time spent in the field as one of the metrics, differs from one to another. It is impossible to train a SAF battalion to a standard, if during one of the cycles, the unit spent only 16 days in the field, not to mention missing the entire virtual and gaming environment in addition to all the training in the field.

Another important thing within the training cycle is the progression of the training. As we can see with the U.S. Army, it is clear that a unit first has to conduct a Tactical Exercise without Troops (TEWT), followed or concurrent with the virtual or gaming example, which saves resources. When this is satisfactory, a unit progresses to Situational Training Exercise (STX), which includes environments designed for a specific event or task, and can be repeated multiple times, as long as the unit does not feel confident with the achieved training standards. Only then a unit is prepared should it conduct a Field Training Exercise (FTX), where they combine all the events in ongoing “Force on force” exercise. For headquarter elements, it is important to practice their procedures before going out in the field. Command Post Exercises (CPXs) are a great tool to drill staff procedures. Only when a unit has mastered their staff procedures, they can command and control subordinate units on the ground. In addition to a CPX, as we can see from the table, there are Communication Exercises (COMEX) and Fire Coordination Exercises (FCX). First is making sure that units are proficient in using their signal procedures and equipment, and the other one that units know how to best utilize their fire support assets.

Live Fire Exercises (LFXs) are important part of the collective training, besides being the culmination of the training; they assure self-confidence in the troops. They are progressive from individual all the way to company, sometimes even battalion level training. Important part of the LFX is also integration of the combat support elements. It is important for combat troops and combat support troops to develop training where they combine skills of combat troops, with the skills of other supporting troops. The synchronization of different levels of combat support to the smaller unit on the ground is one of the goals.

But the most important element when creating a training calendar is an integration and synchronization of all the training within one unit and with available supporting units. First planers have to take into consideration that training just one unit after another, without other supporting players is a wasted training opportunity. It is important to integrate combat units and support units, since they will be in battle together. First are the units within the same battalion, such as manoeuvre companies and reconnaissance platoon, maintenance platoon, etc. We have to use one event to combine and train as much as we can different units. When this is done, planers should also think about who are the available combat multipliers, such as field artillery and close air support. This adds a new dimension to the training, even though it is sometimes challenging, it is not just worth trying but almost obligatory. The last part of the training plan is the synchronization of all the training troops, into a single training event or exercise.

2.3 Training Evaluation

The U.S. Army uses TO&Es for evaluating collective training as part of training development. They are prescribed for each task and are part of the Combined Arms Training Strategy (CATS). The U.S. Army has formal and informal evaluations, which can be done internally or externally. It is known that training without evaluation is a wasted training. The primary evaluators for their units are their commanders. However, formal evaluation is done two levels down (company commander evaluates squads). The next level of evaluation includes the CTC, National training Centre (NTC) or Joint military training Centre (JMRC). These are not the establishments to train troops, but to evaluate them with Mission Readiness Exercises (MRX).

According to AR 350-1, commanders must use Army Training Management System (ATMS), Digital Training Management System (DTMS) continuously to determine the unit's proficiency in mission essential tasks. A unit is proficient when it performs to standard all the METs with supporting tasks evaluated by Standards in Training Commission (STRAC)/CATS. The evaluation encompasses mission command, live fire, and technical/tactical manoeuvre.

Another part of the units' evaluations are the Certification Training Exercises (CTE). These are formal evaluations conducted by external evaluators, normally in the CTCs. According to JBLM Reg. 350-1, all brigade combat teams and multifunctional brigades are required to conduct a CTE before entering the available phase of the ARFORGEN cycle (Department of the Army, Headquarters, I CORPS, *Leader development and Training management*, (Washington, 2013), 5-1)In order to do this, CTCs will be utilized with Warfighter Exercises (WFX) as their (BCTs) CTE.

Similar to the U.S. Army doctrine, the SAF doctrine also assigns responsibility to commanders. It is their final say to confirm whether a unit is trained or untrained according to its mission and METL. Again, the SAF has the same types of evaluations which are formal or informal, and internal or external. Another important document in the SAF that specifies the evaluation of the Bn BG, is the Bn BG Directive from 2015. It specifically specifies that SAF will use NATO prescribed Combat Readiness Evaluation (CREVAL) for BG evaluations. The SAF has therefore officially prescribed BG evaluations. However, the evaluations of companies and subordinate combat support and service support elements are not prescribed. CTC uses Army Training and Evaluation Program (ARTEPs) as a tool for evaluations, which is considered as detailed enough to state that a unit is trained (T) or untrained (U), since CREVAL is a more administrative "Check-the-block"-type evaluation. It is necessary to prescribe the lower part of the evaluation as well; it should not be left up to the individual evaluator.

As we can see, all three main parts of the evaluations have space for SAF BG improvements. First there is assigning proper mission and METL, even though the SAF uses similar principals, the outcomes can be very different from those in the U.S. Army. Then, there is the design of the training calendar or the UTP. Two major improvements should include the progression of the training with key events, and integration of combat support and service support in the training cycle. The last part of the analysis focused on the evaluation. Here, CREVAL is again prescribed, the attaining of training standards in subordinate units is left up to commanders.

Conclusion and recommendations

The mission drives focused training together with METL. It is impossible to be trained in all AUTL tasks for the infantry battalion, and there is also no need to be; not to mention the limitations of time and resources. That is why militaries came up with the concept of focused training. Since the "mission command" approach to training is new, together with a professional force, SAF is looking for other perspectives in order to improve their own training. Since the U.S. Army has a lot of experience and resources, the author used their approach to conduct training within the infantry battalion and BCT as a comparative model.

The first step of every unit training is the assigning of a mission and METL development. Sometimes, this is confusing in the SAF, since the units use mission where it should not be used, and, where it should be used, it is used incorrectly. In order to clarify this confusion, it is thus necessary to distinguish between core mission, training mission and deployment mission. The core mission is used for every unit no matter if they train for deployment or they just perform day-to-day duties. The units that are in any kind of training cycle can use a training mission, and those who are getting ready to deploy, can use a deployment mission focusing their training on the area where they are going to be deployed.

An METL focuses training in even more detail than the mission. It focuses their training tasks into five areas according to the TO&E. There can be again different sets of METLs, such as core METL or key tasks, training METL and deployment METL. This would prevent confusion of what is the day-to-day METL or key task, and what is their training METL, which could also be deployment METL. However, the main part of METL development is not the METL itself; it is the tasks that should be developed in order to support the METL. In the SAF, those supporting tasks are often not developed at all; especially regarding headquarters and staff METL. Supporting tasks should further be supported by other collective tasks that support main tasks. These should further be supported by battle drills at different levels, and crew drills whenever we are talking about combat vehicles or weapon systems. In the end, all of these tasks should be supported by individual skills and training, which all together assure that a unit performs to standard. So, in order to understand and develop training programs according to the concept that we adopted, the SAF should train its personnel within career courses and develop detailed guidance on how to develop training calendars.

The mission and METL are useless or at least limited if units do not have a proper training plan or calendar. With a detailed guidance on how to develop training from individual, crew, battle drill, and collective training, the substance (what to train) should be resolved. The next step would be putting the whole training package into the unit training plan or calendar. It is important to stress that the progression of training, especially collective training, is the key. The SAF should prescribe key events within the training plan and those should be logically followed step by step.

The SAF should improve collective training management and execution in order to use resources more efficiently. The TEWT is the basic step in collective training. It is a waste of resources if a battalion goes out in the field when the key leaders are not on the same page. They need to be aligned with each other's training goals horizontally and vertically. Even though the SAF has some of the virtual/gaming/constructive possibilities, units rarely use them. The next phase of the training cycle should be the STX, training events designed for a special task to be conducted. When all the collective tasks are mastered with STXs, then it is time for FTXs. Those should be used to assist the commanders to be able to find shortfalls and focus on them in this phase. LFX are conducted concurrently with all the collective training at various levels (individual up to battalion). When all the technical and tactical knowledge is gained, units should be focusing on integrating the training for the whole Bn BG. Again, before they go out in the field, a CPX should be the first step to synchronize units with the battalion HQ. Only when this is complete, should the battalion conduct an FTX.

There are also other types of exercises which assist units in maintaining and training without using a great amount of limited resources. Each unit should conduct a COMEX during the training cycle and later when the unit is in the available phase, to maintain its readiness. Another type of battalion training is an FCX, which makes sure that the battalion-level fire support is synchronized and used properly. Each unit should also conduct an FCX during the training cycle and in the available phase to maintain readiness.

With these directed key training events it would also be easy to assign and track the required resources. It would define minimum days to spend in the field and also how much finance is needed to conduct training. As for the field training, U.S. Army battalion commanders estimated at one of the symposiums that 30 days of uninterrupted training is a minimum requirement for every battalion collective training. On the other hand, it would make training more efficient, since it would not allow units to conduct battalion or company FTXs, if they had not conducted TEWT, STX, and possibly virtual training, before any FTX. It would also minimize communications issues in the field by using a COMEX and fire coordination confusion with an FCX.

Training of the headquarters is often neglected, since HQs are dealing with admin issues while manoeuvre units are conducting training in the field. By directing that battalion and also BCT HQs conduct at least a CPX and possibly a Staff Exercise (STAFFEX) prior to an FTX, it would again minimize HQ issues and synchronize staff procedures before deploying in the field with the whole battalion This kind of training using their METL, should focus battalion HQ training and their efforts to achieve proficiency together with manoeuvre units. The TEWT, COMEX and FCX are primary concerns of the battalion HQ, in addition to the CPX, and STAFFEX mentioned above. The SAF BG HQ should also consider other types of HQ training, such as logistical exercises (LOGEX) and deployment exercises (DEPEX), since this is the highest level HQ that will be deployed by the SAF.

The SAF should improve the integration and synchronization of combat support and service support unit training with manoeuvre unit training. The main part of developing an effective and efficient training cycle for the SAF multifunctional BG, is integration and synchronization of combat support and service support units. Since the SAF multifunctional BG consists of manoeuvre units along with other vital support, it is crucial for supporting elements and manoeuvre units to understand and train together, so each understands what the other elements can bring to the fight. So whenever a combat unit is scheduled to perform training in the field, there should be an opportunity to consider what kind of support element could be included in their training event. Integration and synchronization will also save a lot of money. Instead of conducting five separated training events, units should integrate their training goals in one training event. This would greatly improve training efficiency.

The SAF should improve the evaluation of training events. It is a waste of training if there is no evaluation to determine if the training has been done to standard or if the training objectives have been met. Evaluations could be done in the form of AARs or formal external evaluation, but everyone will benefit more from training if an analysis of some kind is conducted. As for the evaluation of SAF multifunctional BG, the NATO methodology using CREVAL has been adopted since the SAF is part of NATO. The one part that the SAF has to improve with CREVAL is how to implement it; to determine who is responsible and who will help them out. For example, the CTC is responsible for evaluation, and since they do not have enough resources and manpower, it is necessary to reinforce them with observer controllers. These additional observer controllers should be from a unit that has done a CREVAL before. Neither should the CREVAL just be a "check-the-block" thing, but should include a quality approach. That means that it is not enough for a unit to have an SOP for operating in an NBC environment; the evaluation should also determine if it works, i.e. if the units are able to conduct operations in an NBC environment.

Since the CREVAL is more of a HQ evaluation methodology, training units also have to be proficient in tactical and technical skills and procedures. Since there is nothing to officially say that certain units are capable of performing METL tasks, it is necessary to prescribe an evaluation procedure which certifies platoons and companies as well. The SAF uses ARTEPS for evaluation of units up to the battalion level, but they are not officially prescribed for the Bn. Although only commanders can say at the end of the day, if a unit is ready or not, sometimes in the case of the SAF this is not enough. As discussed above regarding the mission and METL relationship with the development of the unit training plan, ARTEPS should also be prescribed for certification or evaluation of subordinate units. Directed use of CREVAL for the battalion HQ, and ARTEPs for the platoons and companies, would result in more realistic evaluation and consequently a more effective training.

This research not only gave the author an insight into different approaches to training cycles, but also offers a number of improvements for SAF training. The SAF will never have resources to develop a training management system such as the U.S. Army has; however, these findings should serve as the basis for a new SAF training directive or at least training guidance for a new multifunctional Bn Directive. NATO provides strategic and operational guidance, technical execution of training is up to the member countries. If the SAF adopts the recommendations from this research, it can greatly improve the efficiency and effectiveness of training for its multifunctional Bn BG which will allow the SAF to better fulfil its responsibilities.

Bibliography

SAF Doctrinal documents

1. *Furlan, B., Petelin, D., Toic, B. and Kastelic, G. (2006). Vojaška doktrina (Military Doctrine). Ljubljana. Slovenija. Defensor, Schwarz.*
2. *Slovenska vojska, Poveljstvo za doktrino, razvoj, izobrazevanje in usposabljanje (SAF Doctrine, Development, Education and Training Command). (2011). Priročnik za usposabljanje poveljstev in enot Slovenske vojske (Handbook for training SAF headquarters and units). Ljubljana. Slovenija. Poveljstvo za doktrino, razvoj, izobrazevanje in usposabljanje (SAF Doctrine, Development, Education and Training Command).*
3. *Slovenska vojska, Generalštab (Slovenian Armed Forces, General Staff). (2015). Direktiva bataljonske bojne skupine (Batalion Battle Group directive). Ljubljana. Slovenija. Slovenska vojska (Slovenian Armed Forces).*
4. *Slovenska vojska, Generalštab (Slovenian Armed Forces, General Staff). (2014). Organizacijski ukaz za izvedbo vaje preverjanja MOTBBSK (Operational order for conducting assessment exercise for Bn BG). Ljubljana. Slovenija. Slovenska vojska (Slovenian Armed Forces).*

5. *Slovenska vojska, Generalštab (Slovenian Armed Forces, General Staff). (2015). Usmeritve za izdelavo aktov bataljonske bojne skupine (Guidance for development of Bn TF acts).Ljubljana. Slovenija. Slovenska vojska (Slovenian Armed Forces).*
6. *Slovenska vojska, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (SAF Doctrine, Development, Education and Training Command). (2011). Merila, metode in postopki za ocenjevanje poveljstev in enot pehotni motorizirani bataljon (Army Training Evaluation programmess). Ljubljana. Slovenija. Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (SAF Doctrine, Development, Education and Training Command).*
7. *Slovenska vojska, Generalštab (Slovenian Armed Forces, General Staff). (2012). Direktiva za organiziranje vojaškega izobraževanja in usposabljanja v Slovenski vojski (Directive for organization of military education and training in the SAF). Ljubljana. Slovenija. Slovenska vojska, Generalštab (Slovenian Armed Forces, General Staff).*
8. *Republika Slovenija, Ministrstvo za obrambo (Republic of Slovenia, Ministry of Defence). (2006). Navodilo za usposabljanje poveljstev in enot Slovenske vojske (Manual for training SAF headquarters and units). Ljubljana. Slovenija. Republika Slovenija, Ministrstvo za obrambo (Republic of Slovenia, Ministry of Defence).*

NATO publications

9. *NATO, Supreme Headquarters allied powers Europe. (2014). Volume VII - combat readiness evaluation of land Hqs and units (CREVAL). Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*
10. *NATO, Supreme Headquarters allied powers Europe. (2016). BI-SC capability codes and capability statements. Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*
11. *NATO, Supreme Headquarters allied powers Europe. (2007). NATO task list (NTL). Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*
12. *NATO, Supreme Headquarters allied powers Europe. (2011). BI-SC agreed capability codes and capability statements. Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*
13. *NATO, Supreme Headquarters allied powers Europe. (2013). Bi-SC 75-7 education and individual training directive (E&ITD). Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*
14. *NATO, Supreme Headquarters allied powers Europe. (2013). Bi-SC Collective training And Exercise Directive (CT&ED) 075-003. Mons. Belgium. NATO, Supreme Headquarters allied powers Europe.*

U.S. Doctrinal Documents

15. *Headquarters, Department of the Army. (2004). Mission Training plan for the Staff of the Brigade Combat Team. Washington. DC. Headquarters, Department of the Army.*
16. *Department of the Navy. Headquarters United States Marine Corps. (2013). Infantry Training and Readiness Manual. Washington. DC. Department of the Navy. Headquarters United States Marine Corps.*
17. *Department of the Army, Headquarters, I CORPS. (2013). Leader Development and Training Management. Washington, DC. Department of the Army, Headquarters, I CORPS.*
18. *Department of the Navy. Headquarters United States Marine Corps. (2012). Marine Expeditionary unit (MEU) Training and Readiness (T&R) manual. Washington. DC. Department of the Navy. Headquarters United States Marine Corps.*
19. *Headquarters, Department of the Army. (2012). Training Units and Developing Leaders. Washington. DC. Headquarters, Department of the Army.*

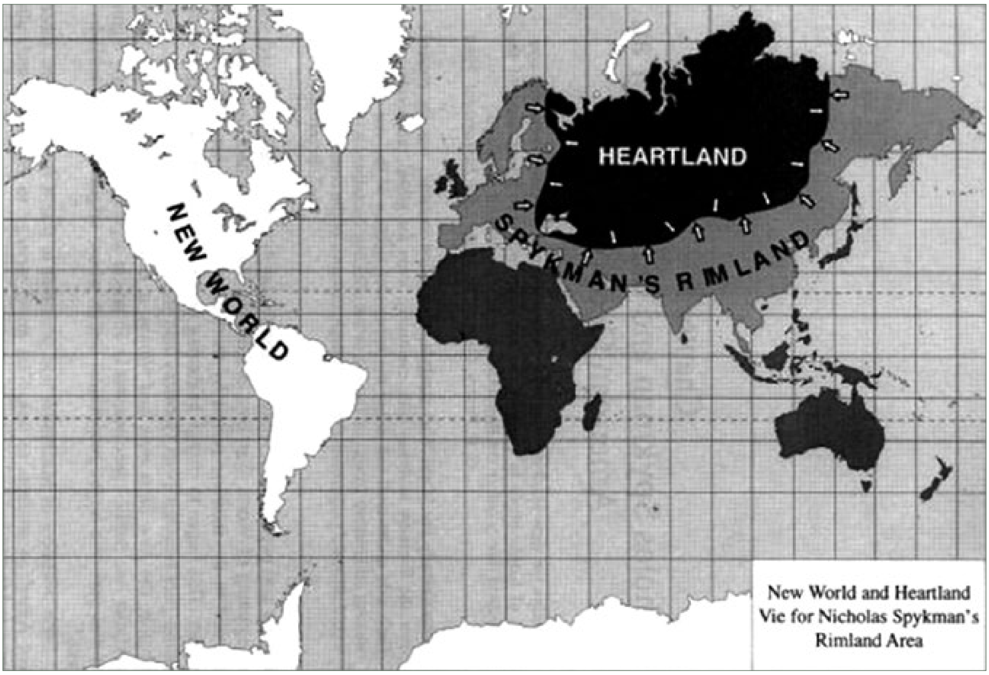
20. *Headquarters, Department of the Army. (2011). Army Force Generation. Washington. DC. Headquarters, Department of the Army.*
21. *Headquarters, Department of the Army. (2003). Battle focused Training. Washington. DC. Headquarters, Department of the Army.*
22. *Headquarters, Department of the Army. (2004).Training Guide for developing collective training products. Fort Monroe. Virginia. Headquarters, Department of the Army.*
23. *Headquarters, Department of the Army. (2012) ADP 7-0 Training Units and Developing Leaders. Washington. DC. Headquarters, Department of the Army.*
24. *Headquarters, Department of the Army. (2012) ADRP 7-0 Training Units and Developing Leaders. Washington. DC. Headquarters, Department of the Army.*
25. *Department of the Army. (2014). CASCOM Training Development Policy. Fort Lee. Virginia. Department of the Army.*
26. *Headquarters, Department of the Army. (2014). Army Training and Leader Development. Washington. DC. Headquarters, Department of the Army.*

U.S. Articles and Publications

27. *Little. M. (2012) The Eight Step Training Model. Washington. DC. Superintendent of Documents, United States Army. http://www.dtic.mil/dtic/tr/fulltext/u2/a560296.pdf (May 26, 2016)*
28. *Doughtery. W.J., Dennis. M.B. (2010) Combiend Arms Training and New, Emerging Theories on Training. Fort Benning. Infantry Magazine. http://www.benning.army.mil/infantry/magazine/issues/2010/SEP-OCT/pdfs/SEP-OCT_10.pdf (May 26, 2016)*
29. *Hernandez. B.P., (2010) A New Battalion Commander's Command Focus Thought the Applications of LLOs. Fort Benning. Infantry Magazine. http://www.benning.army.mil/infantry/magazine/issues/2010/JAN-APR/pdfs/JAN-APR2010.pdf (May 26, 2016)*
30. *Benifeld. P. (2009) Planning, Challenging, Realistic Training at the Battalion Level. Fort Benning. Infrantry Magazine. http://www.benning.army.mil/infantry/magazine/issues/2009/JUL/pdfs/JUL2009.pdf (May 26, 2016)*
31. *Fenzel. M.R., Morgan S. (2014). Harmony in Battle. Military Review. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140228_art013.pdf (May 26, 2016)*
32. *Brendan McBreen B. (2001). One Year to Train. http://www.2ndbn5thmar.com/TrainM/oyttmcbreen2001.pdf (May 26, 2016)*

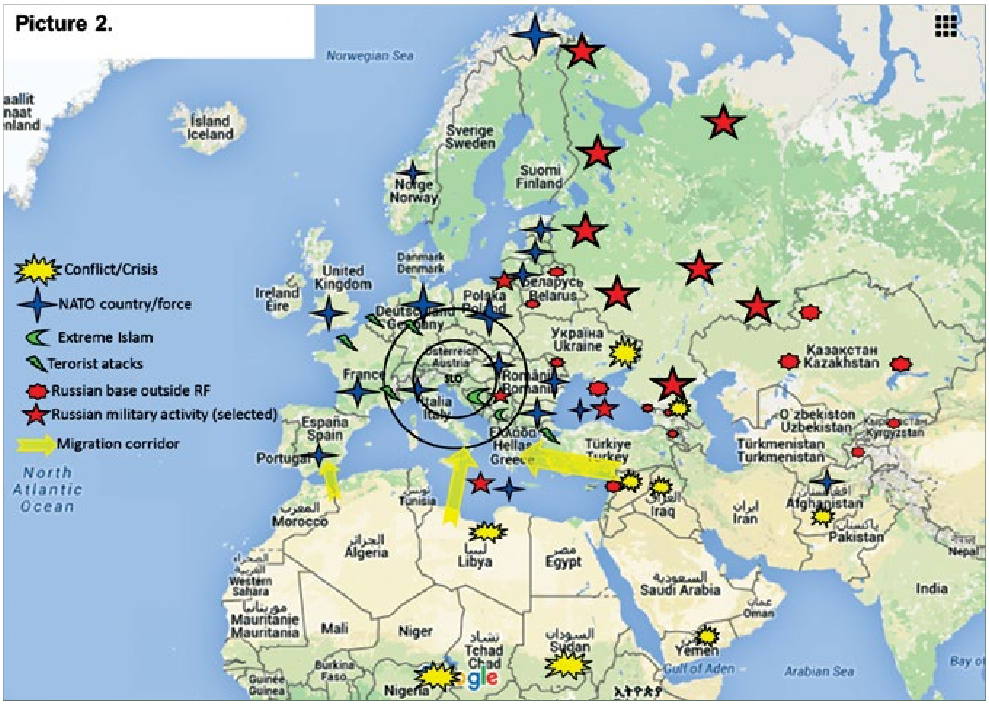
Slikovno gradivo

Photos


HEARTLAND
NEW WORLD
SPYKMAN'S RIMLAND
New World and Heartland Vie for Nicholas Spykman's Rimland Area

Slika 1: Svet po Spykmanu
Vir: Polelle, Raising Cartographic Consciousness, str. 118.

Picture 1: World according to Spyman
Source: Polelle, Raising Cartographic Consciousness, p. 118.

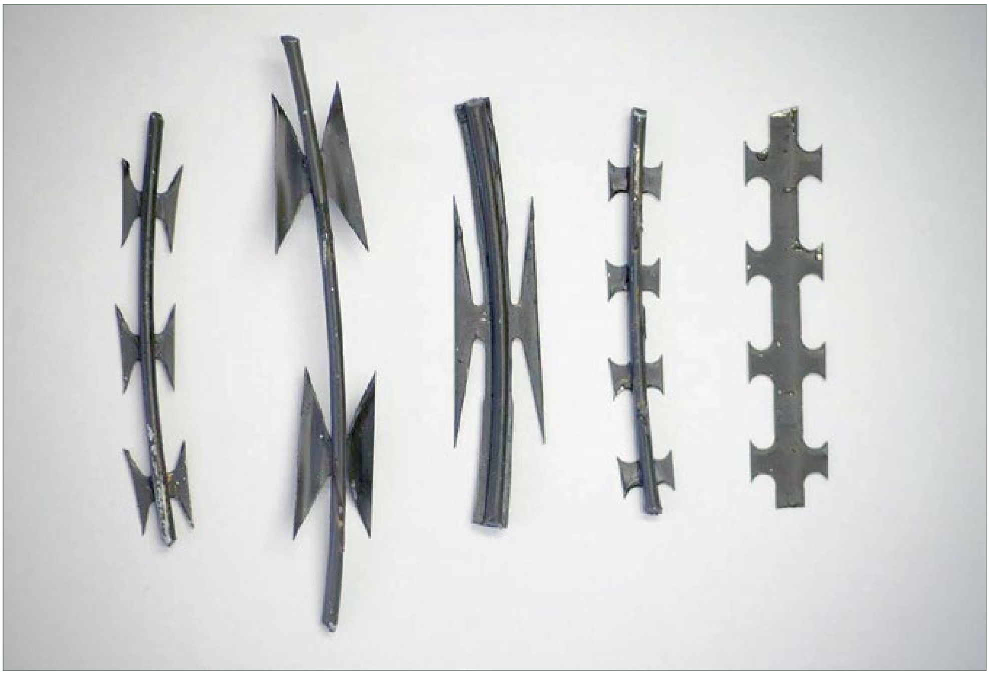


Slika 2: Geopolitični položaj Slovenije v luči sedanjih varnostnih tveganj
Vir: izdelal avtor.

Picture 2: Geopolitical position of Slovenia in light of existing security threats
Source: Made by author

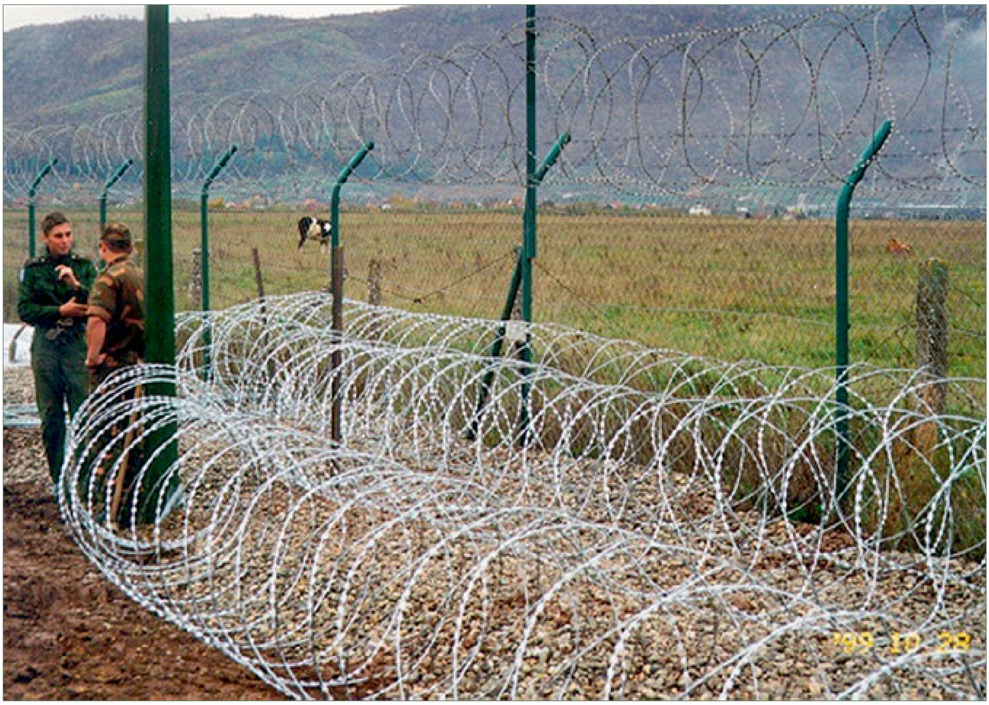
Slika 1: Žice z različnimi vrstami rezil **Vir:** osebni arhiv avtorjev.

Figure 1: Wires with different types of cutting edges **Source:** Photograph taken by the authors



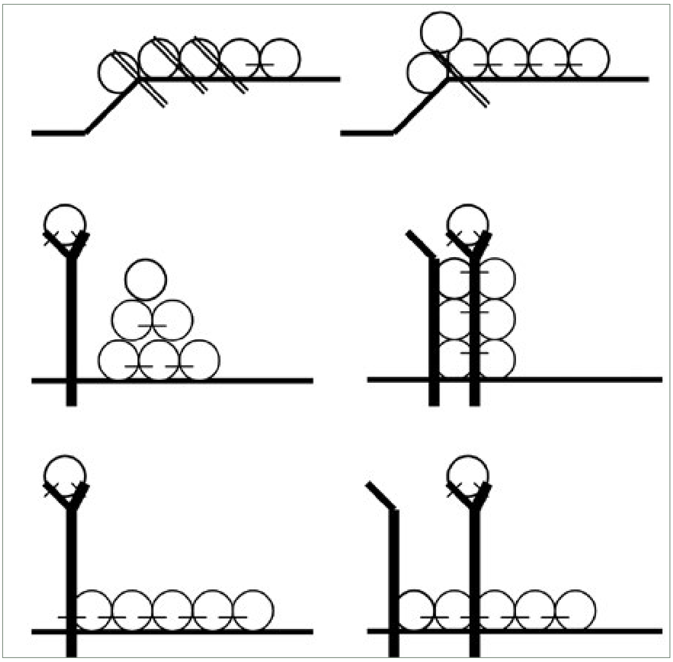
Slika 2: Ograja, ki varuje vojaško bazo **Vir:** osebni arhiv avtorjev.

Figure 2: Fence protecting a military camp **Source:** Photograph taken by the authors



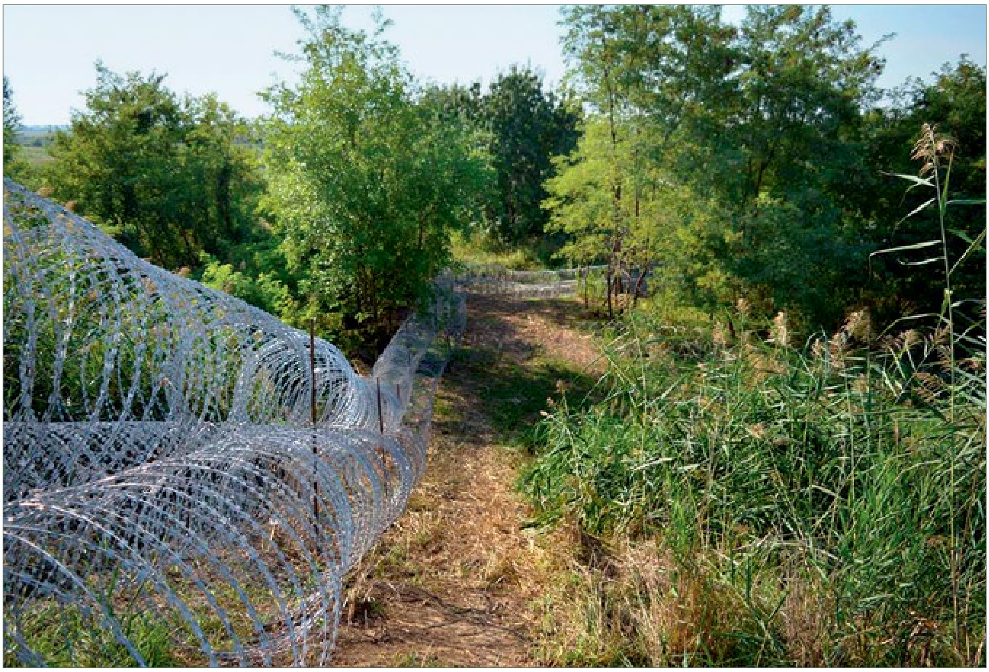
Slika 3: Različne vrste uporabe zvitkov žice **Vir:** osebni arhiv avtorjev.

Figure 3: Different utilizations of wire rolls **Source:** Photograph taken by the authors



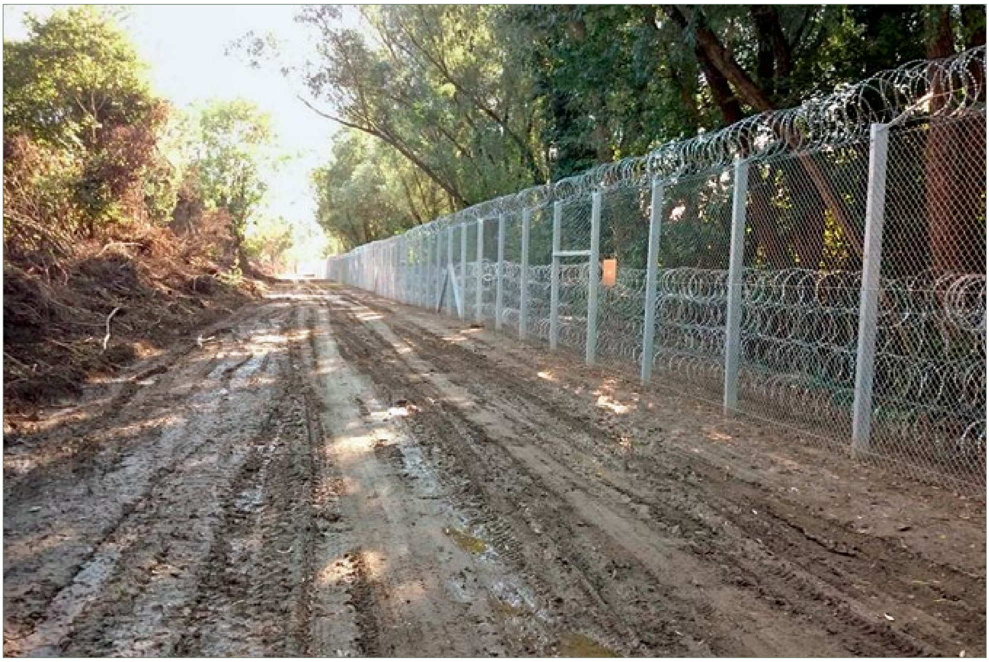
Slika 4: Prvi primer začasne ograje **Vir:** osebni arhiv avtorjev.

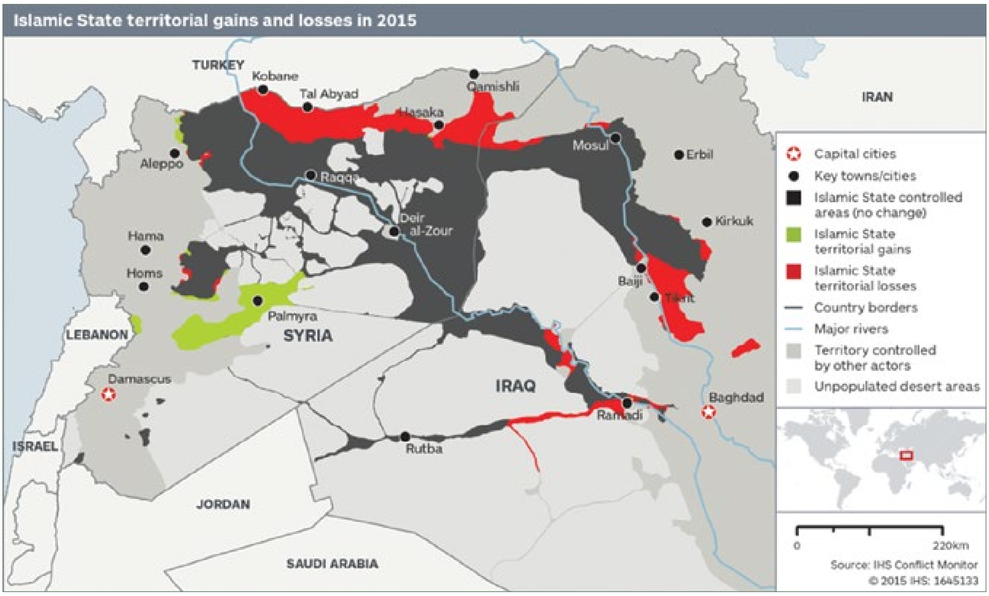
Figure 4: The first type of temporary fence **Source:** Photograph taken by the authors



Slika 5: Ograja, kot je trenutno postavljena vzdolž meje
Vir: osebni arhiv avtorjev.

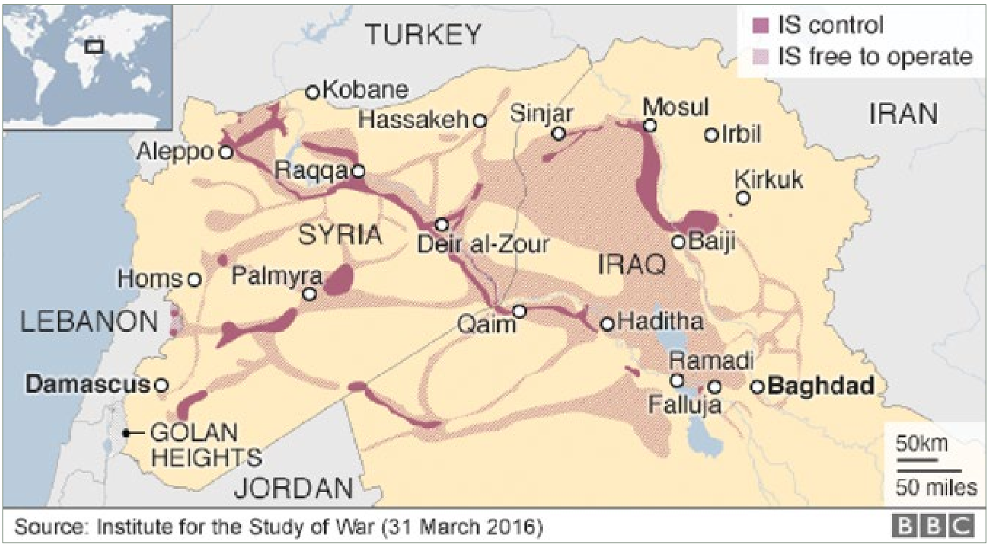
Figure 5: The presently existing fence along the border
Source: Photograph taken by the authors





Slika 1: Ozemlja, ki jih je Islamska država pridobila in izgubila leta 2015
Vir: http://static3.businessinsider.com/image/map.png, nazadnje obiskano 21. 8. 2016.

Figure 1: Islamic State territorial gains and losses in 2015
Source: http://static3.businessinsider.com/image/map.png, last visited 21 Aug 2016.



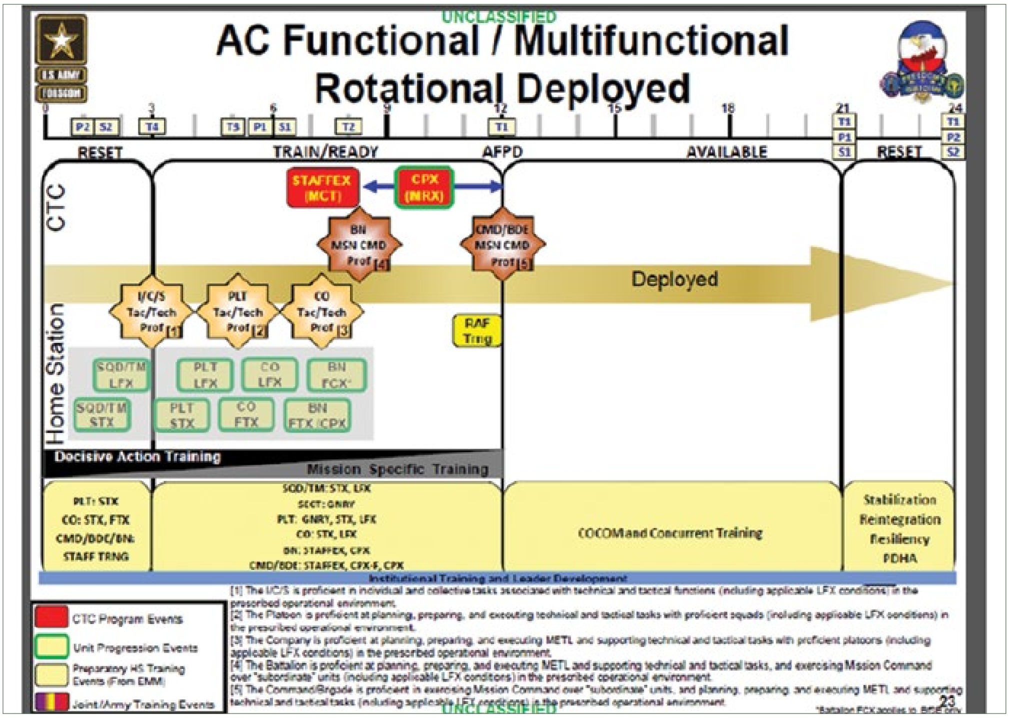
Source: Institute for the Study of War (31 March 2016)

Slika 2: Ozemlja, ki jih je Islamska država izgubila leta 2016
Vir: Institute for Study of war (31. 3. 2016), nazadnje obiskano 21. 8. 2016.

Figure 2: Islamic State territorial losses in 2016.
Source: Institute for Study of war (31. March 2016). Last visited 21 Aug 2016

Slika 1: Glavna usposabljanja pripradnikov stalne sestave (I/C/S-individualno/skupno/oddelčno, PLT-vod, CO-četa, BN-bataljon)

Figure 1: Main training events of the Active Component Training Cycle (I/C/S-Individual/Collective/Squad, PLT-Platoon, CO Company, BN-Battalion)



UNCLASSIFIED

AC Functional / Multifunctional Rotational Deployed

🟥 CTC Program Events

🟩 Unit Progression Events

▨ Preparatory HS Training Events (From EMM)

▨ Joint/Army Training Events

[1] The I/C/S is proficient in individual and collective tasks associated with technical and tactical functions (including applicable LFX conditions) in the prescribed operational environment.

[2] The Platoon is proficient at planning, preparing, and executing technical and tactical tasks with proficient squads (including applicable LFX conditions) in the prescribed operational environment.

[3] The Company is proficient at planning, preparing, and executing METL and supporting technical and tactical tasks with proficient platoons (including applicable LFX conditions) in the prescribed operational environment.

[4] The Battalion is proficient at planning, preparing, and executing METL and supporting technical and tactical tasks, and exercising Mission Command over "subordinate" units (including applicable LFX conditions) in the prescribed operational environment.

[5] The Command/Brigade is proficient in exercising Mission Command over "subordinate" units, and planning, preparing, and executing METL and supporting technical and tactical tasks (including applicable LFX conditions) in the prescribed operational environment.

*Battalion FCX applies to BDE only

23

UNCLASSIFIED

Avtorji

Authors

Viktor Potočnik

Major mag. Viktor Potočnik je v Slovenski vojski zaposlen od leta 2001. Opravljal je naloge poveljnika motoriziranega voda, minometne čete in motorizirane čete v mednarodnih operacijah in na misijah ter načelnika S-3 pehotne brigade Slovenske vojske. Udeležil se je treh mirovnih operacij in misij, opravil je več izobraževanj in usposabljanj v tujini, predvsem za ognjeno podporo. Leta 2011 je končal višje štabno šolanje na CGSC v bazi Fort Leavenworth v ZDA in pridobil naziv Master of Military Arts and Science. Trenutno dela v oddelku J-5 na Generalštabu Slovenske vojske.

Major Viktor Potočnik, MSc, *has worked in the SAF since 2001. So far, he has performed duties of a Motorised Platoon Commander, Mortar Company and Motorised Company Commander in international operations and missions, and Chief, S-3 in SAF Infantry Brigade. He has been deployed to three operations and missions, and has attended several education and training programmes abroad, mainly in the field of fire support. In 2011, he completed Senior Staff Course at CGSC, Fort Leavenworth, USA and obtained the title Master of Military Arts and Science. Currently, he works in J-5 at SAF General Staff.*

Staša Novak

Mag. Staša Novak je diplomirala iz politologije, smer mednarodni odnosi, na Fakulteti za družbene vede v Ljubljani. Magistrirala je iz mednarodnega prava na Pravni fakulteti v Mariboru ter iz mednarodne politike na Centre Européen de Recherches Internationales et Stratégiques (CERIS) v sodelovanju z Collège d'Etudes Interdisciplinaires univerze Paris Sud. Novembra 2006 se je zaposlila na Ministrstvu za obrambo Republike Slovenije, v Direktoratu za obrambno politiko. Od leta 2012 je pomočnica svetovalca za obrambne zadeve pri Stalni delegaciji Republike Slovenije pri Natu v Bruslju.

Staša Novak, MSc, *has a bachelor's degree in Political Science– International Relations from the Faculty of Social Sciences in Ljubljana. She holds a Master of Science degree in the field of International Law from the Faculty of Law in Maribor, Executive Master's degree in International Politics organised by the Centre Européen de Recherches Internationales et Stratégiques (CERIS) in partnership with the Collège d'Etudes Interdisciplinaires of the University of Paris Sud. Her career started at the Defence Policy Directorate of the Ministry of Defence in November 2006. She has been assistant defence advisor at the Permanent Delegation of the Republic of Slovenia to NATO in Brussels since 2012.*

József Padányi

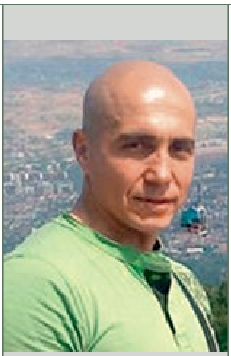
Brigadir dr. József Padányi je prorektor za znanost na Nacionalni univerzi za javne službe in univerzitetni profesor. V vojski se je zaposlil leta 1981. Dve leti je sodeloval v mirovni misiji v BiH. Doktoriral je leta 1995, leta 2008 pa je pridobil naziv doktor Madžarske akademije znanosti. Je avtor osmih knjig, petnajstih poglavij in okrog 120 znanstvenih prispevkov. Raziskuje in predava na področjih civilno-vojaškega sodelovanja, inženirske podpore, pomoči ob nesrečah ter varnostnih vprašanj zaradi podnebnih sprememb. Pod njegovim mentorstvom je doktoriralo pet študentov.

Brigadier General József Padányi, PhD, *is the Vice-Chancellor for Science at the National University of Public Service and a university professor. He entered the military in 1981. He spent two years in Bosnia and Herzegovina as peacekeeper. He obtained his PhD in Military Science in 1995, and earned the title 'Doctor of Hungarian Academy of Sciences' in 2008. He has written eight books, fifteen book chapters, a total of 120 scientific works. He conducts research and teaches courses in civil-military cooperation, engineer support, disaster-relief operations and security issues of climate change. Five students accomplished their PhD programmes under his supervision.*

László Földi

Podpolkovnik dr. László Földi je univerzitetni raziskovalec na področju kemije in se je v vojski zaposlil leta 1990 kot častnik za JRKBO. Od leta 1999 je univerzitetni predavatelj. Doktoriral je leta 2003. Trenutno je docent na Fakulteti za vojaške vede in usposabljanje častnikov Nacionalne univerze za javni sektor ter načelnik podskupine za JRKB-obrambo. Je vodilni član doktorske šole za vojaško tehnologijo in vodja raziskovalnega področja vojaške okoljske varnosti. Na strokovnem področju se posveča kemičnim bojnim sredstvom, strupenim industrijskim materialom, okoljski varnosti in obvladovanju nesreč.

Lieutenant Colonel László Földi, PhD, *holds a university degree of researcher chemist and joined the Army as NBC officer in 1990. Since 1999, he has been a university lecturer. He obtained his PhD in 2003. Currently, he is Associate Professor at the Faculty of Military Sciences and Officer Training of the National University of Public Service, and chief of the NBC defence subgroup. He is a leading member of the PhD School of Military Technology and head of the "military environmental security" research area. His main areas of expertise include chemical warfare agents, toxic industrial materials, environmental security, disaster management.*



Metodi Hadji-Janev

Dr. Metodi Hadji-Janev je izredni profesor prava na vojaški akademiji General Mihailo Apostolski v Skopju Univerze Goce Delcev v Stipu. Diplomiral je na makedonski vojaški akademiji in končal Air Command and Staff College v ZDA. Magistriral in doktoriral je iz prava na Pravni fakulteti Justinian-I v Skopju. Zaposlen je kot prodekan za izobraževanje in raziskovanje na vojaški akademiji in gostujoči profesor na podiplomskem programu Pravne fakultete Justinian-I Univerze Sv. Cirila in Metoda v Skopju.

Metodi Hadji-Janev, PhD, *is an associate professor of Law at the Military Academy General Mihailo Apostolski" – Skopje, a unit of University "GoceDelcev" in Stip, Macedonia. He is a graduate of the Macedonian Military Academy and the United States Air Command and Staff College. He also holds MA and PhD degrees in Law from the Law Faculty "Justinian-I" in Skopje, Macedonia. Dr Hadji-Janev serves as a Vice Dean for education and Research at the Military academy and a Visiting professor of postgraduate studies at the Law faculty "Justinian-I", University "St. Cyril and Metodij" in Skopje.*

Marija Jankuloska

Mag. Marija Jankuloska je diplomirala na Pravni fakulteti Justinian-I Univerze Sv. Cirila in Metoda v Skopju. Na isti univerzi je tudi magistrirala iz mednarodnega prava in mednarodnih odnosov. Trenutno je dejavna članica makedonskega združenja evropskih študentov prava in makedonskega Evroatlantskega sveta. Sodelovala je na številnih usposabljanjih, seminarjih in konferencah na temo kibernetske varnosti, terorizma, prava in tehnologije. Pri svojem raziskovanju se posveča mednarodnemu javnemu pravu, mednarodnim odnosom, človekovim pravicam in varnosti ter evroatlantskim integracijam.

Marija Jankuloska, MSc, *is a graduate at the Faculty of Law "Justinian-I" at the University of St. Cyril and Methodius in Skopje. She holds a masters degree in International Law and International Relations from the same University. She is currently an active member of European Law Students Association of Macedonia (ELSA) and Euro-Atlantic Council of Macedonia and has attended numerous trainings, seminars and conferences concerning cyber security, terrorism, law and technology. Her research interests are at the intersection of public international law, international relations, human rights and security and Euro-Atlantic structures.*

József Kis-Benedek

Polkovnik dr. József Kis-Benedek je častni profesor, ki je večino svoje kariere delal na področju vojaške obveščevalne dejavnosti. Doktoriral je iz vojaške znanosti. Njegova zadnja vojaška dolžnost je bila namestnik direktorja produkcije vojaške obveščevalne službe. Kot obrambni ataše je 10 let služboval v tujini. Predava na različnih fakultetah na Madžarskem. Njegova raziskovalna področja so Bližnji vzhod, terorizem, obveščevalna dejavnost in krizni menedžment.

Col. József Kis-Benedek, PhD*, is an honorary professor with a background in military intelligence. He holds a PhD degree in Military Science. His last military position was Deputy Director of production at the Military Intelligence Office. He served abroad as a defence attaché for 10 years. Today he gives lectures at many universities in Hungary. His areas of research are the Middle East, terrorism, intelligence and crisis management.*

Aleš Avsec

Major mag. Aleš Avsec je v Slovenski vojski zaposlen od leta 1996. Opravljal je naloge poveljnika oddelka, poveljnika voda, poveljnika motorizirane čete, na Šoli za častnike predaval osnove poveljevanja in taktiko. Sodeloval je v mednarodnih operacijah Isafa in Kforja ter bil načelnik S-3 motoriziranega bataljona. Leta 2004 je končal Royal Military Academy Sandhurst v Veliki Britaniji, 2008 štabno šolanje v ZDA in 2016 višje štabno šolanje na Command and General Staff Course v Fort Leavenworthu v ZDA, kjer je pridobil naziv Master of Military Arts and Science.

Major Aleš Avsec, MSc, *has been employed in the Slovenian Armed Forces since 1996. Previously, he has worked as squad commander, platoon commander and motorized company commander. At Officer Candidate School, he has given lectures on Commanding Basics and Tactics. He has been deployed in ISAF and KFOR international operations, and was Chief of S-3 Division in a Motorised Battalion. In 2004, he graduated from the Royal Military Academy, UK. In 2008, he completed Staff Course in the US and, in 2016, the Senior Staff Course at Command and General Staff Course, Fort Leavenworth, USA. He earned the title of Master of Military Arts and Science.*

Navodila avtorjem za oblikovanje prispevkov

Instructions for the authors of papers

NAVODILA AVTORJEM ZA OBLIKOVANJE PRISPEVKOV ZA SODOBNE VOJAŠKE IZZIVE IN VOJAŠKOŠOLSKI ZBORNIK

Vsebinska navodila

Splošno

Sodobni vojaški izzivi je interdisciplinarna znanstveno-strokovna publikacija, ki objavlja prispevke o aktualnih temah, raziskavah, znanstvenih in strokovnih razpravah, tehničnih ali družboslovnih analizah z varnostnega, obrambnega in vojaškega področja.
Vojaškošolski zbornik je vojaškostrokovna in informativna publikacija, namenjena izobraževanju in obveščanju o dosežkih ter izkušnjah na področju vojaškega izobraževanja, usposabljanja in izpopolnjevanja.

Kaj objavljamo?
Objavljamo prispevke v slovenskem jeziku s povzetki, prevedenimi v angleški jezik, in po odločitvi uredniškega odbora prispevke v angleškem jeziku s povzetki, prevedenimi v slovenski jezik.
Objavljamo prispevke, ki še niso bili objavljeni ali poslani v objavo drugi reviji. Pisec je odgovoren za vse morebitne kršitve avtorskih pravic. Če je bil prispevek že natisnjen drugje, poslan v objavo ali predstavljen na strokovni konferenci, naj to avtor sporočiti uredniku in pridobiti soglasje založnika (če je treba) ter navesti razloge za ponovno objavo.

Tehnična navodila

Omejitve dolžine prispevkov

Prispevki naj obsegajo 16 strani oziroma 30.000 znakov s presledki (avtorska pola), izjemoma najmanj 8 strani oziroma 15.000 znakov ali največ 24 strani oziroma 45.000 znakov.

Recenzije

Prispevki se recenzirajo. Recenzija je anonimna. Glede na oceno recenzentov uredniški odbor ali urednik prispevek sprejme, če je treba, zahteva popravke ali ga zavrne. Pripombe recenzentov avtor vnese v prispevek.
Zaradi anonimnega recenzentskega postopka je treba prvo stran in vsebino oblikovati tako, da identiteta avtorja ni prepoznavna.
Avtor ob naslovu prispevka napiše, v katero kategorijo po njegovem mnenju in glede na klasifikacijo v COBISS spada njegov prispevek. Klasifikacija je dostopna na spletni strani revije in pri odgovornem uredniku. Končno klasifikacijo določi uredniški odbor.

Lektoriranje

Lektoriranje besedil zagotavlja OE, pristojna za založniško dejavnost. Lektorirana besedila se avtorizirajo.

Prevajanje

Prevajanje besedil ali povzetkov zagotavlja OE, pristojna za prevajalsko dejavnost oziroma Šola za tuje jezike Centra vojaških šol.

Navajanje avtorjev prispevka

Navajanje avtorjev je skrajno zgoraj, levo poravnano.
Primer:
Ime 1 Priimek 1,
Ime 2 Priimek 2
V opombi pod črto se za slovenske avtorje navede, iz katere ustanove prihajajo. Pri tujih avtorjih je treba navesti tudi ime države.

Naslov prispevka

Navedbi avtorjev sledi naslov prispevka. Črke v naslovu so velike 16 pik, natisnjene krepko, besedilo naslova pa poravnano na sredini.

Povzetek

Prispevku mora biti dodan povzetek, ki obsega največ 1200 znakov (20 vrstic). Povzetek naj na kratko opredeli temo prispevka, predvsem naj povzame rezultate in ugotovitve. Splošne ugotovitve in misli ne spadajo v povzetek, temveč v uvod.

Povzetek v angleščini

Avtorji morajo oddati tudi prevod povzetka v angleščino. Tudi za prevod povzetka velja omejitev do 1200 znakov (20 vrstic).

Ključne besede

Ključne besede (3-5, tudi v angleškem jeziku) naj bodo natisnjene krepko in z obojestransko poravnavo besedila.

Besedilo

Avtorji naj oddajo svoje prispevke na papirju formata A4, s presledkom med vrsticami 1,5 in velikostjo črk 12 pik Arial. Na zgornjem in spodnjem robu naj bo do besedila približno 3 cm, levi rob naj bo širok 2 cm, desni pa 4 cm. Na vsaki strani je tako približno 30 vrstic s približno 62 znaki. Besedilo naj bo obojestransko poravnano, brez umikov na začetku odstavka.

Kratka predstavitev avtorjev

Avtorji morajo pripraviti kratko predstavitev svojega strokovnega oziroma znanstvenega dela. Predstavitev naj ne presega 600 znakov (10 vrstic, 80 besed). Če je avtorjev več, se predstavi vsak posebej, čim bolj zgoščeno. Avtorji naj besedilo umestijo na konec prispevka po navedeni literaturi.

Strukturiranje besedila

Posamezna poglavja v besedilu naj bodo ločena s samostojnimi podnaslovi in ustrezno oštevilčena (členitev največ na 4 ravni).

Primer:
1 Uvod
2 Naslov poglavja (1. raven)
2.1 Podnaslov (2. raven)
2.1.1 Podnaslov (3. raven)
2.1.1.1 Podnaslov (4. raven)

Oblikovanje seznama literature

V seznamu literature je treba po abecednem redu navesti le avtorje, na katere se sklicujete v prispevku, celotna oznaka vira pa mora biti skladna s harvardskim načinom navajanja. Če je avtorjev več, navedemo vse, kot so navedeni na izvirnem delu.

Primeri:

a) knjiga:

Priimek, ime (lahko začetnica imena), letnica. *Naslov dela*. Kraj: Založba.

Na primer:Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

b) zbornik:

Samson, C., 1970. Problems of information studies in history. V S. Stone, ur. *Humanities information research*. Sheffield: CRUS, 1980, str./pp. 44–68. Pri posameznih člankih v zbornikih na koncu posameznega vira navedemo strani, na katerih je članek, na primer:

c) članek v reviji

Kolega, N., 2006. Slovenian coast sea flood risk. Acta geographica Slovenica. 46-2, str. 143–167.

Navajanje virov z interneta

Vse reference se začenjajo enako kot pri natisnjenih virih, le da običajnemu delu sledi še podatek o tem, kje na internetu je bil dokument dobljen in kdaj. Podatek o tem, kdaj je bil dokument dobljen, je pomemben zaradi pogostega spreminjanja www okolja.

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press, str. 45–100. http://www.mors.si/index.php?id=213, 17. 10. 2008.

Pri navajanju zanimivih internetnih naslovov v besedilu (ne gre za navajanje posebnega dokumenta) zadošča navedba naslova (http://www.vpvs.uni-lj.si). Posebna referenca na koncu besedila v tem primeru ni potrebna.

Sklicevanje na vire

Pri sklicevanju na vire med besedilom navedite le priimek prvega avtorja in letnico izdaje. *Primer:* … (Smith, 1997) …
Če dobesedno navajate del besedila, ga ustrezno označite z narekovaji, v oklepaju pa poleg avtorja in letnice navedite stran besedila, iz katerega ste navajali.
Primer: … (Smith, 1997, str. 15) …
Pri povzemanju drugega avtorja napišemo besedilo brez narekovajev, v oklepaju pa napišemo, da gre za povzeto besedilo. *Primer*: (po Smith, 1997, str. 15). Če avtorja navajamo v besedilu, v oklepaju navedemo samo letnico izida in stran (1997, str. 15).

Slike, diagrami in tabele

Slike, diagrami in tabele v prispevku naj bodo v posebej pripravljenih datotekah, ki omogočajo lektorske popravke. V besedilu mora biti jasno označeno mesto, kamor je treba vnesti sliko. Skupna dolžina prispevka ne sme preseči dane omejitve.
Če avtor iz tehničnih razlogov grafičnih dodatkov ne more oddati v elektronski obliki, je izjemoma sprejemljivo, da slike priloži besedilu. Avtor mora v tem primeru na zadnjo stran slike napisati zaporedno številko in naslov, v besedilu pa pustiti dovolj prostora zanjo. Prav tako mora biti besedilo opremljeno z naslovom in številčenjem slike. Diagrami se štejejo kot slike. Vse slike in tabele se številčijo. Številčenje poteka enotno in ni povezano s številčenjem poglavij. Naslov slike je naveden pod sliko, naslov tabele pa nad tabelo.
Navadno je v besedilu navedeno vsaj eno sklicevanje na sliko ali tabelo. Sklic na sliko ali tabelo je: … (slika 5) … (tabela 2) …

Primer slike:

Slika 5: Naslov slike

Primer tabele:

Tabela 2: Naslov tabele

Opombe pod črto

Številčenje opomb pod črto je neodvisno od strukture besedila in se v vsakem prispevku začne s številko 1. Posebej opozarjamo avtorje, da so opombe pod črto namenjene pojasnjevanju misli, zapisanih v besedilu, in ne navajanju literature.

Kratice

Kratice naj bodo dodane v oklepaju, ko se okrajšana beseda prvič uporabi, zato posebnih seznamov kratic ne dodajamo. Za kratico ali izraz v angleškem jeziku napišemo najprej slovensko ustreznico, v oklepaju pa angleški izvirnik in morebitno angleško kratico.

Format zapisa prispevka

Uredniški odbor sprejema prispevke, napisane z urejevalnikom besedil MS Word, izjemoma tudi v besedilnem zapisu (text only).

Naslov avtorja Prispevkom naj bosta dodana avtorjeva naslov in internetni naslov ali telefonska številka, na katerih bo dosegljiv uredniškemu odboru.

Kako poslati prispevek Na naslov uredništva ali članov uredniškega odbora je treba poslati tiskano in elektronsko različico prispevka.

Potrjevanje sprejetja prispevka Uredniški odbor avtorju pisno potrdi prejetje prispevka. Avtorjem, ki sporočijo tudi naslov svoje elektronske pošte, se potrditev pošlje po tej poti.

Korekture Avtor opravi korekture svojega prispevka v treh dneh.

Naslov uredniškega odbora

Ministrstvo za obrambo
Generalštab Slovenske vojske
Sodobni vojaški izzivi
Uredniški odbor
Vojkova cesta 55
1000 Ljubljana
Slovenija
Elektronski naslov
Odgovorna urednica:
liliana.brozic@mors.si

Prispevkov, ki ne bodo urejeni skladno s tem navodilom, uredniški odbor ne bo sprejemal.

INSTRUCTIONS FOR THE AUTHORS OF PAPERS FOR THE CONTEMPORARY MILITARY CHALLENGES AND THE MILITARY EDUCATION JOURNAL

Content-related instructions

General

The Contemporary Military Challenges is an interdisciplinary scientific expert magazine, which publishes papers on current topics, researches, scientific and expert discussions, technical or social sciences analysis from the field of security, defence and the military..
The Military Education Journal is a military professional and informative publication intended for education and informing on achievements and experiences in the field of military education, training and improvement.

What do we publish?
We publish papers in Slovene with abstracts translated into English. If so decided by the Editorial Board, we also publish papers in English with abstracts translated into Slovene.
We publish papers, which have not been previously published or sent to another magazine for publication. The author is held responsible for all possible copyright violations. If the paper has already been printed elsewhere, sent for publication or presented at an expert conference, the author must notify the editor, obtain the publisher's consent (if necessary) and indicate the reasons for republishing.

Technical instructions

Limitations regarding the length of the papers

The papers should consist of 16 typewritten double-spaced pages or 30,000 characters. At a minimum they should have 8 pages or 15,000 characters and at a maximum 24 pages or 45,000 characters.

Reviews

All papers are reviewed. The review is anonymous. With regard to the reviewer's assessment, the Editorial Board or the editor accepts the paper, demands modifications, if necessary, or rejects it. Upon receiving the reviewers' remarks, the author inserts them into the paper.

Due to an anonymous review process, the first page must be designed in the way that the author's identity cannot be recognized.

Next to the title, the author should indicate the category the paper belongs to according to him and according to the classification in the COBISS[1]. The classification is available on the magazine's internet page and at the responsible editor. The Editorial Board determines the final classification.

Proofreading

The organizational unit responsible for publishing provides the proofreading of the papers. The proofread papers have to be approved.

Translating

The translation of the papers or abstracts is provided by the organizational unit competent for translation or the School of Foreign Languages, Military Schools Centre.

Indicating the authors of the paper

The authors' name should be written in the upper left corner, aligned left.

Example:

Name 1 Surname 1,
Name 2 Surname 2,

In the footnote, Slovenian authors should indicate the institution they come from. Foreign authors should also indicate the name of the state they come from.

Title of the paper

The title of the paper is written below the listed authors. The font in the title is bold, size 16 points. The text of the title is centrally aligned.

Abstract

The paper should have an abstract of a maximum 1,200 characters (20 lines). The abstract should include a short presentation of the topic, particularly the results and the findings. General findings and reflections do not belong in the abstract, but rather in the introduction.

Abstract in English

The authors must also submit the translation of the abstract into English. The translation of the abstract is likewise limited to a maximum of 1,200 characters (20 lines).

Key words

Key words (3-5 also in the English language) should be bold with a justified text alignment.

Text

The authors should submit their papers on an A4 paper format, with 1.5 line spacing, fontArial size 12 points. At the upper and the bottom edge, there should be approx. 3 cm of space; the left margin should be 2 cm wide and the right margin 4 cm. Each page consists of approx. 30 lines with 62 characters. The text should have a justified alignment, without indents at the beginning of the paragraphs.

[1] *Co-operative Online Bibliographic System and Services*

A brief presentation of the authors

The authors should prepare a brief presentation of their expert or scientific work. The presentation should not exceed 600 characters (10 lines, 80 words). If there are several authors, each should be presented individually, as shortly and as comprehensively as possible. These texts should be placed at the end of the paper, after the cited literature.

Text structuring

Individual chapters should be separated with independent subtitles and adequately numbered.

Example:

1 Introduction
2 Title of the chapter (1st level)
2.1 Subtitle (2nd level)
2.1.1 Subtitle (3rd level)
2.1.1.1 Subtitle (4th level)

Referencing

In the bibliography, only the authors of references one refers to in the paper should be listed, in the alphabetical order. The entire reference has to be in compliance with the Harvard citing style.

Example:

Surname, name (can also be the initial of the name), year. *Title of the work.* Place. Publishing House.

Example:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

With certain papers published in journals, the author should indicate, at the end of each reference, a page on which the paper can be found.

Example:

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. pp. 45-100.

Referencing internet sources

All references start the same as the references for the printed sources, only that the usual part is followed by the information about the Internet page on which the document was found as well as the date on which it was found. The information about the time that the document was found on the Internet is important, because the WWW environment changes constantly.

Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. p. 45-100. http://www.mors.si/index.php?id=213, 17 October 2008.

When referencing interesting WWW pages in the text (not citing an individual document) it is enough to state only the Internet address (http://www.vpvs.uni-lj.si). A separate reference at the end of the text is therefore not necessary.

Citing

When citing sources in the text, indicate only the surname of the author and the year of publication. *Example:* ….. (Smith, 1997) …

When making a direct reference to a text, the cited part should be adequately marked with quotation marks and followed by the exact page of the text which the citing is taken from.

Example: ...(Smith, 1997, p.15) …

Figures, diagrams, tables

Figures, diagrams and tables in the paper should be prepared in separate files which allow for proofreading corrections. The place in the text where the picture should be inserted must be clearly indicated. The total length of the paper must not surpass the given limitation.

Should the author not be able to submit the graphical supplements in the electronic form due to technical reasons, it is exceptionally acceptable to enclose the figures to the text. In this case the author must write a sequence number and a title on the back of each picture and leave enough space in the text to include it. The text must likewise contain the title and the sequence number of the figure. Diagrams are considered figures.

All figures and tables are numbered. The numbering is not uniform and not linked with the numbering of the chapters. The title of the figure is stated beneath it and the title of the table is stated above it.

As a rule, the paper should include at least one reference to a figure or a table.. Reference to a figure or a table is: … (Figure 5) ……… (Table 2) ………

Example of a figure:

Figure 5: Title of the figure

Example of a table:

Table 2: Title of the table

Footnotes

The numbering of the footnotes is not related to the structure of the text and starts with number 1 in each paper. We want to stress that the aim of the footnotes is to explain the thoughts written in the text and not to reference literature.

Abbreviations

When used for the first time, the abbreviations in the text must be explained in parenthesis; therefore no additional list of abbreviations is needed. If the abbreviations or terms are written in English, the appropriate Slovenian term should be written along with the English original and possibly the English abbreviation in the parenthesis.

Format type of the paper

The Editorial Board accepts only the texts written with a MS Word text editor and only exceptionally those in the 'text only' format.

Author's address

Each paper should include the author's address, e-mail or a telephone number, so that the Editorial Board can reach him or her.

Sending the paper

A print or an electronic version of the paper should be sent to the address of the Editorial Board or the members of the Editorial Board.

Confirmation of the reception of the paper

The Editorial Board sends the author a written confirmation regarding the reception of the paper. The authors who also list their e-mails receive the confirmation via e-mail.

Corrections

The author makes corrections to the paper within three days.

Editorial Board address

Ministry of Defence
Slovenian Armed Forces
General Staff
Contemporary Military Challenges
Editorial Board
Vojkova cesta 55
1000 Ljubljana
Slovenia
Electronic address:
Editor in Chief:
liliana.brozic@mors.si

The Editorial Board will not accept papers, which will not be in compliance with the above instructions.

http://www.slovenskavojska.si/publikacije/sodobni-vojaski-izzivi/
http://www.slovenskavojska.si/en/publications/contemporary-military-challenges/

Sodobni vojaški izzivi – 18/št. 2

Vsebina

Liliana Brožič
UVODNIK: MEDNARODNA VARNOSTNA SKUPNOST NA RAZPOTJU
EDITORIAL: INTERNATIONAL SECURITY COMMUNITY AT THE CROSSROADS

Viktor Potočnik
ČETRTA GENERACIJA VOJSKOVANJA
Prvi del: GEOPOLITIČNI OKVIR SLOVENSKE VARNOSTI
FOURTH GENERATION WARFARE
Part 1: GEOPOLITICAL FRAMEWORK TO SLOVENIAN SECURITY

Staša Novak
NATO IN KIBERNETSKO ODVRAČANJE
NATO AND CYBER DETERRENCE

József Padányi
László Földi
IZKUŠNJE MADŽARSKIH OBRAMBNIH SIL, PRIDOBLJENE PRI RAZMESTITVI INŽENIRSKIH OVIR MED VSEEVROPSKO MIGRANTSKO KRIZO LETA 2015
LESSONS LEARNED FOR THE HUNGARIAN DEFENCE FORCES FROM THE DEPLOYMENT OF ENGINEER OBSTACLES DURING THE 2015 EUROPE-WIDE MASS-MIGRATION EMERGENCY

Metodi Hadji-Janev
Marija Jankuloska
IZZIVI UPORABE DRONOV V DRŽAVAH JUGOVZHODNE EVROPE
THE CHALLENGES OF DRONE USAGE BY SOUTHEAST EUROPEAN COUNTRIES

József Kis-Benedek
ISLAMSKA DRŽAVA IRAKA IN LEVANTA TER MEDNARODNI BOJ PROTI NJEJ
ISLAMIC STATE OF IRAQ AND THE LEVANT AND THE INTERNATIONAL FIGHT AGAINST IT

Aleš Avsec
CIKEL USPOSABLJANJA NAMENSKIH SIL BATALJONSKE BOJNE SKUPINE
BATTLE GROUP TRAINING CYCLE