

# COMPENDIUM 2015

RACVIAC - Centre for Security Cooperation  
Compendium 2015

October 2015  
© RACVIAC - Centre for Security Cooperation





Published by: RACVIAC - Centre for Security Cooperation  
Stari Hrast 53, Rakitje, HR - 10437 Bestovje  
Croatia  
Tel: +385 1 333 0 813  
Fax: +385 1 333 0 809  
E-mail: [infor@racviac.org](mailto:infor@racviac.org)

Senior Editor: RACVIAC Deputy Director - Brigadier General Zdravko Jakop, HR

Editorial Board: Public Affairs Officer - Capt Branko Lozančić, HR  
English Language Expert - Sanja Romić, HR



# COMPENDIUM 2015

**Disclaimer:**

Any views or opinions expressed in this Compendium are solely those of the authors and do not necessarily represent those of the RACVIAC - Centre for Security Cooperation, its staff, Member countries or other institutions and individuals taking part in activities at the RACVIAC - Centre for Security Cooperation.





## **Table of Contents:**

### **Introduction**

- 6 - Forward by RACVIAC Director Ambassador Branimir Mandić
- 7 - Introduction by RACVIAC Deputy Director Brigadier General Zdravko Jakop

### **Cooperative Security Environment With Special Focus on Arms Control**

- 11 - Vienna Document 2011 - The Geopolitical Aspects of the Treaty in Light of Recent Events,  
Laszlo Szabo PhD
- 20 - The Legal Aspects of the Vienna Document 2011,  
Tamás Lattmann PhD
- 28 - Defence, Public Interest and/or Consensus: Limitations and Possibilities,  
Stjepan Domjančić PhD
- 38 - Development Opportunities Regarding Human Protection Through the Triad  
“Human-clothing-Environment”,  
Dr. Daniela Zavec Pavlinić

### **Security Sector Reform**

- 45 - Integration of Military Education Systems in Civil Society,  
Dr. Jelena Juvan
- 49 - Private Military and Security Companies in the Global War on Terrorism,  
Robert Mikac PhD
- 55 - The Importance of Regional Cooperation in the Field of Military Education as  
Support to Confidence and Security Building Measures in SEE,  
Col Goran Dikić
- 59 - Europeanising the Initial Officers' Education: Some Challenges, Many  
Opportunities, Sylvain Paile-Calvo
- 64 - Future Perspectives of Military Education, 21ST Century Challenges Regional  
Aspect (SEE),  
Col Metodi Hadji-Janev

# COMPENDIUM 2015

- 70 - Transition of the Military Education System in Croatia,  
**Col Slobodan Čurčija, 1stLt Tina Orlović**
- 75 - Modelling the European Initial Officers' Education and Training Systems,  
**Sylvain Paile-Calvo**
- 81 - Civil-Military Relations and the Democratic Control of Armed Forces,  
**Dr. Anton Bebler**
- 86 - Flood Risk Management in Lower Austria,  
**Dipl.-Ing. Martin Angelmaier**
- 90 - The Position of the Female Service Members in the Slovenian Armed Forces,  
**Janja Vuga PhD, Ljubica Jelušič PhD**

## **International and Regional Cooperation with Focus on Euroatlantic Integration**

- 101 - Civil-Military Relations in the Protection and Rescue Field,  
**Col Slavko Angelevski PhD**
- 106 - Cyber Security Strategy as a "Must" for South-East European Countries,  
**Col Metodi Hadji-Janev**
- 112 - Building a Cyber-Resilient Society by Forging a Partnership in SEE: An Important Task for Future SEE Strategists,  
**Col Metodi Hadji-Janev**
- 120 - Technical Aspects of Resilience in Cyberspace with Emphasis on Water Supply Critical Information Infrastructure,  
**Mitko Bogdanoski, Marjan Bogdanoski, Zoran Angelov**
- 130 - Protecting Civilians from Activities Related to Cyber Conflict While Respecting the International Human Rights Law Principles,  
**Ljubica Pendaroska**
- 135 - International Law of State Responsibility: Unlawful Orchestration Versus the Omission of the Duty to Prevent the Unlawful Cyber Operation,  
**Andraz Kastelic**
- 140 - Contemporary Trends and Challenges in Cyber Security Legal, Operational and Technical Aspects,  
**Antun Matija Filipović**

# INTRODUCTION



## **Forward**

Dear readers,

It is with great pleasure that the RACVIAC - Centre for Security Cooperation publishes its first Compendium. The decision to publish the RACVIAC Compendium coincides with the celebration of the 15th anniversary of the foundation of the RACVIAC - Centre for Security Cooperation.

The Compendium represents a written history of topics and issues that were discussed during RACVIAC's activities and provides speakers and lecturers with a venue to leave a permanent record of their respective lectures given at RACVIAC.

Being an academic organization, RACVIAC encourages all lecturers and speakers to contribute to the Compendium when taking part in our activities, providing institutional memory and reference for the future.

I sincerely believe that the publishing of this first Compendium, and others in the future, will contribute to the RACVIAC mission of fostering dialogue and cooperation among the member countries and their partners.

RACVIAC Director

**Ambassador Branimir Mandić**

# COMPENDIUM 2015



## Introduction

Dear readers,

The first RACVIAC Compendium represents the fulfillment of an idea that has been on the table at the Centre for Security cooperation for a few years. Contributing to the academic dimension of the RACVIAC - Centre for Security Cooperation, its aim is to provide a tangible form of institutional memory that may be referred to in the future during the development and conduct of RACVIAC activities. It will also provide an insight into RACVIAC activity for readers that may not have had the opportunity to attend a given activity or may have an interest in a given subject matter.

During the development of the Compendium speakers and lecturers at RACVIAC activities were encouraged to provide written works that addressed the subject matter of their respective lectures. Although this first Compendium covers a period spanning more than the last year, it is the intention of RACVIAC to publish its Compendium annually.

The Compendium has been divided into three sections representing the pillars within the RACVIAC - Centre for Security Cooperation: Cooperative Security Environment with focus on arms control, Security Sector Reform, and International and Regional Cooperation with focus on Euroatlantic integration. Each article has been listed under the respective pillar that organized the activity in which the lecturer/speaker (author) participated.

It is my sincere hope that the RACVIAC Compendium will provide interesting reading for experts involved in security related issues throughout the region and that this Compendium will prove to be useful beyond the premises of the RACVIAC - Centre for Security Cooperation.

RACVIAC Deputy Director

**Brigadier General Zdravko Jakop**

A handwritten signature in blue ink, corresponding to Brigadier General Zdravko Jakop. The signature is stylized and cursive.





# COMPENDIUM 2015

## **Cooperative Security Environment With Special Focus on Arms Control**



## Vienna Document 2011 “Efforts to Revitalize Confidence and Security Building”

### *The geopolitical aspects of the Treaty in light of recent events*

Laszlo Szabo PhD

Let me start first with the geopolitics.<sup>1</sup> According to the classical geopolitical school a State is a territory with a frontier and a population that has the right to possess and use its own means of sustenance and, therefore, control its environment. According to his theory the State, much like any other living organism, is constantly changing and, therefore, its boundaries are flexible. Over a “lifetime” the State will expand its frontiers as its power increases, more often than not at the expense of the weakest countries.<sup>2</sup>

According to Classical Geopolitics Europe is a geographic region, a peninsula on the western extremity of the Eurasian “World Island”. Europe is aided by its internal geography in bouts of economic, political and military unification, which is traditionally followed by attempts to expand, usually imposed through force and often led by the German nation in Mitteleuropa. This unification and subsequent power-play expansion have projected into the Eurasian Heartland of Russia and along the Eurasian “Rimland” and its maritime trade routes and chokepoints.

According to one of the most famous geopolitical thinkers (Spykman's)<sup>3</sup> geostrategy highlights the need for the balance of power in Eurasia to be maintained so that the world balance of power would prevail - without any new hegemon rising in Eurasia and at least limiting the potential dominance of the Soviet Union and any other prospective superpowers such as China, Japan and India. The Rimland includes the countries of Western Europe, the Middle East, Persian Gulf, southwest Asia, China and the Far East up to far eastern Russia along the Bering Sea. Control of these maritime areas gives incredible power and influence to the possessor.


The Rimland of Classical Geopolitics is the Eurasian continental coastal land region, surrounding the Heartland and separating it from the Eurasian maritime highway, the encircling seas. Europe is “Rimland”, situated on the west coast of the “World Island” (Eurasia) on top of Africa, west of Russia, and on the sea lane of the great maritime highway from the Barents Sea to the far eastern Mediterranean Sea with two major sea gates or chokepoints, the Strait of Gibraltar and the Suez Canal.<sup>4</sup> Europe also borders Western Russian's sphere of influence which is often strategic in the power play between the European and Russian powers. Obviously, with such a geostrategic location, Europe has been of great importance across the panorama of history for empires and kingdoms, to project their influence afar.

<sup>1</sup> “Geopolitics,” Encyclopædia Britannica Online, 15 June 2010, <http://www.britannica.com/EBchecked/topic/229932/geopolitics>

<sup>2</sup> <http://energygeopolitics.com/about/classical-geopolitics-a-summary-of-key-thinkers-and-theories-from-the-classical-period-of-geopolitics/>.

<sup>3</sup> Nicholas Spykman, Geography and Foreign Policy, The American Political Science Review, Vol. 32, No. 2, April, 1938, p. 236.

<sup>4</sup> Halford J. Mackinder, The Geographical Pivot of History, The Geographical Journal, Vol. 23, No. 4, 1904, p. 422.



The first lesson of geopolitical theory is that location matters: The behavior of states is rooted in where they are; the idea of place is fundamental. Rivers are roads of commerce and cultural unifiers. Plains are easy for armies to march across and thus engender a sense of vulnerability - and a culture of pre-emption. These principles hold for all regions and Europe is no exception.

Most of the key events of world history occurred on the Eurasian landmass or one of its offshore islands. Much of the rest of the world at one time or another became the object of expansion, settlement and colonization by one or more Eurasian or offshore Eurasian powers. Mackinder<sup>5</sup> called Eurasia "the Great Continent." Brzezinski calls it "the mega-continent." Eurasia is the globe's largest landmass and contains most of the world's people and resources. Fortunately, the geopolitical region of Eurasia and its offshore islands has throughout history remained politically divided. Geopoliticians from Mackinder to Brzezinski repeatedly have stressed the importance of preventing a single power or alliance of powers from controlling the major power centers of Eurasia.

The period between the end of the nineteenth century and the end of the Second World War might be defined as the golden era of classical geopolitics both in terms of theory and practice. From the nineteenth century onwards, as the age of geographical discovery drew to a close and global political rivalry was on the rise all of the major rival powers-Great Britain, Federal Republic of Germany, Russia and the USA-had prominent geopolitical theorists who constructed theories to enhance or at least to preserve the power of their countries. These geopolitical theorists were both academics and statesmen and their theories were to a large extent adopted by the decision makers of their home states. Their theories thus played an important role in the relations among the great powers of the age.<sup>6</sup>

When Harry S. Truman became President of the United States, the Soviet Union was far from an enemy. It was a major wartime ally and his predecessor, Franklin Roosevelt, had the aim throughout the war to make the Soviets into peacetime allies too. The idea was to make the Soviet Union an integral part of the postwar world order. In the first days of Truman's administration this aim remained unchanged. However, the new president's inexperience with policy at this level caused the erstwhile vice-president, who had not been informed by Roosevelt of his plans, to adopt a crucial change of tone in his diplomacy toward the Soviet Union. Harriman informed the President that he thought the Soviets were pursuing two policies at the same time: "one, the policy of cooperation with the United States and Great Britain, and the other, the extension of Soviet control over neighboring states through unilateral action."<sup>7</sup>

Consequently, after the Second World War, two relatively coherent ideological blocs would fight each other for over forty years. This confrontation rapidly gave birth to a new concept: the Cold War. During this period, international political forces coalesced around the United States and the Soviet Union,

---

<sup>5</sup> Mackinder, - *The Geographical Pivot of History*, p. 395. No. 4, 1904.

<sup>6</sup> <http://etd.lib.metu.edu.tr/upload/12612289/index.pdf> - Semra Rana Gökmen, *Geopolitics and the Study of International Relations*, August 2010, p. 8

<sup>7</sup> Thomas W. Bottelier, *The Geopolitics of Containment - Reappraising American Foreign Policy During the Early Cold War, 1945-1953*; Master's Thesis, pp. 37-38.

# COMPENDIUM 2015

The American policy of containment<sup>8</sup> developed with remarkable speed in Europe as well. The European Recovery Program, usually referred to as the Marshall Plan, entered into force as a result of the Truman Doctrine. Turkey and Greece were aided financially to counter a possible Soviet influence. Finally, NATO was founded in 1949 as a 12 state military Alliance against the threat of Soviet aggression and eventually expanded to include 16 members.

The containment - according to the former US administration - meant the formation of political and military alliances, the deployment of U.S. air, land and naval forces at key points around

the globe, the buildup of conventional and nuclear armed forces and, on occasion, war.<sup>9</sup>

The concept of Europe that emerged following World War II was the mirror opposite of the older Europe. "Europe" now came to mean a peaceful entity that had overcome its nationalism. The idea of Europe was partly defense against its own past; it also was partly a contrivance designed to give Europe weight in the world. Caught between the United States and the Soviet Union, the fragmented countries of Europe had no weight. Europe needed to transcend nationalism if it were to engage in great power politics. This is the paradox that lies at the heart of Europe, and the underlying crisis within Europe today.

Geopolitics becomes popular during times of change, crisis and war. This was especially noticeable during the dissolution process of the Soviet Union at the end of the Cold War, through which the study of geopolitics came into vogue again after nearly half a century of neglect. During the storm caused by the winds of change at the dawn of the post-Cold War era, the scholars' appetite for geopolitics revived once again. Fukuyama announced the end of history and Huntington proclaimed the beginning of a clash of civilizations. As the World Island became an open space once again Zbigniew Brzezinski, drawing upon Mackinder's Heartland Theory, defined the new but old rules of the Grand Chessboard.<sup>10</sup> What the world or the new superpower needed was a new drama and new geopolitical theories to go along with it.

After the fall of the Berlin Wall the power vacuum created by the retreat of both superpowers suddenly laid the existing States and those that would soon become independent open to major changes in the distribution of power. This transformation of the international system, characterized by high volatility and global instability, made the international situation more complex and gave new impetus to geopolitical factors.


On the one hand, the new frontiers of the former Soviet space have revived ghosts from the past. Old ethnic antagonisms clashed with the mix of national identities imposed by those in power when the political space was reconfigured. On the other hand, some greedy political leaders, looking to expand their power, manipulated history by creating new cultural references in order to serve their ambitions.

---

<sup>8</sup> See more: Thomas W. Bottelier, *The Geopolitics of Containment Reappraising American Foreign Policy During the Early Cold War, 1945-1953*; Master's Thesis.

<sup>9</sup> George F. Kennan, one of the leading US diplomats on Russian affairs suggested the containment policy in his so-called 'Long Telegram' and the new government adopted as the cornerstone of a new U.S. policy toward Moscow. Later on he published his vision in an article in *Foreign Affairs* in July 1947.

<sup>10</sup> Brzezinski, Zbigniew, *The Grand Chessboard*, New York: Basic Books, 1997.



The United States' partial disengagement is allowing the Concert of Powers to return to Europe. The United States is attempting to reforge its most valuable military alliance, NATO, into a form more useful to its current foreign policy goals. For the Federal Republic of Germany that means being swept to the side while countries located further east, such as Hungary and Poland, which traditionally have fallen under the German sphere of influence, become more important and receptive to U.S. strategic doctrine. So, the Federal Republic of Germany, under Gerhard Schroeder, not only has skipped the step of challenging U.S. efforts within NATO but directly and publicly questioned the relevance of NATO itself.

As the U.S. hegemony declines, due to unsustainable debt and a consumer-based economy, the contingent outcome may shift towards American isolation and withdrawal from significant international engagement. This isolationist attitude would facilitate the potential rise of new civilization-based superpowers - an united German-led Europe, an Asian international conglomerate centered around Russia and China plus Iran heading a regional alliance of Islamist Pan Arabia. Spykman believed that the United States should focus its foreign policy efforts toward preventing a power or alliance of powers from organizing and uniting the resources of the Old World.<sup>11</sup>

**Washington is forcing its European allies to rethink their relationship with the United States - not as a group, but as individual nations.** This works to Washington's advantage, since it is much easier to manage allies - or opponents - bilaterally than to deal with them as a bloc. A geopolitically powerful European Union is not in the United States' fundamental interests, and Washington will look to exploit the current splits by nurturing relations with current EU states like the Kingdom of Spain and Kingdom of Denmark, as well as with candidate countries such as Poland. This process is a direct challenge to Europe's ambitions of forging a common foreign policy.

The world's only superpower, the United States, is not only present the way it is everywhere in the world, it is deeply involved in European institutions (NATO, OSCE) in ways that often make analysts define the United States as a European power. The United States supported the development of the EU as part of its own forward defence against the Soviet Union but also worried that the EU might become a challenger to US dominance of NATO.

The United States dominates the Western Hemisphere and participates in the power balance in every region of the Eurasian rimland. Whereas Great Britain once was the "holder" of the European balance of power, the United States is today the "holder" of the world balance of power. The United States is the only country capable of using its power to influence events in every part of the world.<sup>12</sup>

**Europe is at a major crossroads** in its evolution toward what integrationists believe can be a unified political and economic body, with power projection capabilities sufficient to challenge those of the United States. Closely related to the foreign policy challenge is Europe's military crisis. The massive gap in military capabilities between the continent and the United States is well-documented. A lack of military muscle sorely limits Europe's ability to project power -- and it particularly frustrates Paris, which sees Europe as its platform for military legitimacy.

---

<sup>11</sup> Francis P. Sempa, *Geopolitics - From the Cold War to the 21st Century*, Transaction Publisher, 2002, p. 94.

<sup>12</sup> Sempa, p.114.

# COMPENDIUM 2015

Eastern enlargement has more ambiguous effects. On the one hand, the growing of the EU is likely to mean that the Franco-German tandem, which has been the main home of this discourse, becomes less dominant simply because it becomes a smaller fraction of the whole. On the other hand, the project of enlargement reinforces the historic sense of the EU project, of what it has done to Western Europe and now is to do in Eastern Europe. How these two will balance out is hard to predict.

Europe's topography may allow a Berlin-dominated Brussels to rule Europe into one cohesive international super-state rather than becoming a fragmented collection of independent sovereign states, with each state acting on its own interests. In such a union the people, trade and militaries would be able to move across Europe relatively seamlessly and effortlessly. Consequently, when taken as a collective whole, Europe rivals the United States, with economic diversity, a larger, diverse manpower base (with a population of half a billion people) plus more gold reserves and a more trade driven economy (thanks largely to the Federal Republic of Germany) with the largest value of external trade in the world.<sup>13</sup>

The European peninsula, however, remains politically divided and militarily unable (or unwilling) to effectively counterbalance the reduced Russian military threat. The geopolitical imperative of preventing a single power or alliance of powers from dominating the Eurasian landmass is as valid today as it was before.<sup>14</sup>

The Federal Republic of Germany is Europe's typical "center", both geographically and economically and often politically, and these historical manifestations reveal that a powerful German nation tends to dominate Europe, whenever it has the power and opportunity to do so. Presently Europe is experiencing both integration and disintegration forces in economics and politics, which are critical in determining the region's geopolitical future. Current trends could be leading to a German-led superpower in the looming multi-polar world.<sup>15</sup> In this new world order there is the potential decline of the United States and the emergence of other new civilizational superpowers, such as Asia and Pan Arabia, both with nodes of power in the Eurasian Heartland, along the Eurasian Rimland and its encircling oceanic trade routes.

However, despite Germany's tremendous growth, the varying levels of economic development among EU members may prevent Europe from easily achieving its desired status as a future superpower through soft or amicable democratic processes. It is economically impossible to use one currency across states with multiple different economic development levels, since fiscal and monetary policy becomes ineffective when it is not responsive to the economic circumstances in each state. One size does not fit all.


The EU is dependent on Eurasia (and the North African nations bordering on its maritime territory) for energy resources. It imported 84% of its oil and 64% of its gas in 2009. In total Europe imports massive quantities of food, minerals, oil and natural gas. Even more specifically, 40% of European oil was imported from the Persian Gulf in the early 2000s, while it was reported in 2009 that 36% of European gas (through pipelines) and 31% of European oil and 30% of its coal were imported from Russia.

---

<sup>13</sup> Hripsime Nalbandyan, *Regional Security in the European Union*, Hussein Solomon (ed.) *Challenges to Global Security: Geopolitics and Power in an Age of Transition*, I.B. Tauris, 2008. pp. 155-157.

<sup>14</sup> Sempa, pp. 99-100.

<sup>15</sup> James Leigh - Scott Newman, *Contemporary Europe in Eurasian Geopolitics*, p.5.



Consequently, Europe could be almost entirely energy dependent on big rivals and threatening foes from across the Eurasian World Island Heartland and Rimland, thus weakening Europe's chances of dominating this super-continent.<sup>16</sup>

Europe is predominantly Christian. This could pit Christian Europe against the looming superpower civilizations of an Asian conglomerate and an Islamist alliance. If Russia and China conglomerate together to form the core of an international Asian superpower alliance, the EU would begin to feel increasingly vulnerable to amassing geopolitical power of a continental scale in potentially rival civilization blocs.

Russia is also evolving - both politically and strategically. The Russian empire has thus contracted and mellowed during this "time of troubles." Russia's military, however, still fields a powerful land army, a blue-ocean navy, a multi-tentacled intelligence and espionage apparatus and thousands of nuclear weapons and delivery systems.<sup>17</sup> Energy exports constitute the most substantial portion of this new world view. A new energy network to Asia is (belatedly) under construction in an effort to mitigate Russia's current dependence on European markets. Infrastructure shifts in the west are designed to minimize Russian dependence on any transit states. Another new policy is to dangle energy supplies in front of individual powers in an effort to take advantage of the lack of a common front in Europe. Incidentally, the Russian strategy of divide and conquer is remarkably similar to what the Americans have been doing in Eurasia for decades. Such Russian insinuations are not passing unnoticed. For example, the European Union fast-tracked Bulgarian and Romanian membership in part to lock down the Balkans. Now any Russian influence into the Balkans will need to circumvent the union geographically as well as politically.

The erosion of bipolarity, followed by the withdrawal of the Mediterranean Squadron of the former USSR and the dissolution of the Soviet and Yugoslav empires, has drastically changed the security environment and the balance of power in the Black Sea / Caspian Sea basins. New actors like the Ukraine, Georgia, Republic of Croatia, Bosnia and Herzegovina and others entered the Black Sea / Balkan scene after the break-up of the former USSR and Yugoslavia. Thus, the emergence of the Ukraine as an independent regional player has drastically changed the balance of power in the Black Sea region, which is characterised by the relationship within the triangle RussiaUkraineRepublic of Turkey.<sup>18</sup>

At the beginning of the 21th century, the State is still the main actor in the international system and retains its prerogatives on its own territory. The State is not passive. It adapts to new situations and competes in the economic race. In fact, the State's national security objectives - to gain control over territory and expand its sphere of influence - are no longer bound by military deployment; they are more complex and involve new considerations such as control of and access to scarce resources and the conquest of foreign markets with the geo-economic weapon.

---

<sup>16</sup> Tatiana Mitrova, *The Geopolitics of Natural Gas - The Geopolitics of Russian Natural Gas*, James A. Baker Institute for Public Policy, February 2014, pp. 6-11.

<sup>17</sup> Sempa, p. 95.

<sup>18</sup> Olga A. Vorkunova, *Regional Security in Russia and Near Abroad*, In.: Hussein Salomon (ed.) *Challenges to Global Security: Geopolitics and Power in an Age of Transition*, I.B. Tauris, 2008. pp.172-174.



# COMPENDIUM 2015

The end of the Cold War signaled the end of the old geopolitical world order and the beginning of a geopolitical transition period. Moreover, it was the beginning of new global rivalries jostling to gain world leadership, historically perceived as long cycles of world leadership. These rivalries have always formed attempts to create a new global system with a new rule and new distribution of power which in some geopolitical studies has been called a geopolitical world order. According to this view, immediately after the end of the Cold War era, the structure of the global system faced geopolitical disorder. It means that the global governing system broke down and changed the old order, while the new order had not yet been established. This uncertainty and geopolitical disorder, on the one hand, was the consequence of inefficiency of previous rules, institutions and ideas as well as current geopolitical codes to solve international problems. On the other hand, it warned of the necessity to redefine the geopolitical codes as the 'main building blocks of geopolitical world orders' based on new conditions, in particular, for great powers. In this respect, it was an attempt to impose geopolitical codes or a specific political agenda, associated with a particular culture, rule and ideas on other states, through either command power or co-optive power. This formed the beginning of a new type of rivalry amongst the great powers to forming a new structure of distribution of power around the world and eventually the reconstruction of geopolitical world order.

What is important here is that until that time, the United States, as the sole remaining power from the last world order, had not been able to impose its code on others. There were attempts by the US to promote its position in the international system on the one hand and regional disorders and resistances in different levels to accept US global desires on the other hand.


**Eastern Europe** has been considered a "crush zone" by political geographers for over a century and the region has been intimately connected with the geopolitical re-orderings of this century. Strenuous avoidance of geopolitical issues, including long-term relations with Russia, was notable during the NATO expansion debates. The stark contrast of "chaos" (Russia and its neighbours in the former Soviet Union) to "cosmos" (the European Union and three new central members of NATO) dominated the NATO enlargement debate. The end-consequence of recent NATO and U.S. foreign policy decisions will be a re-drawing of the geopolitical divide across Europe from the eastern Baltic to the Black Sea. The fear of being placed on the eastern side of this new "iron curtain" has caused many East European states to re-discover their "European" credentials and claim entry to the West. We have thus re-entered an era of geopolitical uncertainty as major domestic and international debates about issues such as NATO (North Atlantic Treaty Organisation) expansion and Russia's relations with her neighbours in the "Near Abroad" (countries formed after the dissolution of the republics of the former Soviet Union) draw pundits from all perspectives.<sup>19</sup>

The modern Balkans were formed through the disintegration of the Austrian and Ottoman Empires. Much of the variation among the successor states stems from differences between these two empires and the time and nature of their disintegration. Belgrade is a power centre with or without Yugoslavia. The *boundary* of the subcomplex has remained ambiguous: the region has two cores. The first one is the conflict constellation of Serbs, Croats and Bosnians; the second one around The Former Yugoslav Republic of Macedonia\* involving the Republic of Albania, Republic of Serbia, Republic of Bulgaria and Greece plus the Republic of Turkey. The key point here is the influence of outside powers on the break-up.

---

\* Turkey recognizes the Republic of Macedonia with its constitutional name.

<sup>19</sup> New Geopolitics of Central and Eastern Europe - Between European Union and United States, Stefan Batory Foundation, Warsaw 2005, pp.173-204.



The ongoing development of various information, biotechnological, robotic and other technologies has potentially enormous implications for world politics. While it is impossible to predict precisely how these and other technologies will mature in the coming decades, continuing rapid technological development appears certain. In the past, technological breakthroughs repeatedly have served to advance the interests of some powers and damage the prospects of others - indeed, the very concept of technological (as opposed to doctrinal) military revolutions implies that some polities are able to leverage technology to their advantage in warfare, a zero-sum endeavor. As in the past, one may expect that powers capable of effectively harnessing one or more key technologies will enjoy critical advantages over less-adaptable rivals. Geopolitics in the twenty-first century will also be affected by the ongoing struggle for control of outer space.<sup>20</sup> Space power enthusiasts, however, should avoid the temptation to oversell the strategic value of space power the way the early air power enthusiasts oversold air power's capabilities.

### **Confidence Building in the 21th Century**

The CSCE was a product of the Cold War. Its initial negotiations were launched in 1972 and ended in 1975, with the *Helsinki Final Act* establishing a basis for coexistence and eventually cooperative relations between the two superpowers and their respective treaty organizations of the period - NATO and WTO - plus the neutral and nonaligned of Europe. Over the years, there were numerous review and summit meetings of the CSCE, further refining and implementing provisions based on the three "baskets" of the Helsinki Final Act (1975).

But when the participants signed it, the geopolitical situation radically differed from the Cold War situation. The world changed so quickly that the participants were not able to adopt it to the new reality. But in the transition period during which Russia has been weak it was very useful for both sides. The objectives of the CFE Treaty are described in its mandate. They include strengthening stability and security in Europe through the creation of balanced conventional forces; establishing lower levels for conventional armaments and equipment; eliminating disparities prejudicial to stability and security; and, as a priority, precluding the capability for launching surprise attacks or large scale offensive operations.

All of these objectives could help to maintain the stability during the Cold War. It was a step on the way to create a secure Europe, and a small part of the Western strategy. We cannot forget the thesis that (1) arms control only serves as a part of any nation's overall national security strategy. As such it is a "method" to be used in seeking the overall "objective" of improved security. (2) "Arms control" differs significantly from "disarmament." "Arms control" is a policy method whereby states seek through negotiations to improve their security. It can not change ideologies and may not reduce hostilities. (3) Arms control is a political process and can not be divorced from other aspects of a nation's security or foreign policy. (4) Conventional arms control is more difficult and less likely to result in success than nuclear arms control.

After 1999 Russia suspended its participation in the treaty<sup>21</sup> and from (December 12) 2007 withdrew from the crucial data sharing and inspection function and from the restrictions on the number of

---

<sup>20</sup> Everett C. Dolman, "Geostrategy in the Space Age: An Astropolitical Analysis," *Journal of Strategic Studies* (June/September, 1999), pp. 83-106.

<sup>21</sup> [http://en.ria.ru/military\\_news/20130402/180392027/Russian-Military-Says-CFE-Treaty-Has-No-Future.html](http://en.ria.ru/military_news/20130402/180392027/Russian-Military-Says-CFE-Treaty-Has-No-Future.html) „Russian Military Says CFE Treaty Has No Future”, 02-04-2013.

# COMPENDIUM 2015

weapons and where they could be deployed. But for almost two decades the treaty remained in the best interests of most of the participants, because of several reasons:

First, with the stabilizing limits established it, consequently, prevented arms racing throughout the continent.

Second, it enhanced conventional deterrence by expanding the "transparency".

Third, the treaty requires states to notify participants of change in the size and character of their military forces and provide an annual exchange of information. Fourth, the strict inspection and verification regime insures compliance. This, coupled with information exchanges, insures that all members have a great deal of predictability in forecasting the military forces of their neighbors. Fifth, the treaty also establishes a clear momentum in the process which may bear fruit in other areas.<sup>22</sup>

## BIBLIOGRAPHY

Brzezinski, Zbigniew, *The Grand Chessboard*, New York: Basic Books, 1997.

Fukuyama, Francis, *The End of History*, in Toal, Gerard; Dalby, Simon; Peter

Routledge (eds.), *The Geopolitics Reader*, London: Routledge, 1998, pp. 114 -124.

Huntington, Samuel P. *The Clash of Civilizations*, in Toal, Gerard; Dalby, Simon;

Peter Routledge (eds.), *The Geopolitics Reader*, London: Routledge, 1998, pp.159 - 169.

Kissinger, Henry, *Diplomacy*, New York: Simon&Schuster, 1994.

Mackinder, Halford J., *The Geographical Pivot of History*, *The Geographical Journal*, Vol. 23, No. 4, 1904, pp. 421 - 437.

Francis P. Sempa, *Geopolitics From the Cold War to the 21th Century*, Transaction Publisher, 2002.

Hussein Solomon (ed.) *Challenges to Global Security: Geopolitics and Power in an Age of Transition*, I.B. Tauris, 2008.

---

<sup>22</sup> [http://jamestown.org/edm/?article\\_id=2372298](http://jamestown.org/edm/?article_id=2372298)



## **The Legal Aspects of the Vienna Document 2011**

**Tamás Lattmann**

(Tamás Lattmann JD PhD is an Associate professor of law at the National University of Public Service and the Eötvös Loránd University, Budapest.)

The Vienna Document 2011 is a set of confidence and security-building measures (CSBMs), prepared under the auspices of the Organisation for Security and Co-operation in Europe. It has been designed to increase openness and transparency concerning military activities conducted inside a specified territory, thus contributing to the security of the continent.

This territory is called the zone of application (ZOA), which includes the territory of all European (Russia from the western border to the Ural Mountains) and Central Asian participating States, including their sea areas and airspace. Military forces and activities of the United States and Canada are also subject to the document, if those are located inside the ZOA.

The provisions of the document provide for a variety of information exchanges, inspections on-site, evaluation and observation visits and other activities. All of these serve the main goal of growing security via mutual confidence.

This paper offers a deeper insight into the legal aspects of the document and, additionally, it tries to identify some of the vague and uncertain elements still requiring our attention.

### **International legal background**

First, let us analyse the basic international legal norms which serve as a basis for documents similar to the Vienna Document 2011.

#### **Prohibition of the use of force**

The first of these international legal norms is the general prohibition of the use of force, embodied in Article 2 Paragraph 4 of the UN Charter. This is one of the fundamental legal norms that our contemporary international legal order is being built upon. The abolishment of the use of force in international relations has been the result of a long, and examining current international politics, it is safe, though, unfortunate to say still not completely finished, gradual process. There was a long road leading from the early philosophers, theoreticians and legal thinkers to the negotiation rooms and diplomatic delegates of San Francisco, where the final text of the Charter has been drafted. Earlier attempts of history to reach a similar goal have never brought exhaustive results with the League of Nations Charter's legal framework having only a temporary timeframe and the Briand-Kellogg Pact of 1928 which, while prohibiting "war", left an interpretational gap for military actions "short of war".

The theoretical background behind the idea of introducing this provision is the political will for a firm reaction to the horrors of the two recent world wars. But we also have to consider another not so idealistic or even naïve reason: states have finally realised that the use of force can be counterproductive. The economic and political costs of force-backed power politics have significantly started to grow already during the 18th century and the introduction of nuclear weapons has also opened up new and extremely dangerous dimensions. As if the incredible losses of human life (both military and civilian, the latter in an already clearly disproportionate amount) of the previous world wars had not been enough, the chance of mankind destroying itself has become a reality with nuclear

weapons and this has led the most powerful states to find new ways to pursue their interests. Channelling them into international organisations and institutions (UN Security Council and permanent membership being the most obvious example) provided a chance to replace direct conflict between these states and, thus, the threat of mutually assured destruction (MAD) has, absurdly enough, become a key element of peace to peace among them.

Some may also come to the conclusion that Article 2 of the UN Charter does not have any serious relevance in relation to superpowers. Still, local conflicts and armed hostilities among states of lesser gravity have remained a serious concern that has to be evaluated in the light of this provision, as most of the actors of these conflicts are not able to follow the ways of the superpowers: they often lack influence, capacity and resources to do the same, so they may find use of force to be a possible option its price usually rises to the surface only afterwards. Most of the smaller states have clearly recognised this, so they take the "influence-competition" stand instead, regardless of their less favourable position, but in many cases they may decide otherwise. The important task is to prevent these wrong decisions.

While the provisions of the UN Charter aim at a more general prohibition, referring to the "use of force" instead of "war", some elements of the text still leaves space for many different interpretations. State practice unfortunately often uses this to try to find legal explanations for its military actions of dubious legitimacy, but the scope of the present paper is not to cover or analyse these. Here it is important only to refer to this phenomenon which demonstrates that, unfortunately, even this solid and very important legal fundament of contemporary international law is not completely free from trouble while there is an obvious consensus about on the desire to live without the threat of use of force, in some situations this desire does not conform to reality.

### **Obligation of peaceful cooperation among states**


Prohibition of the use of force is an international legal provision aimed at trying to avoid the worst. But there is another rule of fundamental nature supporting it, with a more general scope of application. This principle is the general obligation of peaceful cooperation among states, also provided for by the Charter of the United Nations, Article 1, Paragraph 2-3. Apart from its codified nature, it is also widely accepted as having customary force, thus being legally binding upon all states under all circumstances.

The scope of these provisions is actually quite wide: they aim to achieve friendly relations among states, an important part of which is the basic obligation of peaceful cooperation, meaning also the obligation of peaceful settlement of disputes. Direct negotiations, diplomatic solutions, judicial proceedings by international fora are all available tools at the disposal of states, but usually none of those are explicitly obligatory under all circumstances meaning that the methods by which the states may fulfil their obligations could take many forms.

Related to international cooperation in the field of security, the current state practice has developed many methods which have been incorporated into various international treaties and documents. The Helsinki Accords of 1975 meant a very important first step in this process, with the Paris Charter of 1990, the Global Exchange of Military Information and the CFE treaty of 1990 following suit.

### **Possible ways and methods to achieve more security**

The legal norms of international treaties or international customary law are obviously very important



and useful when it comes to their application or evaluation of states' respect towards them, but in themselves they do not guarantee security and state compliance. As international law and, especially, compliance with provisions of international law is mostly subject to sovereign states' own decisions, in the most cases state behaviour is determined by numerous non-legal factors.

When it comes to security, this applies all the more so: governments often have to encounter realistic legitimate security concerns as well as wrong perceptions or misperceptions of security. The latter ones in some cases may lead to political pressure from local public opinion of such gravity that it cannot be left unanswered in the worst case, this may easily lead to serious international crises. Finding answers other than recourse to the use or threat of the use of force to such situations is one of the most complicated things that states may face. The previous part has demonstrated this problem, this part deals with possible solution elements in order to deal with it.

Decision-making of states is usually based on information possessed by them, so gathering of information from various sources is just as old as the states themselves. Information regarding other states' military capacities and capabilities is extremely important because it may lead to considerations and predictions of the other state's possible political or military movements and it can lead to the planning of the other state's own responses accordingly. As this information is extremely important to states, its collection is historically considered to be problematic, both in the legal and political sense. Sovereign states usually consider security-related information related to their own capabilities and capacities to be sensible and not to be disclosed to the public, especially not to other states which may pose a threat to their security and relevant provisions of international law also support this attitude.

At the same time much of this information cannot be considered as being really vital to the security of states. Especially if the given state does not prepare for any hostile activity against other states. In such situations there is virtually no good reason to uphold such strict confidentiality of such information, at least not against other countries with the same attitude. The ease of this strictness can result in growing trust and confidence between states that can in many cases also contribute to international security, maybe more effectively than some other methods.

This kind of trust and confidence can be achieved by providing reassuring information. The so-called confidence- and security-building measures developed by state practice during the last century can also be qualified as methods of "legitimate intelligence gathering" to help actors of international relations and politics to evaluate given situations and make best-fit decisions.

The value of this method has already been recognised, which has been proven by some historical examples though with various success. The military restriction clauses of the Versailles peace treaties after the First World War have not served explicitly for the building of confidence, but they could have had the same effect. Unfortunately, they rather contributed to the overall failure of the whole post-war collective security system as states had made effective efforts to circumvent these provisions widely seen as a political tool of revenge and precaution by the Entente Powers. After the Second World War, the creation of the European Coal and Steel Community has proven to be much more effective, even though its trust and confidence building effect has only been indirect. But by providing an effective control to states concerned over the German coal and steel production and trade this has made it possible to shift the focus of attention to economic cooperation as the security concerns have been properly met. By making sure that any state can access the strategic raw material and steel products the alleged strategic advantage of Germany has not been considered to be of such importance, and a new era of cooperation in Western Europe could begin have started.

## **The Vienna Document 2011**

### **Development of the Vienna Document 2011**

The Vienna Document is an instrument of vital importance regarding arms control and confidence-building between European states. It had been adopted by the Organisation for Security and Co-operation in Europe (OSCE) in 1990 after the end of the Cold War, as part of an effort to assure long-term security of the continent, a common goal shared by all 57 member states.

During the 1990s, the document has gone through updates in 1992, 1994 and 1999. It has undergone its last major revision in 2011 (at the OSCE Ministerial Council in Vilnius on 6 December 2011), reflecting the needs and requirements that surfaced over time. Historically it is built on the 1975 Helsinki Final Act, the Document of the Stockholm Conference of 1986 and the 1992 Helsinki Document. Today it serves as a component part of a network of international agreements, including the Treaties on Conventional Arms Control in Europe (CFE) and the Open Skies agreement, which form the contemporary framework of European conventional arms control. Minor amendments have been adopted in 2012 and 2013. Today it includes measures for achieving increased transparency capable of leading to confidence-building and also mechanisms for peaceful resolution of conflicts, if needed.

OSCE member states today consider this documents as a cornerstone of European security and most of them advocate strengthening its crisis response mechanisms and transparency of armed forces and their activities. They have committed themselves to detailed information exchange on their armed forces and weapon systems, military budgets and military activities.


Generally speaking, the Vienna Document is an agreement between the states of the Organization for Security and Co-operation in Europe with the aim of implementing confidence and security building measures. Its provisions include:

- annual exchange of information about military forces located in the zone of application (meaning the territory from the Atlantic to the Ural mountains);
- notifications for risk reduction (which includes consultation about unusual military activities or hazardous incidents as well as prior notification about certain military activities);
- mutual observation of certain military activities;
- exchange of annual calendars;
- compliance and verification, mostly by inspection and evaluation visits.

It may be useful to differentiate these measures from those that derive from other OSCE programmes. For example, the Global Exchange of Military Information, that has been created at the 91st Plenary Meeting of the Special Committee of the CSCE Forum for Security Co-operation in Budapest is not limited to forces only in Europe but applies to all military forces of participating states, located anywhere. The annual information exchange under the Vienna Document 2011 is conducted separately from the annual exchange of information under the CFE, which takes place in Vienna, Austria every December.

### **Obligations deriving from the Vienna Document 2011**

The document creates a set of mutual obligations for participating states. First and foremost it



stipulates a general obligation of mutual cooperation, which can be interpreted as a direct application of the international legal principle of peaceful cooperation among states, described above. Secondly, the document creates a framework of information exchange, with the aim of deepening confidence and trust between states. Thirdly, it creates the obligation for states to adopt proper domestic legislation for the above mentioned goals.

The legal nature of the document also merits attention. It is not an international treaty in the strict sense of international law, as it is not subject to state ratification, and its paragraph 160 emphasises that "The measures adopted in this document are politically binding". This political binding power provides for something like "soft law" in international law, but it does not mean the lack of any obligation between states covered by the document, but, rather said, the lack of any enforcement mechanism. This binding power is subject to reciprocity, not to judicial enforcement in case of a breach of the agreement, the responsible state has to consider an in kind response as a consequence. Namely, other states will also react with a violation, firstly excluding the violating state from the system of cooperation, and could in the worst case possibly lead to the collapse of the system as a whole if the violation becomes the general reaction.

Some may argue that this is a weak obligation, but there are two arguments against it. Firstly, international law is based much more on common interests than enforcement mechanisms. Thus, when consensus is broken, the operation of the whole system becomes compromised, and this is especially the case when talking about confidence building as a result, this consequence is just proper for an agreement of this kind. Secondly, the lack of an enforcement mechanism cannot serve as a valid argument against the binding nature of a norm in international law, as existing enforcement mechanisms are not too common even when related to international treaties. Any procedure by the International Court of Justice or any other international judicial forum is still and most probably will go on to be subject to consent of states as long as the current system of international law built on the concept of state sovereignty exists. As a consequence, the lack of an enforcement mechanism could be used as an argument against the binding nature of any norm of international law or of any document.

We can conclude that the document has a binding force in relation to OSCE member states, even without any enforcement mechanisms, and that it is capable of creating a framework of confidence and security-building and to regulate the conduct of states related to the activities needed to achieve that.

#### **Overview of Vienna Document 2011**

The nine chapters of the document provide for a complex system. As indicated above, their provisions apply only to military forces in the ZOA, except for those in Chapter II, which serve the goal of general transparency, thus there is no limitation of this kind.

Chapter I covers the so-called Annual Exchange of Military Information (AEMI). This means the exchange of military information among participating states. The information covers the command structure, location, personnel strength and major conventional weapon and equipment systems of both active "combat" and "support" forces. It also includes the plans for the deployment of major weapon and equipment systems of the states. Information exchange is due according to the annual calendar.

Chapter II covers defence planning. Information on planning can be of crucial importance regarding



# COMPENDIUM 2015

confidence building, as partner states can reassure themselves about the lack of hostile intent based on this data. The document provides for the exchange of information on defence policy and doctrine, force planning, relevant budgets, military or other security-related procurements.

Chapter III of the document deals with risk reduction, which is one of the most important, regarding confidence building.

It provides for a mechanism for consultation and co-operation regarding unusual military activities. The aim of this provision is to create an option through notifications and meetings for prompt settlement and prevention of any tensions deriving from a military movement of a participant state. This can be extremely useful in situations of political tensions between two states, when even the actions of various non-state actors (for example, private organisations hostile to the other country) may raise security concerns. The document creates a proceeding for such situations: upon the request of the state concerned, the other state has to reply within forty-eight hours, and, if requested, has to participate in a meeting within the same time frame. The meeting is held under the auspices of the OSCE Chairperson-in-Office (CiO) and third parties may also participate if they wish to do so.

The chapter also provides for similar co-operation regarding hazardous incidents of a military nature and also for voluntary hosting of visits to dispel any concerns about military activities.

Chapter IV covers the issues of contacts. It invites participating OSCE states to visits to other states' air bases and demonstrations of new major weapon systems or equipment. Apart from the specific events, it also facilitates contacts between the armed forces of these countries. These can take the form of joint trainings, academic exchanges or other programmes that help create confidence on the level of individuals of the armed forces. As decision making is conducted by these persons even within the military structure, the importance of the individual is still crucial.

The document also deals with the so called "Certain Military Activities" (CMA) which may raise concerns from participating states, thus being very important when it comes to mutual trust and confidence. Chapter V provides for a prior notification procedure of CMA at least 42 days before it happens, if the activity exceeds pre-determined thresholds. This means the inclusion of 9,000 troops, 250 tanks, 500 amphibious combat vehicles or 250 pieces of artillery. Additionally, chapter VI creates a possibility for observation of CMA. It invites all participating OSCE states to observe any CMA that exceeds the thresholds of 13,000 troops, 300 tanks, 500 amphibious combat vehicles or 250 pieces of artillery. These provisions serve as a reassurance to states in cases of military movements that may threaten mutual confidence among states and build on already existing state practices of military observation, putting them into an OSCE context. Chapter VII deals with annual calendars, it provides rules for exchanging information on CMA subject to prior notification planned for the subsequent calendar year.

Chapter VIII contains constraining provisions according to which participating states agree to limit certain large-scale military activities, which include limiting both the numbers of activities and their levels.

The last chapter (IX) provides for compliance and verification. The possibility of on-site inspections and evaluation visits is of vital importance for states in order to have the opportunity to confirm the accuracy of information previously obtained via the exchange methods under the document. This does not only help confidence building, but, generally speaking, is the guarantee that keeps the concept of information exchange alive as long as states can trust it.



### **Domestic legal obligations**

The most important domestic legal obligation of states deriving from the document is to create the necessary domestic legal environment that makes it possible to achieve the goals set by it. State authorities and military forces are, first and foremost, subject to their own states' jurisdiction and authority, so it is imperative that states provide for applicable legal rules. Most of the countries' constitutional systems require domestic legal implementation of international legal rules so that they can have a legal effect within their jurisdiction, and this is especially important in the case of an international document having "political binding force", since in this case the legal binding force may be questioned on the level of international law. Proper domestic implementation of these norms circumvents the above-mentioned problem and helps achieve the goals of the document.

Domestic legislation has to cover every possible activity mentioned by the document. States have to analyse their existing domestic legal systems and provide for any missing legal rules regarding, for example, information exchange and visits. This work may require very detailed scrutiny to make sure that no legal norm poses a threat to any activities required by the documents: data to be exchanged has to be de-classified (that was classified under domestic law) in due time, clearance has to be provided to visit sites and domestic proceedings for notifications and information disclosure have to be created as well. Logically, and according to the document, domestic legislation is needed for the cooperation mechanisms provided for by the document, but it may be beneficial if participating states think about other possible means of cooperation as well, though it is not obligatory.

Apart from legislation strictly focusing on the contents of the Vienna Document 2011 states are also responsible to provide for proper domestic application of the above-mentioned domestic norms, which may require additional legislative work. These can cover, for example, various rules related to domestic judicial proceedings (in case of disciplinary or criminal measures related to military conduct related to a site visit) or non-judicial proceedings, executive regulations, even standing orders. Such legal provisions usually exist regardless of the Vienna Document, but they need to be revised and evaluated if they can be applied properly.

### **Some questions about the future of the Vienna Document 2011**

#### **Future legislation**

While the Vienna Document 2011 is a complex set of rules, which are in my opinion capable of achieving the goals they have set, the question of future legislation is always on the table. Apart from amending the document with detailed rules that can be created by using the experience gained by actual practice, the fundamental question is the one aiming at the adoption of a legally binding document, possibly in the form of a general international treaty.

Based on the analysis above on "political binding power", I do not think that this is absolutely necessary. It would probably be useful as it could strengthen the international legal obligations (and domestic ones in the case of some of these states), but for OSCE member states and their political community this web of mutual political interests is enough to provide for this co-operation system. On the other hand, by shifting the weight from this common political interest towards possible judicial enforcement mechanisms, a weakening of the already existing co-operation system may occur, with

some elements arguably reaching customary power, which is definitely an unfavourable option.

While I do not argue that there is a need for a general international treaty that would replace the Vienna Document 2011, I consider the adoption of additional bilateral or sub-regional agreements useful. Based on the document, some of its provisions may be included in such international treaties either on an ad hoc basis or permanently. Nothing keeps states from creating tighter bonds in on this field, if they feel the need to do so. In some cases, these additional guarantees may be useful, especially in near-crisis situations. For these types of situations, a model treaty could be drafted, with provisions based on the document, but with stronger enforcement measures that may include referral to international dispute resolution organs, for example the International Court of Justice.

One question of concern is the number of quotas included in the document, for example those related to CMA. These numbers can be subject to change, as the question of CMA thresholds can serve as a basis of concern in many cases. But this may be subject to future negotiations of states, as there are strong arguments in favour of lowering the threshold as well as those against it.

#### **More efficient enforcement measures?**

The practice of the annual Implementation Assessment Meeting (AIAM) is useful and can be considered to be satisfactory overall, but it can only address issues and negotiation between states, which may prove to be inefficient in case of crisis situations.

In the latter cases, a dispute resolution method could be adopted that could offer a possible political compromise. Accepting the document as "politically binding", this may be considered to be an overextension of its original goals, but in some cases it may be useful and necessary. First of all it is important to emphasise that in a situation of serious crisis that would pose a threat to international peace and security, the United Nations Security Council has the possibility to act under Chapter VII of the UN Charter to adopt legally binding resolutions, which would take precedence over any agreement of the states concerned meaning that this institution has the leading role. But in case of the Security Council's paralysis for example, because one of the permanent powers is involved in the crisis and uses its veto power, or simply does not act- this possibility would be an option. Dispute resolution techniques, for example, arbitration under the auspices of the OSCE or even a referral option to the International Court of Justice are valid options.

An overall problem related to all international documents, not only the Vienna Document 2011, is the need for stricter domestic legal provisions related to their subject matter. As indicated above, proper domestic implementation is a must for any of those to be able to reach their goals. With all due respect to state legislations, sometimes this work is not completely successful. To prevent incomplete or wrong domestic legislation, a set of model rules could be drafted and offered to participating states for consideration. The drafting process of these model rules shall incorporate the experience and expertise of all participating states it shall examine already existing domestic laws, compare and evaluate them. The scope of this work shall cover all possible levels of domestic legislation, from the most fundamental constitutional norms to the executive ones, or even standing individual orders related to anything connected to the Vienna Document 2011.



## **Defence, Public Interest and/or Consensus: Limitations and Possibilities**

Stjepan Domjančić PhD

Ministry of Defence, Republic of Croatia

### **Introduction**

Recently we have witnessed a revival of interest shown for military and defence issues. This phenomenon can be observed on two levels: the global level - followed by dramatic remarks concerning the tectonic disturbances in the geo-strategic theater, and at the national, Croatian level through the extensively exploited topic regarding the future of the Croatian Air Forces. However, the increased public interest reflects the daily political inputs; it is not the result of substantial changes in the attitude of citizens towards the formulation and implementation of public policies, or increased awareness of the problems of modern societies. Therefore, one cannot speak of a different positioning of defence as one of the policy areas in relation to other public policies, nor does it present the reevaluation of defence issues in society - it shows an increased level of forms which are primarily determined by highly emotional patterns used in approaching these issues. Such an increase of public interest is generally inversely proportional to the relevance of the topic involved. The main reason for this is found in the over-simplification of the issues and their arbitrary and superficial contextualization.

The prerequisite for identifying a repositioning of defence in a society still amounts to the volume of mythical, dogmatic material that we are ready to give up on. Consequently, the main issue is not the quantity of the defence themes represented in the public media space but whether defence gained a policy status as is the case for example with the area of health, public administration, the judiciary, etc. or whether they only represent a surrogate for public policy.

This paper examines the position of defence in modern societies, with special reference to the European post-communist societies; discusses the attitude of the society towards defence, especially the civil-military relations issues. The basic idea is that defence and civil-military relations must be understood beyond the dominant discourse in which the majority of issues in this area are being reduced to relations pertaining to political power.

Defence and civil-military relations are a very good indicator of the overall democratic consolidation of modern societies. The moment when defence will be predominantly understood as a policy, rather than as politics we will have created the proper conditions for the appropriate attitude of society towards defence and the optimal level of consensus.

### **Defence as a Policy Issue**

Is defence, therefore, at all public policy? If we take as a criterion meeting the needs and community interest, there is no doubt that defence should be treated as policy. To feel protected and secure is one of the basic needs of the people, citizens and communities. When it comes to its formulation and

implementation, defence is relatively distant from policy if one takes into account the influence criterion of the policy stakeholders (in the broadest sense of the word). Policy stakeholders, who are not part of the national management mechanism, especially those who operate within its horizontal dimensions, have been excluded from the overall policy cycle to the extent that is unparalleled to any other public policy.

There are three key reasons for such a positioning of defence or defence policy in the society:


1. Defence Policy is still highly militarized; Defence is conceptually identified with the Military, which, as a consequence, has implications in the area of management; it focuses defence mainly in the zone of the state and beyond the reach of the society and the area of defence policy gets a dose of mystification inherent to a military organization;
2. Consequently, the Armed Forces, as one of the mechanisms for the implementation of the policy, becomes a policy stakeholder (also within the vertical dimension of the policy);
3. Civil defence managers do not have the required level of expertise to position the defence as public policy and, therefore, this void is filled by military expertise provided by the military structure. Citizens are not seen as policy stakeholders but as objects of that policy.

In fact, the issue of consensus in the field of defence raises the question of how society relates to defence and security and its awareness or need to examine this relationship. In modern Europe we can observe two parallel processes: one where the society shows below-average interest in defence issues and the one where periodical intensified interest in defence is shown, induced by daily political content, filled with superficial and irrelevant topics. In both processes, consensus is not relevant. Consensus in Western societies is generally perceived as a value that contributes to peace and stability in human relationships, promotes cooperation and understanding but also reduces competitiveness and, thus, development. Consensus and indifference can easily go hand in hand. In order to avoid such a situation consensus should derive from a deep understanding of social processes and the implications they bring. To make this possible, state management structures are required to manage the defence sector taking into account the content, specificity and the importance of defence.

## **Historical Context of Understanding the Military Phenomenon**

Understanding of the military segment of defence policy, or, moreover, civil-military relations, is opening the way to withdraw from the dogmatic approach to defence and to liberate it from mystification.

During its historical development, the military as an institution has undergone many transformations. Independently of their significance and proportions, it is worth saying that changes have been a constant characteristic of its historical duration. In that regard, three key points concerning military transition can be distinguished. Each of them is denoted with new concepts and requirements in relation to military organization and its mission. So, in the late 18th century, concurrently with the social and political changes that were given impetus by the American and French revolution, the idea of modern mass (national) military was born. The basic premise of this concept was conscription of the citizens for the purpose of defence of their nation-state.



The idea of mass military was widely accepted, particularly after 1870 and eventually adopted at the time of both World Wars. This model that had prevailed for a long time underwent a deep metamorphosis during the Cold War.

At the end of the Cold War the modern mass military entered a transition process that has changed its organization, the purpose of its existence and is called the post-modern armed force. That is the beginning of expansion of the military's domestic role that now includes assistance in disasters as well as a series of functions connected with lawfulness, social order and governmental organizational system that has automatically brought changes as regards civil-military relations too. These changes will certainly lead to the question whether the military should outgrow its role as a deterrent force or whether it should be a force for constructive change at home or abroad.

Generally, numerous references in literature associated with military issues could be divided into two groups: one that refers to the narrative of the military in the social and political context (including its foreign policy and the internal policy function) and the other relating to military expertise (in terms of overall knowledge, skills and many more elements the military organization possesses, builds, or aims to build). A somewhat paradoxical conclusion could be drawn from that fact. We can almost unanimously agree about the military being a government institution that to the fullest extent personifies the essence of the modern state, which is completely monopolized by the state, and that in most of the countries has a special and highly idealized and emotionalized status; however, the same society is much less involved in studying this phenomenon, but, this is the case with many other phenomena. There are much more serious and relevant researches conducted not only on the military but also on its position in the wider social and political context, created under the auspices of that very same military, rather than in the other areas.

The key challenges for the military organization, and even more so for their managers and the social environment are not in the political or military institution-building, not even in mastering technological capabilities and their application for military purposes; the challenge is by no means defined by the number of troops and the corresponding weapons. The key challenges are in understanding the phenomenon of the military and its functions and in using this basis to build appropriate relationships and management processes. To respond to this challenge a lot more is needed than just declarative siding with the liberal-democratic tradition. It will not be achieved through any organizational changes in the military, nor a generous military budget, nor through attractive political messages for military "ears". The only way to deal with these challenges is by breaking the existing dogmas and myths.

### **The Military and Democracy**

In modern Western democratic countries the central point of deliberation on civil-military relations is the question of having an efficient and well-balanced control. This type of control fits the liberal model. The liberal model avoids two unfavorable/antagonistic scenarios: militarization of society due to insufficient and/or ineffective control and the politicization of the military due to excessive control.

Nevertheless, apolitical military in democracies should not be taken quite literally, at least for two reasons:

- Military professionalization is followed by the growing overlap of strategy and politics and, therefore,

the role of a modern military officer includes many political aspects, requiring training in order to be able to deal with complex political and strategic issues (Abrahamson, 1971: 13);

- The policy - making must take into account the interests of the military. In liberal democracies the Armed Forces present a powerful institutional interest; for example, senior officers of the American Army use their positions and knowledge at the National Security Council and the Congress to secure a bigger defence budget.<sup>1</sup>


In those new circumstances, a mission change in the military organization and with that of the officers' role has driven to intermingling of the military and political issues. An officer is forced to deal with complex politico - strategic issues and, therefore, military professionalization has caused one undesired but necessary consequence instead of separating officers from politics, it has driven to merging of the military and political roles. However, such political roles of the professional officers does not mean disruption of the concept of political neutrality. In some ordinary democratic context, a demand that a professional soldier is above politics implies his/her lack of connection with political parties and inexpressible affiliation to a political party. However, that party neutrality does not mean an apolitical attitude, particularly not in the part in which the mentioned new officer's role also includes a political role (e.g. advisory) (Smerić, 2005: 458). Therefore, we could say that only when bounds are crossed of such «political» engagement in participation in politics that would not be a result of the governmental regulation and institutionalization but of an autonomous decision of the military élite would represent an unallowed political involvement of the military. Only such an engagement would represent a disruption of the norm of political neutrality and Huntington warns that such participation of officers in politics represents a factor of diminishing professionalism and professional competency and is a source of interprofessional divisions (Huntington, 1994: 71).

Although there is almost universal consensus that the Western democracies built an effective, well balanced control over the military, it would be too presumptuous to draw the conclusion that all the challenges have ceased to exist and there is no need for further consideration and possible improvement of civil-military relations. Like any other organization, a military organization presents a dynamic organism and the civil-military relations are thus subject to a certain kind of dynamism. Military organizations are changing over time, in response to changing conditions. The key factors influencing the transformation of the military profession are: the growing importance of the role of technology, the weakening of social isolation of the military due to amassing of the armed forces and due to the modeling of deterring strategies in the nuclear era. These changes, which have occurred mainly in the second half of the 20th century, have resulted in the weakening of the boundaries between the military and civil society and they set targets for the military organization to participate more actively in the broader social context with the imperative to maintain the autonomy, competence and group cohesion (Smerić, 2005: 200-201).

There is an evident increase in the convergence of military and civilian institutions, and a more powerful intertwining of military and civilian sectors of society, due to a technological and organizational revolution. Complex consequences of this process reflecting on the characteristics of

---

<sup>1</sup> «At the highest level, generals and admirals are inevitably politicians in uniform, who spend more time in the political arena, rather than on the battlefield.» (Hague, Harrop, Breslin, 2001: 379)



the military organization Janowitz called "civilianization" (Janowitz, 1974.). It is the result of technological development of the complex machinery of warfare, which has weakened the line distinguishing military and non-military organizations and, therefore, the military establishment is increasingly showing characteristics typical of any large organization.<sup>2</sup>

No doubt that through such intertwining of military and civilian spheres the control of the military faced new challenges. If there is no longer such a clear distinction between military and civilian, how is it possible to set up an effective control over the military? On the other hand, some theorists, in the manner of Samuel P. Huntington warn that military organizational authority is now compromised by social marginalization of the Armed forces (in areas of "post-military" societies without war), despite the strengthening of their operational capabilities. This is done through a redefinition of the old and the emerging of new "non-traditional" military tasks, reducing the autonomy of action (caused by building and strengthening of global norms and powerful transnational movements and institutions) and the transformation of the Armed forces from the organization that "personifies" the state, to being the one of the actors among many who require the allocation of state resources. This way military organization loses its exclusivity in its relations with the state. Certainly, these are not contradictory processes but processes that exist parallelly. Democratic societies are confronted with a very ambivalent processes and warnings: radical liberals will, in the interweaving of military and civilian roles and tasks see creeping, almost imperceptible militarization of society, while the advocates of radically exclusive military professionalism will see the elements of "eroding" of military professionalism and degradation of unity of the military profession (the weakening component of officers being oriented towards expertise in the "management of violence" - combat-oriented - and to the growing technical, administrative and techno managerial component) while the allocation of new "non-traditional tasks" to the Armed Forces on the one hand will be interpreted as an expression of a dynamic environment, and in a way just indicated the ability of the Armed Forces to answer to changes in their environment with necessary structural and functional adaptations while, on the other hand, it would be perceived as a way to marginalize the mMilitary.

### Eastern European Transition

When considering the established model of civil-military relations and the overall elements of what we call defence policy framework, the dominant type of political culture is a factor of critical importance. Although it is changing over time, these changes are very slow and gradual. Numerous sources are having an influence on the creation of a dominant type of political culture, but the biggest impact probably lays in the historical heritage and the key processes in different segments of society.

If we look at the European post-communist sphere, in general, the political culture is not marked with the willingness or the motivation to compromise. It unavoidably lead to a "zero-sum game" in which the gain on the civilian part means a loss on the military side and vice versa. Compromise was not

---

<sup>2</sup> Christopher Gibson and Don Snider investigated the dynamics of civil-military relations in the United States, focusing on the decision-making process. They showed that the Armed Forces have a large capacity to participate at the highest levels of decision-making, and a growing experience in political decision-making (Gibson, Snider, 1999). This is also the case in Latin America. The Armed Forces are not only taking over new missions that are predominantly of a civilian nature, but are also enhancing their ability to influence government decisions in other areas and departments. Latin American countries are a good example that shows an increased level of involvement of the military in the government decision-making process (Diamint 2003: 71).



perceived as a normal (and desirable) part of the political process, but as a weakness.<sup>3</sup> In order to introduce the political culture that generates compromise, the political system has to be based, on the one hand, on the rule of law and, on the other hand, on the broad consensus of fundamental values. For transition countries, in the area of civil-military relations this means that the restraint control (control by containment), should be gradually replaced by control of firm belief (control by conviction) (Lambert, 2009: 116). We could say that the transition to democratic institutions and values has been followed by problems on the military and on the civilian side as well. We will review some of the key issues which the area of civil-military relations in post-communist transition faces (Joó, 1995).

## ***1.) The Lack of Appropriate Expertise in the Field Of Defence***


A proper civilian expertise in security and defence matters did not almost exist in the early post-communist days. This applies equally to the communist party successors i.e., the reformed Communist Party and the Party of Democratic and liberal opposition. New Parties did not have the professional competence nor any experience in the field of defence and security. Moreover, parliamentarians, civil servants and officials, academics, journalists and others were not familiar even with the basics on when it comes to defence issues. At the beginning of the transition period, activities in this area were marked with what is commonly called the "demilitarization" of the defence sector and "civilianization" of defence policy and defence structures. However, this "civilianization" of the defence ministry sometimes had an extremely counterproductive effect. For example, this above mentioned effect shows the misunderstandings of civilian control and a conviction that civilians should have professional military knowledge, although it is clear that civilians within the Ministry of Defence do not exercise operational command and, therefore, do not represent a substitute for operational commanders. Expertise in the defence area is not the same as expertise in military affairs and in the execution of operational tasks. Civilian expertise and political control should not disrupt the area of professional military autonomy due to the risk of spillover of political and social conflicts into the military area and consequent weakening of the effectiveness of the military organization.

## ***2.) The Absence of Credible Inputs from Civil Society and the Electorate***

The interest of the society as a whole in defence issues is constantly on a very low level in most European post-communist states. Although the lack of interest is often explained by the presence of powerful liberal, anti-military, pacifist attitudes of the new generations with widely spread new lifestyles that have been rejected, the previously existing, traditional patterns and conservative values, which were considered to be imminent to a military organization, should be taken with certain skepticism. Specifically, the new, predominantly liberal values of a new era that are to a significant extent expressed in Western consolidated democracies do not lead to the same effect as is the case in post-communist countries. Moreover, while in the post-communist countries consolidated liberal tendencies are undoubtedly emerging in many areas, we are simultaneously seeing that strength is

---

<sup>3</sup> It is understandable that the absence of compromise broadly characterized the social and political scene of most post-Communist countries, and this did not occur in the area of civil-military relations only. Due to the fact that civilian control over the military during the Communist regime was implemented using the penetration model, which meant a high level of politicization of the military and the militarization of society in post-Communist transition, the new political elite was particularly ruthless in the projection of its power in the area of civil-military relations, because it signified a great victory on the symbolical level. Ironically, as it happened for example in Poland, which had a dominant military power in Communism, the new post-Communist political elite was quite benevolent toward the old military elite, emphasizing the "patriotic Januzelsky motives", while in the countries where the Army quietly allowed the disintegration of the old Communist government and, thereby, enabled a bloodless path to democracy, as was the case in the Czech Republic or Hungary, the absence of any higher level of compromise was strongly shown.



being given to an extremely rigid, conservative and xenophobic attitudes and ideas. While no Western societies are exempted from such conflicting ideological positions, they are far more resistant to any attempts to challenge liberal democracy and its legacy and, therefore, rough reactions that come across are being rejected. The military organization in the Western societies has been liberated to a significant extent from bearing the conservative image of the patroness of traditional values and is increasingly starting to represent different values and ideological orientations that are a part of the society from which it has originated.

As a result, the indifference of the society regarding defence issues in the post-communist countries is to a large extent caused by the same reason that affects and produces the lack of appropriate expertise. The absence of civilian expertise is largely responsible for the fact that defence issues are rarely being articulated as relevant social issues, but are rather being treated as a budget issue.

### ***3.) Lack of Understanding of the Concept of Civilian Control***

In the post-communist period, a large number of new political actors are often facing the problem of how to maintain political neutrality when it comes to defence. Civilian control is perceived as the process of creating personally and politically loyal leading military personnel. Essentially, this process has retained the key features of penetration models of the previous period.

### ***4.) The Lack of Experience in Working Together With Civilians***

The first transition and reform challenge on the military side was particularly relevant in the interaction between the military and the highest managerial and / or supervisory levels in the ministries of defence and parliaments. Defence Ministries have been fully militarized institutions and civilian employees were mostly in support, technical and lower-paid positions. The military, therefore, was somehow reluctant to accept the new situation in which a civilian defence minister and civilians were both present in the defence department, which, up to then, had been exclusively military. However, in post-communist countries, the reluctance was more pronounced in terms of certain clumsiness and disorientation, and less in terms of deliberate obstruction. In general, the military has accepted the new situation relatively well. Admittedly, it was probably not the result of democratic beliefs in the military but of the real overview of the present situation. In fact, it was perfectly clear to the military that civilians do not, nor will soon have, the capacity which could effectively compete with the military expertise, and that despite the formal "civilianization" of the defence sector the actual extent of the civilian impact on defence issues would be rather small.

The problem of inexperienced soldiers working with civilian partners, their immediate superiors/officials, parliamentarians, etc. in high structures of the military or in the defence hierarchy showed a misbalance in defence expertise between soldiers and civilians. Regardless of this imbalance in defence expertise, and even if hidden intents of the military to maintain the highest possible level of influence in the defence would not transpire, this problem was clearly visible and went through various stages.

### ***5.) Relative Isolation from Civil Society***

The military has been far more intensely confronted with transition problems than it is the case with other social groups in a situation of adapting to new conditions brought about through pluralist democracy and a market economy. In the Communist society, the military was a closed society within

a closed society. Under these new circumstances, the military was supposed to come out of this sub-social context and enter the new open society. Its former relative social isolation made this change more difficult for the military than it was the case with other social groups. The military was faced with a completely new, unusual, and quite different position – it went from a long period of being protected from public view to being exposed to critical media, public debates, judgment and assessment. For the first time, the military felt very vulnerable and did not have the answer how to protect itself. In addition, it had to acquire some new management and leading capabilities, which were previously not required. On the one hand, there was a need for acquiring ability/skills to communicate with the public and with civilian control and/or supervisory elite; on the other hand, it was necessary to develop defence management skills in the framework of budget constraints and to take the account of the overall social context at any time.


## **Civil-Military Relations in the Post-Modern Age**

Studies of democratization and civil-military relations are usually being done separately. Those analyzing the world of democracy rarely dare to enter the world of the military, and if they do, they mention the military only briefly. Those who are involved within the military are generally concerned with security and defence issues and are excluding the broader political context of democracy.

In deliberation of civil-military relations it is necessary to shift the focus from military reform to the debate on democratic progress. Transition studies often show a sort of reduction when it comes to analysis of civil-military relations. In transitional states civil-military relations will be directed almost exclusively towards military reforms (in Eastern Europe it will be evaluated in terms of meeting the requirements of Euro-Atlantic integration processes) and the absence of threats will be perceived as evidence of an established subordination and of regime's democratic consolidation (primarily in Latin America). This brings us to the conclusion that the transitional states are facing only and exclusively issues belonging to the so-called "First generation" challenges from the area of civil-military relations, and that only the Western consolidated states can talk about the new challenges that appear in the postmodern era.

The "First generation" issues are related to the potential hazards of military Praetorianism. Consistently established legal framework of civilian control is generally considered to be an appropriate instrument for prevention of such threats (Lambert, 2009: 27). "Second generation" of challenges relates to the question of how generally defence policy is being managed. However, the conceptualization of defence policy management does not attract the attention of researchers such as is the case with a set of questions from the "first generation".

The "Second generation" problems in civil-military relations marked, in fact, a move of focus from "civilian control" and from the state to the broader societal aspects of the "democratic control", not only of the military but also of the number of security sector institutions and related activities. While the measures taken in the context of the "first generation" were mainly focused on the process of democratic transition and the establishment of effective political control over the military, the "second generation" measures are undertaking a far more ambitious task - to establish effective control mechanisms throughout the security sector, including developing and shaping defence and security policy. The "second generation" measures are determining the essentials for the process of democratic consolidation.



Socio-military relations are strongly influenced by major changes into the elements of social organization, general reorganization of the post-industrial societies and their positions and interconnections. The new era, formed by new societal paradigms such as pluralism, fragmentation, heterogeneity, disintegration, diffusion and ambivalence brought changes regarding the way the state uses the power, as well as in terms of citizen's loyalty. The current trends are fundamentally transforming the military structure, its culture and missions and thus civil-military and socio-military relations. The conditions of military training and its engagement are rapidly changing and the military is, therefore, faced with the social environment and cultural patterns on the one side and political demands on the other side and those factors are strongly eroding its identity and traditional characteristics. The disappearance of the traditional images of the soldier's job as a purely "male job", the introduction of private military corporations in the area that was considered to be the last monopolized area by a military organization, the dominance of military humanitarianism over conventional military action, etc. are just some examples of these changes.<sup>4</sup>

The problem of the transition states lies in the fact that they had to deal with the challenges of the "second generation" of civil-military relations, which had already swept Western consolidated democracies, while at the same time the "first generation" issues were not resolved.

The degree of speed and change in civil-military relations in transition countries has been determined by a limited number of qualified persons among the powerful party leaders, as well as by parliamentary and executive power, financial constraints and bureaucratic inertia. Different historical and cultural background, the dominant foreign economic ties, tying the political elite to the West or Russia, ideological and political manner of new (or new / old) political leaders - all this affects the different levels and styles change, not only in civil-military relations but in other areas of public life as well (Bebler, 1994).

#### **Defence and Democracy: Conclusion**

Although the focus should be shifted from military reform to the debate on democratic progress when considering civil-military relations, the reduction of the area of analysis of civil-military relations in transitional studies is very often the case. Thus, in transition countries, a deliberation on civil-military relations is directed almost exclusively toward military reforms (which are evaluated in terms of meeting the requirements of European integration). This would bring us to a conclusion that the transitional governments are faced only and exclusively with matters belonging to the so-called "First generation" challenges in the area of civil-military relations, and that only in the Western consolidated states it is possible to explore new challenges, known as the "Second generation" challenges that appear in the postmodern era. We have already shown that the essential characteristics of civil-military relations of post-communist transition is precisely that, the simultaneous presence of both generations' challenges.

It is necessary to understand civil-military relations in a much broader context than tie it to exclusively

---

<sup>4</sup> Although the attitude that after the fall of the Berlin Wall and the disintegration of the Soviet Union peacekeeping and humanitarian missions replaced war is an exaggeration, some trends are undisputed and the data they confirm is very interesting. For example, in 1998 more civilian employees of the United Nations than, military personnel which operated under the UN flag (Moskos, 2000) were killed in Peacekeeping and humanitarian missions for the first time.

# COMPENDIUM 2015

to the issue connected with ensuring political neutrality of the military that presents a "first generation" challenges in the field of civil-military relations. The real agenda of civil-military relations is the "Second generation" challenge that is related to a much broader framework and includes the establishment of effective control mechanisms throughout the security sector, which means designing and shaping defence and security policy. The "Second generation" challenges are crucial for the process of democratic consolidation.

## References:

- Abrahamsson, B.** (1971.) *Military Profesionalization and Political Power*. Stockholm, University of Stockholm
- Bebler, A.** (1994.) *The Evolution of Civil-Military Relations in Central and Eastern Europe*. NATO Review, No. 4., Web Edition, na <http://www.nato.int/docu/review/1994/9404-7.htm>
- Diamint, R.** (2003.) *The Military*. U: Dominguez, J. I., Shifter, M. (ur.) *Constructing Democratic Governance in Latin America*. Second edition, The Johns Hopkins University Press, Baltimore London, 43-73
- Gibson, C.P., Snider, D.M.** (1999.) *Civil-Military Relations and the Ability to Influence: A Look at the National Security Decision-Making Process*. *Armed Forces and Society* 25 (Winter)
- Hague, R., Harrop, M., Breslin, S.** (2001.) *Komparativna vladavina i politika*. Fakultet političkih znanosti u Zagrebu, Zagreb
- Huntington, S. P.** (1994.) *The Soldier and the State: The Theory and Politics of Civil- Military Relations*. Cambridge, Massachusetts London, England: The Belknap Press of Harvard University Press
- Janowitz, M.** (1974.) *The Profesional Soldier. A Social and Political Portrait*. New York-London: The Free Press-Collier Macmillan
- Joó, R.** (1995.) *The Democratic Control of Armed Forces*. Western European Union's Institute for Security Studies, Chaillot Paper, No. 23, February
- Lambert, A.** (2009.) *Democratic Civilian Control of Armed Forces in the Post-Cold War Era*. Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva
- Moskos, C.** (2000.) *Towards a Postmodern Military?* U: Cohen, S. (ur.) *Democratic Societies and Their Armed Forces: Israel in Comparative Context*. England: Frank Cass, 3-26
- Smerić, T.** (2005.) *Sparta usred Babilona? Sociologijski aspekti vojne profesije*. Hrvatska sveučilišna naklada, Zagreb



## **Development Opportunities Regarding Human Protection Through the Triad “Human-clothing-Environment”**

Dr. Daniela Zavec Pavlinic

CEO of Titera Ltd. Technical Innovative Technologies, Murska Sobota

Assoc. Prof. Dr. University of Primorska, Faculty of Mathematics, Natural Science and Information Technologies, Applied Kinesiology, Koper, Republic of Slovenia

### **Introduction**

The optimal design of military personal protective equipment (PPE) must account for the anticipated activity of the wearer and the environmental conditions. Despite the modern working protocols and significant advances in defense technology on different working fields, PPE remains one of the main factors influencing the efficiency, level of protection and comfort of war-fighters and/or peacekeepers, particularly under extreme environmental and/or operational conditions. The PPE still has a major impact on human comfort, since it presents an element which is directly connected to the largest human organ – skin. Regarding this, development and evaluation of personal functional (protective and working) equipment for soldiers, fire-fighters, rescuers and workers in extreme working environments involves a variety of factors that depend on physical requirements of the mission and/or working activities and environmental conditions to which personnel is exposed. For this reason the triad „human-clothing-environment“ accounts for the design and optimization of PPE. Under normal conditions, thermal and ergonomic comfort is of primary importance, but under extreme environmental conditions; prevention of injuries (heat, stress, burns, disturbance in the cardiovascular system, dehydration, cold and non-cold injuries, etc...) may become the principal objective.

### **Development opportunities**

To protect humans in extreme environmental and working conditions (extreme high and low temperatures, fire, explosions, virus, weapon, poison, etc...), the development process of functional clothing systems should combine knowledge of textiles/clothing and physiology. During the past studies the standardised process for the development of optimal personal protective and working equipment was developed (see Figure 1). The 5-level development approach proposed by Umbach in 1987 [1, 2] has been upgraded. The process incorporates factors which are of most importance in the process of optimisation and development of functional clothing: the demands of the triad “human-clothing-environment” as well as the wearer's behaviour and activities, performed in a certain geographical environment. It combines textile and clothing laboratory tests as well as laboratory and field tests with human subjects as well as modelling and evaluation of the functional clothing ensembles [3].

## Model of development of the optimal clothing system

For example, this Model can lead you through the optimization of use for combat ensembles as well of the other different protective and working clothing ensembles. The aim of such an optimization process can help in the evaluation of the desert combat ensemble in terms of thermal and moisture (dis)comfort and to assess the contribution of each component: clothing items inside the desert ensemble (underwear, middle layer, outer layer), helmet (and under cap), bullet proof vest, gloves, boots, socks, backpack, NBC (nuclear, biological, chemical) outer layer of ensemble to overall heat strain in simulated conditions. This would provide information regarding the adequacy of individual components as well as the complete combat ensemble. An adequate multilayer clothing system should allow heat exchange between the body and the surroundings so that excessive displacement of core temperature is prevented regardless of the wearer's activity level.

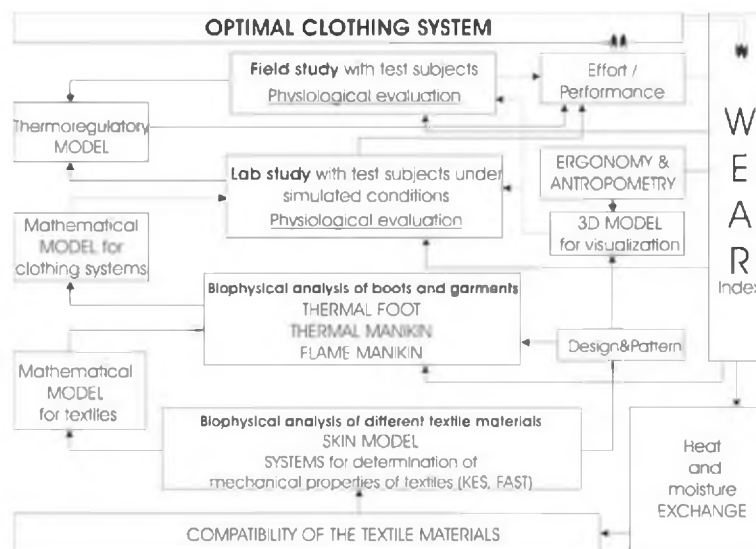


Figure 1: Model of development of the optimal clothing system

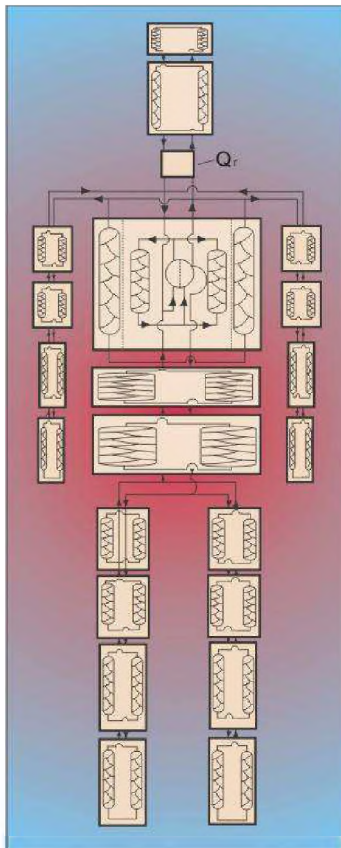
Regardless of how familiar we are with the properties of the particular protective material, the development process should start at the level of compatibility of the textile and non-textile materials (see Figure 1 [2]). Thermal properties of clothing depend on the physical properties (thickness, density, water vapor, evaporative resistance, thermal resistance) of fabric from which it is made, the fit which is affected by body posture and motion and environmental conditions (cold, heat, wind, snow, ice, radiation, nuclear and biological threats) [3].

Using a thermal manikin, the thermal (RT) and evaporative (RE) resistances of the investigated desert ensemble could be evaluated within different PPE combinations. In addition to the manikin tests, the heat strain induced by the five PPE combinations could further be evaluated by human subjects who will performed a predefined activity protocol (like guard duty, hiking, cycling, step tests) in simulated environmental conditions (like desert conditions with ambient temperature at 46.1 (0.2)°C and relative

humidity at 20.3 (1.5%) wearing several different PPE combinations. The main aim of such a development protocol is to investigate the significant added contribution of the NBC layer, helmet, bulletproof vest or a combination thereof to the overall thermal strain. The main concern in future development of desert garment ensembles is the NBC outer layer.

### Human thermal model

Thus, knowledge of high technology textile materials of basic physiology with in-built composites and is often not sufficient in the understanding of human thermoregulation while exposed to extreme environment. Sometimes additional textile layers are added to the overall clothing system with the aim to increase insulation and protection against environmental impacts. Consecutively, the thickness can decrease thermal balance and cause thermal overloading. It is very important to understand well the end users' requirement and the purpose of the personal protective equipment and afterward to choose an appropriate development protocol. One of the development possibilities is to investigate physiological responses of military personnel and to predict their thermoregulatory responses in advance using the Human Thermal Model developed by Prof. E.H.Wissler.



Human thermal models have been developed with several purposes in mind. One is to provide a theoretical framework for understanding human responses to exercise under various environmental conditions and another is to provide a rational basis for predicting human responses to exercise under various conditions. Clearly, the second objective depends on the first. Even though our understanding of important physiological phenomena remains incomplete, it seems to be sufficient to allow the use of modeling for predicting human response to stressful conditions; although a model should only be used for prediction after it has been adequately validated by comparison with the results of careful experimental studies. The model was used for some of the first predictions of expected survival time during accidental immersion in cold water [8]. Other applications were the prediction of expected survival time during a "lost bell" accident [9], analysis of performance while wearing a CBR garment [10] and analysis of astronaut performance during a spacewalk [11, 12].

The Model represents human geometry through 21 cylindrical elements as shown in Figure 2. In each major element temperature is computed as a function of time at fifteen points along twelve equally spaced radius vectors. Each cylindrical element is divided into 157 small regions defined by 15 cylindrical shells subdivided into 12 angular sections (see Figure 2 [4]).

Figure 2: Twenty-one element human model used in this study



Temperatures and physical and physiological properties such as density, specific heat, thermal conductivity, rate of metabolic heat generation and perfusion rate are computed for each of the 157 small regions. An additional 6 radial shells divided into 12 angular sections are used to define the properties of clothing on each major element. Longitudinal conduction of heat is neglected and transport of heat between major elements is affected by arterial and venous blood flow. The model makes allowance for counter-current heat transfer between arterial and venous blood in each element. An atlas of human anatomy [ 5 ] was used to position bone, brain, lung, viscera, muscle, fat and skin in each section and information regarding the distribution of bone, muscle and fat were obtained from the literature and used to place an appropriate amount of each material in each element. Regional thicknesses of subcutaneous fat is assigned according to gender and the mean skinfold thickness [6,7].

## Orientations

Nevertheless, as the personal protective clothing systems are developing, the heat transfer from a wearer to the environment at an appropriate rate during various work intensities in a range of environmental conditions must be carefully designed. Properties of a particular garment and of the overall clothing system can be measured in the laboratory using heated manikins, as presented in Figure 1, but those values are usually not sufficient to define how well the overall personal protective equipment will perform under field conditions. Mathematical human thermal models help to bridge the gap between laboratory studies and field performance, although their use only reduces the requirement for field trials; it does not completely eliminate the requirement. However, the demanding test of human performance in a field study provides a good opportunity to evaluate the human thermal model.

As seen through several researches in the field it is obvious that a numerical mathematical model is capable of providing useful results for different conditions, different environments and different activities. If one asks only how the subjects performed during the trial, the model provides the same answer as the experimental data subjects performed well. On the other hand, if one measures performance of the model in terms of agreement between computed and measured parameters (temperatures), there are differences that may or may not be significant depending on one's point-of view. Certainly, the difference between computed and measured parameters, especially during different activities, could be a concern, but the proper relationship between those parameters is not known with certainty.

However, the model can be used to analyze human performance under different conditions. It helps, for example, to define the differences between central and skin temperatures during different activities, and one might want to know how long a soldier could remain in one position without becoming hypothermic in a cold environment or becoming hyperthermic in a hot environment. Such questions can be answered through field trials and/or manikin tests, but it would be preferable to answer them through modeling, if possible. Several studies suggest that it should be possible to do so.



**Literature:**

- [1] Umbach K.H.: Physiological tests and evaluation models for the optimisation of the performance of protective clothing. In: *Environmental Ergonomics. Sustaining Human Performance in Harsh Environments*. Eds.: Mekjavic I.B., E.W. Banister and J.B. Morrison. Taylor & Francis: Philadelphia, (1987), pp. 139-161.
- [2] Zavec Pavlinic D. & Mekjavic I.B.: Potrebe okolja sooblikujejo bojne oblačilne sisteme, Revija Slovenska vojska, Oktober 2009, str. 29-31.
- [3] Zavec Pavlinic D., Wissler E. & Mekjavic I.B.: *Modeling thermophysiological responses of military personnel conducting a variety of activities during simulated field operations in a cold environment: presented at NATO Conference, HFM-168, "Soldiers in cold environments", 20-22 April, 2009, Helsinki, Finland. 2009.*
- [4] Qian, X. and J. Fan (2006). *Prediction of Clothing Thermal Insulation and Moisture Vapour Resistance of the Clothed Body Walking in Wind*. Ann. Occup. Hyg., Vol. 50, No. 8, pp. 833842.
- [5] Netter, F.H. (1989). Atlas of Human Anatomy. Ciba-Geigy Corp., Summit, New Jersey
- [6] Hayes, P.A., P.J. Soward, A. Belyavin, J.B. Cohen, and F.W. Smith (1988). Sub-cutaneous fat thickness measured by magnetic resonance imaging, ultrasound, and callipers. Med. Science in Sports and Exercise, Vol. 20, pp. 303-309
- [7] Hayes, P.A., J.B. Cohen, and P.J. Soward (1987), Subcutaneous fat distribution of adult males and females measured by nuclear magnetic resonance. IAM report No. 655, RAF Inst. Aviat. Med., Farnborough, Hampshire, UK
- [8] Wissler, E.H. (2003). Probability of survival during accidental immersion in cold water. Aviation Space Environmental Medicine Vol. 74: pp. 4755.
- [9] Haveland H.J. (1992). Evaluation of the NEWTSUIT ADS. SINTEF Report No. STF23 F92041, Trondheim, NO.
- [10] Peterson, D.J. (1983). Use of a mathematical model of the human thermoregulatory system in predicting tolerance times and supplementary cooling requirements for subjects in chemical-biological protective garments. Unpublished Master's thesis, the University of Texas at Austin.
- [11] Nyberg K.L., K.R. Diller, and E.H. Wissler (2000). Automatic control of thermal neutrality for space suit applications using a liquid cooling garment, Aviat., Space, and Environ. Med., Vol.71: pp. 904913.
- [12] Pisacane V.L., L.H. Kuznetz, J.S. Logan, J.B. Clark, and E.H. Wissler (2006). Thermoregulatory models of safety-for- flight issues for space operations. Acta Astronautica, Vol. 59: pp.531-546.

**Security Sector Reform**



## **Integration of Military Education Systems in Civil Society**

**Dr. Jelena Juvan**

Faculty of Social Sciences, University of Ljubljana Ljubljana, Republic of Slovenia

### **1 Introduction**

Due to the changing nature of warfare the armed forces of the future will require a much broader range of competences than their predecessors. New challenges and threats are arising every day. Different and more complex threats and challenges demand a different military professional of the 21st century than the one fighting in the World War II or in the small-scale armed conflicts during the Cold War.

New kinds of warfare as well as operations other than war (OTW) are changing the standards of military requirements and military education and training. This is not only a question of new equipment, command, control and communications structures or logistics. It is also very much a question of the skills and abilities of human beings (soldiers) working in a new technological and globally interconnected environment.

One example of these new challenges is knowledge based operations; they will accelerate operating tempos and decision-making processes in staffs. Success in this stressful environment will require leaders who are technically capable of fulfilling missions utilizing computer-based interconnected global networks. International missions are another example of the new complex challenges. Acting in multinational units and in cross-cultural contexts demands new skills and techniques. Dealing with several non-military actors (humanitarian organizations, NGOs,...) demands different kinds of skills and knowledge. Basic combat skills also require advanced competencies with technologies in order to perform better on the modern battlefield (Paile 2008).

New missions have changed the relationship between the military elites and the society. A new military officer has emerged from the post-Cold War era, with some OTW

entering his core competencies. Multilateralism, or at least international responsibility for peace preserving, keeping and maintaining proved that military officers were meant to serve also supranational purposes. In his/her professional career he or she may now face civilian participation in his/her mission and the use of civilian means. Within the specific European context, military officers are also called upon to deal with the growing integration of the Common Security and Defence Policy (Paile 2008). Challenges and issues a contemporary military officer is facing are enormous. Therefore, also military educational systems need to transform themselves in order to give as good results as possible, i.e. as skilled, trained and educated military personnel as possible.



## 2 Military profession

The end of the Cold War has brought about major political and security changes, which have had in addition to economic, demographic and socio-cultural changes a significant impact on the development of military organizations. Armed forces have been given new roles and tasks, which have consequently brought about the internal changes in their structure.

All of these changes have their own historical background and are inter-related, deriving from the nature of the perceived threats and key tasks of the armed forces (Moskos 2005, 314). "The postmodern military organization is characterized by its increasing permeability between the civilian and military environment, in organizational as well as in cultural terms" (Moskos 2005, 314).

The tasks of the armed forces are closely related to the understanding of the military profession. According to Abrahamsson (1972, 12) the military profession "is a group of technically and organizationally trained experts in the management of violence, connected with common educational and corporate practice and professional ethics". The military profession reflects the main purpose and role of a professional in a military organization. If the period until World War II was characterized by the role of an officer as a warrior - commander, the Cold War period was characterized by the role of an officer - manager and technician, and the postmodern period by the role of an officer - diplomat (Moskos 2000). Moskos' distinction of different types of officers reflects the different types of tasks and obligations officers have been facing.

The debate on the military profession is based on the distinction between officers as the most professionalized group in the military organization and lower ranking positions: soldiers/NCOs. A profession is typically represented by a group characterized by specific skills acquired during intensive training (Janowitz 1964:6). Skills required by the profession can't be obtained only in the apprenticeship system. General features and versatility of the military profession, regardless of time and space, are inherently intellectual and rely on the knowledge of their prior historical use. A professional is a member of the corporate association which manages the use of his/her abilities and carries a responsibility in performing his or her work. A professional group develops a sense of group identity and system of internal governance, which leads to the formation of ethical principles and performance standards (Janowitz 1964, 6).

For the members of a profession, several major characteristics can be identified:

1. Possession of a high degree of specialized theoretical knowledge, certain methods and plans to use that knowledge in everyday practice;
2. Performance of their duties according to ethical rules, code of conduct;
3. Sense of belonging together or connection with a high degree of corporativity, stemming from joint exercises and collective attachment to certain doctrines and methods. Educating future military officers.

Historically, the area of military education was focused exclusively on the training, while education was the subject of individual inspiration of persons who recognized the need for a deeper understanding of the nature and essence of the organization in which they were employed.

Pioneer work in the area of (self-) education and research has often experienced appropriate recognition only through later technological development and partly through changing social conditions, which resulted in increasing difficulty and complexity of the warfare, but has also indicated the need for a more educated staff.

This model was particularly established and developed from 1945 onwards, with the aim of deterrence and intimidation of opponents. In this model, which has particularly established itself in the UK, the French Republic, Federal Republic of Germany and the Russian Federation, a key role in the education of officers is given to the best internal (military) cadre, while civilian academic staff does not play an important role. This model is characteristic of a strategically stable period.

## 2 Model "Falklands"

The "Falklands" model is characterized by an environment that is strategically less stable. It is named after the Falklands War (1982), which was considered a surprise in terms of the event itself and development. The development of this educational model was influenced even more strongly by the fall of the Berlin Wall. This model is based on the premise that a military organization is not a closed system, that it is a part of the wider (civilian) environment and thus depends on its educational, economic and political content.

## 3 Model "Kosovo"<sup>1</sup>

The "Kosovo" model eliminates significant shortcomings of the previous model and aims to facilitate postgraduate study for all officers deemed intellectually capable for it. The main difference lies in the surrounding for the use of military force. It is more complex. This complexity is associated with the rapid changes that are politically and socially conditioned, borders between strategic and tactical environment being blurred and the extremely complex social environment. Officers are being educated in an academic environment. Study programs are accredited by the civilian universities.

Today, the new role of an officer - scientist and an officer- diplomat - puts before the military educational system several main key challenges:

- How to increase the analytical skills of officers to be able to understand the increasing complexity of the strategic environment;
- They will have to be trained to deal with a wider range of operations;
- They will have to learn to work in a gender, racially, culturally and religiously diverse environment.

---

<sup>1</sup> This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence. (In accordance with Arrangements regarding regional representation and cooperation.)



## SOURCES:

**Caforio, Giuseppe** (2006). Military Officer Education. In: Handbook of the Sociology of the Military. Ed. Giuseppe Caforio, 255-278. New York: Springer.

**Fajdiga, Patrik** (2008). Razvoj sodobnega vojaškega častnika /*Development of a contemporary military officer*. FDV, Ljubljana.

**Janowitz, Morris** (1964): The professional soldier: a social and political portrait. London, New York: The Free Press of Glencoe: Collier-Macmillan Limited.

**Moskos, Charles**. 2005. The postmodern military. In *Sodobno vojaštvo in družba*, ed. Anton Bebler, 313-322. Ljubljana: FDV.

**Paile, Sylvain**, 2008. "Towards a European understanding of academic education of the military officers?" Paper prepared for the annual congress of the *International Association for Military Pedagogy (IAMP)*, Helsinki, 19-23 May 2008.

**Rožanec, Miran**. 2011. Izobraževanje slovenskih častnikov - povezovanje javnega in vojaškega izobraževainega sistema /*Educating Slovene officers - connecting public and military educational system*. FDV, Ljubljana.

**Zabukovec, Stojan**. 2008. Razvoj nadaljevalnega vojaškega izobraževanja in usposabljanja častnikov SV in primerjava z nekaterimi tujimi izkušnjami /*Development of continuous military education and training in the Slovene Armed Forces and comparison with foreign experiences*. Bilten Slovenske vojske. 2008 - 10/ No. 1. 135 - 160. Generalštab SV.

**Žabkar, Anton**. 2008. Ahilovi peti sistema izobraževanja častnikov (razprava)/ The Achilles' heels of the education system for SAF officer candidates - a discussion. Bilten Slovenske vojske. 2008 (10/1), 131-134.



## Private Military and Security Companies in the Global War on Terrorism

Robert Mikac, PhD\*

Private military and security companies have never been involved in military operations on such a scale in recent modern history and such important state affairs as through their activities in the Global War on Terrorism. The wars in Afghanistan and Iraq as well as the need for engagement in other places have transformed private military and security companies from mostly logistical support to state security forces in the implementation of activities that are labelled inherently governmental functions, like direct participation in hostilities, intelligence operations, interrogation of prisoners of war and the protection of the highest-ranking political and military officials. The mentioned phenomenon raises many issues that are currently unanswered, concerning responsibilities, long-term profitability, transparency and accountability on both sides, regarding private military and security companies and also countries that engage them in the crisis areas of the world. The aim of this article is to show the area of engagement of private military and security companies in the Global War on Terrorism and the depth of their involvement in the inherently governmental functions of the United States of America.

### Key words:


Private military and security companies, Global War on Terrorism, inherently governmental functions, the United States of America, Afghanistan, Iraq

### Introduction

Shortly after the terrorist attack on the United States of America on September 11, 2001 the Global War on Terrorism (GWOT) was launched whose first goal was to overthrow the Taliban and to shatter the Al Qaeda in Afghanistan, and in the year 2003 to overthrow the Saddam Hussein regime in Iraq. Within the corps of allies involved in the so-called antiterrorist *Coalition of the willing*, a very large contribution from the first day was provided by private military and security companies (PMSC). The listed companies through the example of engagement in Afghanistan and Iraq radically changed the traditional role of the national state as the only protagonist of military activities and the main provider of security to its citizens. With their appearance the doors opened for competition but also a partnership in an area that until recently was the monopoly of the state institutions. For companies functioning according to the market principles the space opened for participation in security affairs recently attached to states, the kind of work we call inherently governmental functions. After the first few years of the war in Afghanistan and Iraq, PMSC staff accounted for more than half of all engaged allied human resources on both battlefields. On the GWOT platform they took part in other important

---

\* PhD Robert Mikac (robert.mikac@yahoo.com) is an explorer of subjects associated with contemporary security. He participated in NATO's ISAF mission in Afghanistan and has published two books: *Afghanistan: never ended conflict (2008)* and *Contemporary security and private security companies: the privatization of security and the consequences (2013)*. The views expressed in the article are the personal opinion of the author and cannot be associated with the views of any institution.



international operations (counterinsurgency, counter narcotics and anti-piracy activities) and all systems of national security of the U.S. and its closest allies. The impulse of such a state in the security arena is spreading to other states through the paradigm of the neo-liberal economy market, privatization revolution and handing over of yesterday's inherently governmental functions to the private sector, a model known as outsourcing.

Proponents of outsourcing point out that when certain functions from the field of national security are carried out by PMSC this helps bring about a certain acceleration, relief and update of important resources while opponents of this way of thinking and operating highlight the lack of transparency, questionable long-term profitability and effective responsibility for this policy. With time, the process of outsourcing in the field of inherently governmental functions has become a pragmatic solution, which is a sort of an opportunity and the question is how much is right. Thomas X. Hammes (retired U.S. Marine Brigadier) thinks that so far no one has systematically analyzed how much a PMSC involvement in conflict zones is strategically justified and what the long-term strategic consequences of their engagement (Hammes 2010) are.

However, PMSC' involvement in the field of security, especially in the fight against terrorism, is a part of the solution, but also a part of the problem. The aim of this paper is to show the extents to which PMSC are involved in inherently governmental functions of the largest military force in the history of mankind, U.S Armed Forces.

### **Strategic framework for private military and security companies' action in the USA security paradigm**

The private sector, whose integral parts are also PMSC is referred to in the U.S. strategic documents as an inherent element of national security architecture engaged to achieve goals and protection of national interests.<sup>1</sup> Somewhere this relationship is more, somewhere less expressed, but it is permanent and uncontested. Participation of the private sector as an integral part of the total U.S. power is much more strongly outlined in documents at the military doctrine level that specify the operational and tactical procedures and cooperation between all involved elements of the defense system, whose integral part is also the private sector.<sup>2</sup> James J. Carafano points out that the connection between the U.S. military forces and the private sector is also important because the U.S. military spends most of the U.S. resources intended for GWOT, and with that, from the year 2003 to the year 2008, the Pentagon has closed more than two million contracts with the private sector and about half of the Pentagon's budget is being spent on the payment of the private sector (Carafano 2008). The mentioned relationship between state institutions and the private sector, especially PMSC, is most clearly expressed by employing the latter in Afghanistan and Iraq.

---

<sup>1</sup> The National Security Strategy, 1997, 2002, 2006, 2010; The National Strategy for Homeland Security, 2002, 2007; The national counter-terrorism strategy, 2003, 2006, 2011; National Defence Strategy, 2005, 2008; The National Military Strategy, 2004; The Quadrennial Defense Review Report, 1997, 2001, 2006, 2010.

<sup>2</sup> Common regulation of the Armed forces and the Marine corps Field Manuals *FM 3-24 (MCWP 3-33.5), Counterinsurgency (2006)* and *FM 3-07 Stability Operations (2003 and 2008 versions)*, except the instructions and guidelines that provide, thoroughly process and point out cooperation with the private sector, for which it is stated that, when contracted, forms a part of the same system. PMSC company MPRI has written Field Manuals *Contractors on the Battlefield (FM 3-100.21)* and *Contracting Support on the Battlefield (FM 100-10-2)* for the purpose of U.S. military forces under contract with the U.S. Army Training and Doctrine Centre.

## Reasons for engagement of private military and security companies in the Global War on Terrorism


By launching Operation Enduring Freedom 2001 (Afghanistan) and Iraqi Freedom 2003 (Iraq) as part of the GWOT, the vast space of operations was opened which required an extraordinary human and financial potential. Since President Bush demanded a quick response, he did not leave too many options to U.S. Military Command regarding the strategic development of operations, cooperation with allies and ensuring logistical support. Although all members of NATO supported USA and for the first time in the history of the Alliance they activated Article 5 of Washington Treaty, they were not ready to accept large scales of operations and engagement, and it was questionable with how many military forces the members are ready to participate in the field. Therefore, the U.S. went into the formation of the so-called *Coalition of the willing* for attack on Afghanistan and Iraq. Among other things cooperation was offered to the private sector, and in particular PMSC.

Thomas P.M. Barnett says that in 1991 Americans forced Iraqis out of Kuwait with half a million soldiers, and that in 2003 they went with 240,000 - 250,000 troops to occupy Iraq (Barnett 2009). There is an obvious imbalance between the numbers of soldiers engaged in 1991 and 2003. Furthermore, with a much smaller number of soldiers operation Enduring Freedom in Afghanistan was launched. But time has shown that the strategic assessments of the architects of both operations about the required number of forces were wrong and greatly underestimated. Due to the insufficient number of "boots on the ground" on the part of the regular forces, the role of the private sector gained prominency with each year. Through time, in both operations, PMSC received, beside initial logistics services a greater role in the stabilization and reconstruction operations, as well as greater support in the war against terrorists and enemy forces.

Following the termination of conventional operations and initial illusion of stability the security situation in both countries soon deteriorated. The main war lever in both interventions was the fact that the U.S. military gained with time additional functions: establishment and maintaining of the security environment, supporting reconstructive operations and the construction and training of local security forces by reforming the security sector. As part of that kind of mission the U.S. military, apart from its strength, safeguarded also civilian professionals employed in the U.S. Department of Defence and the companies and their employees who are a direct support to combat units. Everyone else in the field, even if they belonged to U.S. government agencies or large American private corporations, could not count on the protection of the U.S. military. The security of their employees and projects was their own responsibility. This is where PMSC became prominent.

According to the United States Government Accountability Office there are two main reasons for the enormously increased demand for PMSC in the sector of security services provision and their operational capabilities in the field. The first reason is that the security situation on the ground has deteriorated so rapidly that all found themselves in great danger and should have protection. Another reason is the lack of preparation and lack of information about the security situation on the ground and that many private companies rushed into both countries guided by the possibility of enormous profits in reconstructive operations neglecting security requirements (Rebuilding Iraq..., 2005; Rebuilding Iraq..., 2006).

As the years passed, the number of hired private security companies and their employees constantly increased, and after a few years the number of regular forces grew. The Government Accountability Office transmitted data from the quarterly reports of the Department of Defense that in April 2008 in Afghanistan and Iraq worked a total of 197,718 contract partners (Contingency Contracting..., 2008) for the Department itself. A year later the U.S. Commission on Wartime Contracting in Iraq and



Afghanistan stated that more than 240,000 contract partners supported the work of the Department of Defense in Southwest Asia (including Afghanistan and Iraq). More than 80 percent of these are not citizens of the United States (At What Cost?..., 2009). These figures apply only to the U.S. Department of Defense, and it should be taken into consideration that a number of PMSC also work for other employers. Literally, both countries are networked by involving the private sector and their employees, and such a trend is present to this day.

### **Activities of private military and security companies in the field**

The tasks, roles and activities of the private sector and PMSC and the traditional military forces in the area of operations overlap mostly in reconstruction operations, maintenance of installations and their systems, transportation of most goods needed for the smooth functioning of war operations, physical security of important objects and people, security sector reform and, most controversially, in direct participation in hostilities. According to Moshe Schwartz in recent years in both operations the share of PMSC employees in certain jobs that they perform for the U.S. Department of Defense has stabilized. Most members of PMSC personnel are employed in support operations within and around military installations (as much as 65 percent) while work on security operations is carried out by more than 12 percent of those employed. Translators and interpreters make up 8 percent of all employed. On logistical and maintenance operations works almost 4 percent. On the construction business more than 2 percent. Around 2 percent deal with transport and 1 percent deals with communications and training of local forces. All others who do not fit into any of these categories equal 4,5 percent (Schwartz, 2010:8).

All previously mentioned tasks performed by PMSC in the area of operations (reconstruction and logistics operations, protective security operations, translation and interpretation, communication, transportation of almost all of the most important resources, training of local security forces) are the functions that were previously the functions performed by the regular forces. Regular forces and PMSC today sometime act together, sometimes - PMSC supports and complements the regular forces while in some functions such as transport almost completely independently performs this extremely important task of supplying all the allied forces in the field. Opinions differ about whether to leave the mentioned functions to PMSC. Professional societies lead a debate about how these functions are not inherently state tasks and, therefore, are suitable for PMSC which should perform these tasks with a lower cost equally well or even better. However, longer discussions are led when PMSC are involved in direct participation in hostilities, which is a central function, but also the role of a state power.<sup>3</sup> This concept is so attached to statehood obligations and responsibilities that assigning jobs from this domain to PMSC brings into question the very function of the state.

Among all the (various) companies and their mutually overlapping operations in the field, the Blackwater company (originally established under that name though later the company name was changed to Xe and then to Academi) is a particular example in that it serves as a role model of direct participation in hostilities with all sorts of imagineable implications. In a number of sources concerning the Blackwater participation in GWOT the following activities stand out: training of Afghanistan security forces and U.S. forces in the U.S., safeguarding of high-ranking persons and convoys, delivery of

---

<sup>3</sup> The most important activities of direct participation in hostilities include: combat activities, delivery of funds intended to cause losses to the opponent on the front line of conflict, physical protection of legitimate military targets, interrogation of prisoners, gathering of tactical intelligence information, maintenance of arms on the front line of the battlefield, management and guidance of means with which current damage or death of opponents is inflicted.

important resources to the field, safeguarding of the CIA base in Afghanistan, intelligence activities, the arming, launch and protection of unmanned aircraft designed to destroy opponents, combat engagements of a small scale, secret operations in Pakistan, finding and executing the members of Al Qaeda in Iraq, Afghanistan and Pakistan. All this is a direct challenge to the concept of statehood and the definition of a state which involves two postulates – a legal and a practical monopoly of the legitimate use of force within a given territory. The implications of direct participation of Blackwater in hostilities are numerous.

David Perry, in comparing his own attitudes with the contemplations of other authors points out that, apart from PMSC engagement alongside the military forces is a noticeable trend of its involvement also in the field of intelligence activities. Intelligence activities are the core of any counter-terrorist operation and, currently, the U.S. intelligence community spends more than 70 percent of its budget to pay external contract partners who make more than a quarter of the staff involved in intelligence activities. More than 25 percent of them are involved in the most important intelligence functions. He believes that "private participants currently have a larger role than governmental subjects in several aspects of U.S. counterterrorism activities" (Perry 2010:2-10).

## **The consequences of private military engagement and security companies in the Global War on Terrorism**

PMSC give a great contribution in the current GWOT. They have shown a willingness to follow, support, complement, but also to take responsibility in meeting national and international tasks in the field of national security. They have developed important skills and compensated abilities that regular forces are lacking and along with them they participate in meeting important national goals. In addition to numerous tasks in their own country, the most prominent feature is their role in Afghanistan and Iraq, where they are the first force on the ground based on the number of available forces. Most of America's political and military elite considers that support of PMSC reduces the defense costs and is a key "force multiplier" to achieve the goals of today's anti-terrorist activities.

Although thus the regular forces are disburdened of certain functions, dependence on PMSC is too big, which gradually takes over the performance of the functions that were previously under the jurisdiction of the state. Thereby the states themselves disable the supervision of the implementation of all phases of the war against terrorism, which can be very dangerous. Additionally, they lose institutional memory and operational capacity in certain areas. Furthermore, a lack of coordination between the regular and private forces has been recorded, both on the ground and in the preparatory phase.

In carrying out U.S. policy of international use of PMSC in GWOT (Afghanistan and Iraq) also the problem is that for many years they were exempt from legal authority and jurisdiction of the states in which they operated for them. Afghanistan and Iraqi government officials for years have tried to restrict and/or prohibit and/or put under their own jurisdiction the work of foreign companies, but due to the pressure from Washington D.C. they could not achieve that. The changes occurred during the years 2011 and 2012, but they are sporadic and not comprehensive. This practice is an international legal paradox and one reason more to explore the overall phenomenon of privatization in the field of national security.



## Conclusion

GWOT after more than ten years of duration proved to be extremely complex with an unpredictable ending. With all that was happening, the essential feature is that the PMSC has become an inherent part of this conflict. Since the capacities and resources of the regular security forces proved to be insufficient, assistance was sought from the PMSC. Thus, the U.S. decided to bridge the gap between the needs and opportunities and unload its security systems of those tasks which they considered that PMSC will fulfill more successfully and with fewer resources. PMSC in GWOT have been a part of the overall U.S. security architecture, became a force multiplier in the field and they complement the existing capabilities of U.S. military forces. The companies complete the tactical, operational and, sometimes, strategic needs of the U.S. By including PMSC in GWOT they endeavoured to reduce the gap between the strategic goals and prestressed potential of military and intelligence forces.

## Literature

**Barnett, P. M. Thomas** (2005) *Great Powers: America and the World After Bush*. New York: Penguin Group.

**Carafano, J. James** (2008) *Private Sector, Public Wars; Contractors in Combat Afghanistan, Iraq and Future Conflict*. Westport, Connecticut: Praeger Security International.

**Commission on Wartime Contracting in Iraq and Afghanistan** (2009) *At What Cost? Contingency Contracting In Iraq and Afghanistan*. Interim Report to Congress, June 2009, [http://www.wartimecontracting.gov/docs/CWC\\_Interim\\_Report\\_At\\_What\\_Cost\\_06-10-09.pdf](http://www.wartimecontracting.gov/docs/CWC_Interim_Report_At_What_Cost_06-10-09.pdf) (accessed September 27, 2010).

**Hammes, X. Thomas** (2010) *Private Contractors in Conflict Zones: The Good, the Bad, and the Strategic Impact*. National Defense University, Institute for National Strategic Studies, <http://www.ndu.edu/press/lib/pdf/StrForum/SF-260.pdf> (accessed November 19, 2010).

**Perry, David** (2010) *Blackwater vs. Bin Laden: PMCS involvement in American Counter-Terrorism*. Canadian Political Science Association Annual Convention, June 2010, Montreal, <http://www.cpsa-acsp.ca/papers-2010/Perry.pdf> (accessed March 1, 2012).

**Schwartz, Moshe** (2010) *Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis*. Congressional Research Service, July 2, 2010, R40764, <http://www.fas.org/sgp/crs/natsec/R40764.pdf> (accessed July 30, 2010).

**United States Government Accountability Office** (2005) *Rebuilding Iraq: Actions Needed to Improve Use of Private Security Providers*, <http://www.gao.gov/new.items/d05737.pdf> (accessed June 8, 2009).

**United States Government Accountability Office** (2006) *Rebuilding Iraq: Actions Still Needed to Improve Use of Private Security Providers*, <http://www.gao.gov/new.items/d06865t.pdf> (accessed August 3, 2009).

**United States Government Accountability Office** (2008) *Contingency Contracting: DOD, State, and USAID Contract and Contractor Personnel in Iraq and Afghanistan*, <http://www.gao.gov/new.items/d0919.pdf> (accessed August 4, 2009).

## **The Importance of Regional Cooperation in the Field of Military Education as Support to Confidence and Security Building Measures in SEE**

Col Goran Dikic, University of Defence in Belgrade, Republic of Serbia

Confidence and security building measures have been defined by many authors as the actions taken to reduce any kind of conflict situation. This term has been appearing frequently in reports and documents regarding the period of the Cold War. Politicians, conscious of the threats caused by the existence of nuclear arms, have been trying to do something with the intention to avoid any kind of conflict initialized by misunderstanding or lack of communication and accidental errors in systems for early warning. They established a "hot line" among governments to prevent terrible consequences of nuclear conflict but, in real life, it was not enough. More conferences were organized and several agreements were accepted and, finally, some of those weapons had to be destroyed.

Considering the definition mentioned above, it can be said that people always have been trying to apply some kind of confidence and security building measures in conflict and post-conflict situations during history around the world. Firstly, the situation can be recognized when conflicting parties are interested in overcoming problems during the conflict, that are bad enough for each side. Sometimes, local leaders succeed to establish a temporary agreement, but as a rule, one side breaks the promise and the conflict continues. Unfortunately, they usually need the help of the international community to stop the conflict and find an acceptable solution. Practicing international diplomacy and the participation of the peacekeeping troops is the logical mosaic of events that follow that situation. All participants, soldiers and civilians feel the consequences of these conflicts for a long time.


One of the most important results of international cooperation must be sustainable peace among the people in any region in the world. Bearing in mind the history of the world, we could easily get disappointed in this regard. Fortunately, people are always healthy-minded and optimistic when trying to find new solutions for a better society. As is known, RACVIAC was established in 2000 as the Regional Arms Control Verification and Implementation Assistance Centre with an aim to provide arms control training, promote confidence and security building measures and broaden cooperation in South-Eastern Europe (SEE).

Many ideas were analyzed and serious discussions were realized with the intention to establish peaceful coexistence in the world but now our focus will be on trying to consider ways of building confidence and security in our region - SEE- through cooperation in the field of military education.

In December 2013, the first meeting of the chiefs of military educational institutions in the region was held at the Central Club of the Serbian Armed Forces in Belgrade. The aim of the meeting, which was attended by the representatives of the Republic of Serbia, Montenegro, Republic of Croatia, Bosnia and Herzegovina, Republic of Slovenia and the Former Yugoslav Republic of Macedonia<sup>1</sup>, as well as

---

<sup>1</sup> Turkey recognizes the Republic of Macedonia with its constitutional name



the Norwegian and British defence envoys was to define a model for enhancing regional cooperation in the field of military education.

Considering the existence of the relevant agreements between the governments in the region, cooperation in military education can be established in numerous ways. The list of possible forms of cooperation could consist of:

**1. Courses organized on a local level** with the intention to provide well-trained personnel for special tasks in the frame of local and international cooperation. It assumes the exchange of soldiers, students, officers as well as instructors.

**2. Courses organized through the support of the international organizations**, such as the NATO Partnership for Peace consortium. For example, one of them was organized in 2013 in the Republic of Ukraine and tackled the problems what to teach students and how to teach them. The next the Multi-National Defense Educators Workshop- was organized in April 2014 at the Military Academy in Belgrade. This is only a small part of the activities organized in the frame of the Defence Education Enhancement Program (DEEP) that is being organized for several countries. Last autumn we had a meeting with a NATO team of renowned international experts. One of the main topics during this meeting was the balance between the Bologna rules and the requirements of military education.

**3. The joint exercises** represent a fruitful form of training with multiplied effects. On the one side, there is joint personnel which needs to prepare the activities, work together in appropriate headquarters and participants who have to achieve defined goals with colleagues from other armed forces. On the other hand, they do the preparations under different conditions, in their units. After that, they collaborate with nonnative speakers, in real time, in situations very similar to the conditions during the international missions. Of course, it is more than training. The soldiers meet each other. They exchange experiences and learn from other teams in concrete situations. It is a good opportunity to learn more and exchange experiences about:

- the importance of the joint patrols;
- the organization of the observation posts during the missions in peacekeeping operations,
- preparation for the task at the time of patrols;
- the organization of support in emergency situations;
- how to organize communications in order to enable that monitoring units recognize the situations when they need support without direct request for engagement of quick response forces, etc.

**4. Exchanging personnel as students or instructors at military academies, military schools and war colleges.** In some ways, this is the most important form of cooperation. The explanation is very simple. They are or they will be the leaders in concrete situations. Bearing in mind the differences among programs in military academies it is not easy to organize mobility of students but short time exchange of cadets and participation in smaller exercises can be achieved. It also involves student weeks when students have more opportunities to meet their colleagues and know better other countries and their academies.



In January 2012 at the University of Defence in Belgrade we launched the Advanced Security and Defence Studies. It is a new organizational unit of the National Defence School, organized as the fourth, highest level of career professional development provided for the military officers and civil servants of the Ministry of Defence. It is also attended by high-ranking officials of other ministries and agencies of the Government of the Republic of Serbia and other states in the region. The studies last twenty one weeks.

The main goal of the Advanced Security and Defence Studies is the education and preparation of participants from the Republic of Serbia and the countries of our region for assuming the highest duties in the national defence system. The focus is on enabling the participants to:

- a) analyze the contemporary security environment using a multidisciplinary approach
- b) assess long-term political and security trends
- c) develop elements of national security policy
- d) cooperate with other national security systems at the regional and global level

The good practice that foreign officers participate in higher levels of military education has been established at our university (the Command Staff Course, the General Staff Course and the Advanced Study of Security and Defence). In addition, our officers are also educated in higher military education institutions in other countries.


Every year, groups of foreign officers visit our university during their study trips. We organize similar activities for our officers in accordance with the appropriate agreements between our MOD and other MODs. For example, the second class of participants in Advanced Security and Defence Studies (ASDS) visited Brussels from 25 February to 1st March 2013. Staying in the Belgian capital enabled the participants to comprehend the scope and the current tasks of organizational entities of the EU and NATO responsible for the civilian and military aspects of security and the role of diplomatic missions of the Republic of Serbia and the countries in the region working in Brussels. Up to today, the ASDS was completed by forty two participants. The first three classes consisted of twenty civilian officials of the Republic of Serbia (RS), one state representative from the Former Yugoslav Republic of Macedonia<sup>2</sup>, seven officers from the countries of the region (2 from HR, 4 from BA and 1 from SI) and 14 SAF officers. Now, in the fourth class, we have a similar situation. Only four among fifteen participants are the officers of SAF, one is an officer from BA, one is from the Former Yugoslav Republic of Macedonia<sup>3</sup>, one from the Republic of Algeria, one is a civilian representative from BA and others represent RS (six of them are from the ministries of RS and one is a representative of TV Serbia).

**5. Joint projects and publishing of papers:** The Science for Peace and Security Program, originally founded as the NATO Science Program in the 1950s, now offers grants for collaboration projects, workshops and training involving scientists from NATO member states and partner countries.

---

<sup>2</sup> Turkey recognizes the Republic of Macedonia with its constitutional name

<sup>3</sup> Turkey recognizes the Republic of Macedonia with its constitutional name



**6. Participation in Europe Defence Projects:** Catherine Ashton, at the time the High Representative of the Union for Foreign Affairs and Security Policy and Head of the European Defence Agency (EDA) and Nebojša Rodić, former Serbian Minister of Defence, signed an Administrative Arrangement between the EDA and the Serbian Ministry of Defence in December 2013. The Administrative Arrangement formalizes the relationship between EDA and the Republic of Serbia, enabling Serbia's potential participation in EDA's projects and programs. Cooperative areas remain to be further defined, but Research & Technology and training are examples of possible areas of cooperation. For example, our lecturers are engaged, together with the University in Belgrade, in a project funded by the Serbian Ministry of Education, Science and Technological Development. We are awaiting to become involved in some of the EDA projects at the moment.

**7. Activities regarding the competitions involving military athletic teams.** The military academy has celebrated 10 years of membership in the International Council for Military Sports (CISM). For example, we can offer some kind of joint training or organization of competitions during the winter in our ski-center on the Kopaonik mountain.

Many activities could be organized using new technologies. Bearing in mind the solutions such as the advance distance learning systems, lectures via the video link, we can say: „**The door of knowledge has never been more open than today**”.

**What should we say in conclusion?** Confidence building measures is not a simple list of tasks or our wishes. It is a multidimensional process and every element of the community has its own specific role in that process. The contribution of every individual as well as organizations will offer positive results in a global sense only through joint activities, well supported by the governments in a concrete region. Cooperation among armed forces represents a valuable form of verification of the efforts done by a certain society with the intention to improve the confidence among neighboring countries. Considering the role of the armed forces, we could say that successful cooperation among these parts of the society represents a significant indicator of well established relations as well as a high level of confidence among countries.

In general, we could conclude that cooperation in the process of military education offers a cheaper process of education (a unique group, at the same time, at the same place, with the best lecturers from the region), the opportunity to learn from each other and a lot more. Using the headline form maybe it would be most suitable to say: "**More confidence among the countries in the region equals more readiness for new challenges**".

## Europeanising the Initial Officers' Education: Some Challenges, Many Opportunities

By Sylvain Paile-Calvo, Senior Researcher, University of Liège, Belgium


The profession of a military officer is in fact, and necessarily so, one of the most “internationally-oriented”. The *raison d'être* of the military professions in general is international. The classical mission of the armed forces - *i.e.* defending the national territory - implies a certain degree of openness to the potential enemy(ies)' ways of thinking and acting. This requirement is even stronger with regard to modern or “new” missions. International operations involving a deployment of armed forces are now multilateral in most cases. Multilateralism, implying a virtual philosophy of acting in concert, is sometimes substituted by a sort of “multilaterality” where involvement is more pragmatic, as was the case in Iraq in 2003, in Libya in 2011 or, in general, in the CSDP military operations, such as the EUFOR RCA launched in 2014 in the Central African Republic. Nonetheless, it is a fact that States no longer engage alone in operations to maintain or restore peace, no matter what their political weight is and the size of their armed forces. The reason certainly lies in the fact that, especially in times of economic crisis, defence budgets are being downsized and can no longer support intervention that may involve rebuilding State infrastructures and, therefore, be lengthy and costly. Furthermore, modern societies no longer accept, or at least much less readily, the sacrifice made by their soldiers on missions not regarded as vital for the Nation<sup>1</sup>. Lastly, it could be argued that this multinationalisation of operations is also the result of participation in the case of United Nations operations, by “new” States from all continents; States which, before the fall of the Berlin Wall, did not traditionally take part in conflicts and which now wish to flex their muscles in a multipolar world.

Becoming a serviceman implies, therefore, the acceptance of these challenges, the individual adaptation to these challenges and always keeping an eye on the evolution of his/her environment. This need is even stronger at the officers' level since they are meant to become leaders and chiefs, commanding units and deciding on the conduct of the operations, in headquarters or in the battlefields. Any education on the operational and strategic level, in the 21st century, must include a high degree of openness to international facts and cultures. This is verified in the everyday work and life of a young European officer. In many European Member States young officers must participate, in the years following their commissioning, in a military operation abroad.

The threats - like economy and, somehow, culture - are now globalized. Instability in one region of the world brings insecurity everywhere in the world. Security, therefore, is also globalized and requires global actions. Owing to their history, their weight in the conduct of the world's political and economic affairs and their cultures, the European States play a major role in-maintaining and enforcing peace in the world and they may be brought to use either military or civilian force, if allowed to under international law, when diplomatic solutions have failed. The geographical scope of the European armed forces' action, since the fall of the Iron Curtain, is worldwide. In the framework of the European Union, since the Saint-Malo summit in 1998, the Member States commit themselves to increase the integration of their security and defence policies through the Common Security and Defence Policy, as a part of the Common Foreign and Security Policy of the Union. The governance and conduct of this

---

<sup>1</sup> Read, for example: André Dumoulin, “Le zero-mort, le moindre mort: vers une assimilation européenne?”, *Revue du Marché Commun et de l'Union Européenne*, No. 469, 2003, pp. 354-364.



policy, and the military affairs thereof, remain submitted to the principle of sovereignty of the States<sup>2</sup>. Specifically, any initiative under the CSDP umbrella must be unanimously agreed upon. In fact, the latter ones have clearly demonstrated their will, during the first years of existence, for a greater coordination and collaboration in defence-related issues such as the definition of the threats or the creation of multinational capacities and capabilities. The Lisbon Treaty, which came into force in 2010, pushed forward the coordination of the European external action and the rapid evolution of the CSDP observed since 1998 and will certainly maintain its pace and dynamics in the future. The EU's response to globalized threats is not only coordinated. It is also comprehensive<sup>3</sup>. The CSDP, indeed, is not only concerned with military response to threats but also with civilian tools. In fact, most of the missions and operations led by the European Union in the framework of CSDP use civilian "forces", possibly combined with military ones and the classical image of the military officer as merely the leader of conflict resolution on the field needs to be revised. The CSDP is a "toolbox" for the response to the modern threats with modern instruments and it requires from the Member States to train their soldiers for being interoperable. It is fundamental, therefore, that the future military elites are familiarized, educated and trained in accordance with this reality of their profession as early as possible in their military career.

This adaptation is also an obligation during the officers' initial education and training. Punctually, after managing a crisis, it is necessary to draw lessons or, more regularly, to anticipate the crisis situations and adapt to the realities of the battlefield. A disconnection from the "civilian world" and the public opinion could be observed at the end of the Cold War. The defensive role of the armed forces in the event of an invasion was challenged and so was the overall consideration of their role in general. The status of the military officers in the society, seen in the past as the "guardians" of the European sovereignty, was also questioned. The military elites, due to the fact that their training did not match certain "intellectual standards", were decreasingly being recognised and accepted as "societal elites". In parallel with these historical and social changes a historical and political one also occurred. As the direct threat of an invasion faded, the European States started downsizing their armed forces' manpower. In the mid-1990s, the servicemen - officers foremost - began to face issues of the perspective of their re-conversion on the civilian labour market. Their qualifications, too rarely sanctioned by diplomas, were not recognised by the civilian sector. The recovery of their prestige and legitimacy as elites, therefore, had to go through a modernisation and internationalisation of their education and training even at the initial level, when the values of "working together" can be first spread.

In order to prepare their future military elites to these realities and challenges in their duties, most of the responsible education and training institutions made the choice of exchanging military students and/or staff. Exchanges, indeed, are assumed to the benefit of all actors of European security and defence. The future officer or the member of the scientific, academic or managerial member of staff is expected to open his or her mind to new cultures and to acquire new knowledge and know-how that is not-or, in a different way-available in the national curricula. The sending institution undoubtedly profits from these gains acquired by their individual "ambassadors". The host institutions presumably profit from these exchanges to increase their visibility as elite institutions and promote the excellence of their education and training. Since the institutions are necessarily closely related to the armed forces

---

<sup>2</sup> See: Treaty on the European Union as amended by the Lisbon Treaty, Chapter 2, Section 2 "Provisions on the Common Security and Defence Policy".

<sup>3</sup> The literature that theorised the concept of the "comprehensive approach" is numerous. For example, see: Nicoletta Pirozzi, "The EU's Comprehensive Approach to Crisis Management", Brussels, EU Crisis Management Paper Series, Geneva Centre for the Democratic Control of the Armed Forces, June 2013.

themselves, their exchanges have also a diplomatic dimension, which benefits the reputation of the States parties to the exchanges. And, at a macro level, the international security and defence organisations - or coalitions - such as the European Union through the CSDP, are assumed to benefit from this apprenticeship of interoperability on the part of the future leaders of their contingents, the future decision makers in capitals or in headquarters, with a more senior perspective.


Real policies for enhancing the international and European, first and foremost, mobility of knowledge and know-how, were thus developed as early as the 2000s by the European military higher education institutions, with the view to engage in mutual exchange and/or with their civilian counterparts. It quickly became evident that the efforts to harmonise the systems with a view to make them "compatible" for exchanges as well as the efforts to facilitate mobility were needed. The military higher education was entitled to use the instruments originally created in the civilian area but intended to be used by the entire system of higher education.

These instruments could be divided into two categories. In the first place, the higher education institutions, including the military ones, were invited to adopt measures aimed at making their education and/or training compatible, though not standardised. The Bologna Declaration of 1999 and the Process it initiated progressively and successfully led to the creation and reinforcement of the European Higher Education Area. Complementarily, all higher education institutions that were recognised as such on the European level were granted access to programmes and financial support giving them the opportunity to develop their exchanges of students and staff. The Erasmus programme of the European Union is the most famous example and its success has been impressive in developing the mobility of the civilian higher education area. The officers' basic education and training institutes were, already at the time of their creations, entitled to benefit from the *acquis* of these two different types of measures. However, it rapidly became necessary to create - additionally, but not alternatively - military-specific instruments with the view to allow these institutions benefiting from the progresses reached through the civilian instruments. The "military specificity" of the military higher education, i.e. the fact that the students are also cadets with military obligations and that their education and training institutes have only one "customer", i.e. the national Armed Forces, quickly became an obstacle to the free mobility of knowledge and know-how through the exchanges of students. The military institutes had set practices of mobility on an ad hoc basis. Before 2008 already, for example, some academies used to meet in individual service *fora* outside the CSDP context and started engaging in mutual exchange. However, the exchanges between the military institutions in general were rare or poor, i.e. they were limited to formal visits not involving real exchanges of knowledge or know-how.

In 2008, the European initiative for the exchange of young officers, inspired by Erasmus (hereafter the "Initiative"), was launched and proposed to all European Union Member States and their institutions from all services. It is specifically designed, in the framework of the European Union, for making young officers in their basic education and training familiar with the role they are expected to play in the future European common defence. This initiative was the first of its kind to be launched within an international organisation and builds upon the foundations of existing basic education and training systems, their institutions, and on their respective individual and collective achievements. The Ministerial Declaration<sup>4</sup> that founds the Initiative expressly provides that it should develop interoperability in initial

---

<sup>4</sup> Council conclusions on the ESDP, *Statement on the European Young Officers Exchange Scheme, Modelled on Erasmus*, Brussels, 10 and 11 November 2008



officers' training, with due regard for specific national characteristics and traditions. The measures recommended should therefore not be seen as an attempt to standardise curricula, but only as a way of reducing the differences that might impede the mobility of students and teaching staff. Three avenues were singled out to achieve this goal.

The first part of the recommendations deals with measures to be taken at the European level. Measures common to both academic and vocational training include comparing the required skills of cadets in the national curricula, creating a database containing the curricula of military colleges and offers of and requests for places for exchanges and identifying obstacles to these exchanges. On the more specifically academic aspects, the Declaration recommends developing training modules on the CSDP and international security-related issues to be made available to military institutions and facilitating access to internet-based distance learning in order to expand the range of courses offered by the institutions, notably in the field of CSDP education. The Declaration also calls for the development of credit transfer systems, such as the ECTS, along the lines of what is offered in academic education and mechanisms for stimulating exchanges in military vocational training.

The second part of the recommendations concerns the Member States and their military institutions. They mainly relate to the implementation of the Bologna Process: Member States are asked to make full use of the instruments and measures offered by the Process and to fully recognise the education received in other Member States. Moreover, they are asked to encourage the mobility of students and teaching staff and to promote the teaching of foreign languages and the learning of two foreign languages within the institutions.

Quickly after the Declaration the participating European Union Member States, their institutions and the European Security and Defence College, meeting in an implementation group, started working on "quick wins", consisting of a Common Security and Defence Policy and other common thematic modules specifically designed for addressing a cadet audience, the creation of a platform of communication and information<sup>5</sup> and the adoption of a Framework Agreement aimed at facilitating the use of existing mobility programmes such as Erasmus - by military educational institutions and to create additional opportunities for short-term exchanges. This model agreement takes into consideration exchanges between institutes, the specific nature of the military, such as discipline, the responsibilities of hosting or the right to carry weapons, and it complements the agreements concluded by partner institution exchanges.

Following in-depth scientific investigations into European military higher education<sup>6</sup> the Implementation Group established a new set of "lines of development" for its efforts to achieve unimpeded mobility. These lines implement or supplement the measures expressly set out in the Ministerial Declaration. The Implementation Group first emphasised the need to create a system of credits to recognise the outcomes of officers' vocational training exchanges, even though practices differing from one Member State to another or from one institution to another. A working group issued intermediary guidance for such recognition, based on the cadets' workload<sup>7</sup>. The long-term aim, however, is to standardise the use of a regular credit system, such as the ECTS, which encourages consideration of training outcomes as a second, additional factor to workload. Another line of

---

<sup>5</sup> At the following web address: [www.emilyo.eu/](http://www.emilyo.eu/).

<sup>6</sup> Sylvain Paile, *European Military Higher Education Stocktaking Report*, Brussels, Council of the European Union DG F Press, May 2010.

<sup>7</sup> Harald Gell, *Users' Guide for Workloads' Calculation of Non-Academic Basic Officer Education*. Available: [www.emilyo.eu](http://www.emilyo.eu).

# COMPENDIUM 2015

development was to define the qualifications offered by military education and training and their operational implementation in terms of learning outcomes. To allow a comparison between the different curricula of potential partners, a common European vocabulary to describe the desired results of the basic education and training was needed. This instrument of common understanding will take the form of a sectorial "basic officers' education and training" qualification framework. The Implementation Group also converted the database on the initiative's website into an actual platform of information on education systems, institutions and their education and mobility policies. This platform is meant to become an important instrument for the day-to-day development of the exchanges and for information on European military higher education. In order to promote efforts to remove obstacles to mobility, obtain the maximum political and operational support, and match the supply of and demand for exchanges, the initiative itself needed to be publicised. Steps have been taken to promote the initiative in public through the media and to target experts and practitioners in the field of military mobility through specific actions. A newsletter was created for distribution to military institutes and a compendium was drawn up to provide information on the different military higher education systems that exist in Europe<sup>8</sup>. Working groups also meet and investigate the best use of existing mobility programmes in the European higher education system and what administrative support is needed for the practical implementation of exchanges, within or outside these programmes. Meanwhile, common curricula on issues of mutual interest to Europe's armed forces are being developed and new teaching materials are continually being produced. National institutes also regularly open up, or adapt, their existing learning modules to European participation.

After a six year run and achievement of positive results in providing national systems with an adequate ground for the development of their exchanges, the initiative has proved to be the framework of reference for the European integration of military higher education. It successfully promoted to the military higher education the potential and benefits of Europeanisation in order to be recognised as delivering excellence in education and training. It allowed the establishing of communication channels- and sometimes even "bridges"-between actors in military education and training. It allowed bringing closer, through "harmonising without standardising", of the military education and training cultures, policies and mechanisms in encouraging the implementation of compatibility measures based, notably, on the Bologna Process. And, subsequently, it permitted the direct increase in the number and quality of the exchanges between the European military officers' basic education and training systems and institutions.

Its actors, nonetheless, constantly seek to identify the ways forward in the development of mobility and to cope with the challenges they meet. The European improvement of mobility of knowledge and know-how, indeed, is a commitment that must be sustained by the involvement of the States, notably as regards the political and financial aspects, their institutes, notably as regards the recognition of the values of an exchange for the curriculum of a future military elite and of the cadets themselves. The Europeanisation of the future officers' initial education and training, in this regard, is a renewed challenge and process that is animated by the opportunity to set the most solid foundations for the security and defence of Europe of tomorrow.

---

<sup>8</sup> Sylvain Paile (Ed.), *Europe for the Future Officers, Officers for the Future Europe Compendium of the European Military Officers' Basic Education*, Polish Ministry of National Defence, Department of Science and Military Education, Warsaw, September 2011, p. 226.



## **Future Perspectives of Military Education, 21<sup>ST</sup> Century Challenges - Regional Aspect (SEE)**

Associate professor **Metodi Hadzi-Janev**, Colonel  
Military Academy "General Mihailo Apostolski Skopje",  
University "Goce Delcev" - Stip  
E-mail: metodi.hadzi-janev@ugd.edu.mk

**Keywords:** military education, doctrine, training, operational environment, political and security environment, planning and execution

### **Abstract**

The end of the Cold War brought significant changes into the political and security realm. These changes, among others, have affected the operational environment. Non-state actors with malicious agendas have started to pose asymmetric and unconventional threats. To counter these threats the South East European (SEE) countries' military forces need to adapt. Although training and doctrine adjustments are necessary without proper education the SEE military will fail to accomplish political leadership's vision and end-state. Therefore, the article explains how changes in geopolitical landscape affect employment of SEE military as an instrument of national power. Then, it discusses why education should be a platform for doctrine and training development and why doctrine and training alone could produce just short-term solutions. Finally, it provides some recommendations for future SEE political and military leadership that need to be considered while building curriculum for military education.

### **Introduction**

The international political and security environment after the Cold War has drastically changed. Many of the existing security concepts designed to maintain peace and security in the new security and political realm have little value. At the same time, the intensified process of globalization and the technological boom have empowered new non-state actors. Thanks to the new environment and technological development groups and individuals that use terrorism gained power to accomplish a strategic end. Thus, the changed security and political landscape, the intensified process of globalization and technological development with all of their benefits and negative influence and the rise of the new non-state actors with strategic and global ambitions have changed the operational environment.

Consequently, these dynamics have urged changes in employing the military as an instrument of national power. The new role of the military focused on solving political problems from warfare to "peace-fare" starting - to echo the idea of collective security sponsored by the UN's and NATO's vision to maintain peace and security around the globe. Hence, the new requirements by the political leaders unequivocally push military leaders to reconsider existing concepts of warfare and to produce adequate doctrine that will accomplish political ends. However, so far, from practice we learn that to achieve these requirements is not an easy process.

It is common wisdom that traditional processes of adaptation, i.e., changing and improving the training and doctrine should produce military actions that will be in line with-political guidance and the



end-state. Nevertheless, the experience from Afghanistan and Iraq for example attests quite the opposite. According to numerous military scholars, warriors and experts, the armed forces accomplished a military end-state. They have removed the Taliban regime, destroyed what was called the physical structures of Al Qaeda and toppled the Saddam regime in Iraq. Furthermore, after a decade of military engagement, changed doctrines and adjusted training on the lessons learned, military actions on the ground failed to produce envisioned progress and accomplish the political end-state. Therefore, the article argues that in order to be able to give better advice and accomplish political guidance, produce adequate plans and execute them on the ground, the armed forces must focus on military education. In fact, training and doctrine alone could not produce novel solutions, something that is required of modern warriors.

South East European countries have so far participated in these operations in one or another way. At the same time, these countries are a part of the globalized and changing military culture shaped by the Euro-Atlantic integrations. Therefore, this debate is relevant for their armed forces too. Given that most of these countries share the common history and similar culture and values the article will address specific SEE challenges in this context. Finally, the article will provide some solutions that SEE military and political leaders should consider if they are about to successfully and smartly build and employ their armed forces as an instrument of national power and contribute to the regional and world peace and security.

## 1. Understanding the changes in the geopolitical environment and security trends

The political and security environments have changed. As some have argued we no longer have the luxury of commodity under the walls<sup>1</sup>. The world we leave behind is smaller and faster for human beings and their political systems<sup>2</sup>. These changes have shaken the world and challenged previously established security and political concepts that have held the international system stable.

Thanks to the globalization and technological development many non-state actors (corporate, groups and individuals) but also some states have gained strategic power. As a result new security threats are hybrid, composed of criminals, terrorists, insurgents, religious extremists and some states. Hence, one could argue that the modern understanding of security among others depends on states' political system; economic development (social stability), cultural perspectives (religion, traditions, history, beliefs, customs, traditions and personal perception of belonging), scientific development (technological advances) and environment and the influence from and on the environment. This argument is perhaps best supported by professor Seyom Brown's observation about the re-conceptualization of security. He argues that these changes are two-dimensional, i.e. broadening changes (nonmilitary security threats) and deepening direction, i.e. consideration of the security of individuals and groups<sup>3</sup>.


This idea of the new approach to security has also been recognized by the UN and has culminated in the Report of the High-level Panel on Threats. Phrases such as: "[I]n today's world, a threat to one is a threat to all...; ...Every State requires international cooperation to make it secure... Meeting the challenge of today's threats means getting serious about prevention...", attest that the political and

---

<sup>1</sup> John J. Mearsheimer, "Why we will soon miss the Cold War", August 1990, The Atlantic online, retrieved from <https://www.theatlantic.com/past/politics/foreign/mearsh.htm>

<sup>2</sup> Thomas L. Friedman, *The World Is Flat. A Brief History of the Twenty-first Century*, Farrar, Straus & Giroux, 2005, p. xx

<sup>3</sup> Seyom Brown, "World Interests and Changing Dimensions of Security", in Michael Klare and Yogesh Chandrani (eds), *World Security: Challenges for a New Century*, 1994, New York: St. Martin's, p. 1-17



security reality has changed<sup>4</sup>. Accordingly, the modern understanding of security is tidily connected to world peace and security. The practice shows that the UN and NATO have a leading role in enforcing collective peace and security, but also building it, i.e., acting in the post-conflict environment. Nevertheless, under the changed reality the contemporary post-conflict operational environment is full of asymmetric threats posed by non-state actors. These actors have their own agenda or act as a states' proxies. As Charles C. Krulak, a US Marine General puts it: *"The future warriors must be ready to answer the Three Block War challenge, an increasingly important arena of military operations characterized by engagement with hostile, neutral and friendly forces, all at the same time, in a very geographically limited area, e.g., three blocks"*.<sup>5</sup>

Although many have recognized these changes and have also recognized that the new operational environment has radically changed the military wisdom did not follow. The training and doctrine adjustments were largely focused in a linear fashion driven by technological dynamics such as greater firepower, better stealth, better digitalization, more efficient logistics, network centric warfare and the ability to deliver high-tech "Shock and awe". Furthermore, instead of education, the focus was on training and doctrine. Although it could be argued that training and doctrine adjustment are necessary it could also be argued that without proper education future warriors who should win the peace will fail to recognize the threats that stem from the changed security reality and operational environment. Given that SEE countries are a part of these global dynamics the following debate has significant relevance for the military and political leaders in SEE.

## 2. Challenges to Military education - the training and doctrine vs. education dilemma in context

The "problem solving" through the military "periscope" has developed over time a culture where military wisdom's approach to warfare is twofold: doctrine and training. So, when a change is needed the military puts faith in these tools as the means for re-orientation. Following this approach John Kiszely, paraphrasing Huntington observes that the Military developed the so called "Professional monastery". This, according to him "inhibits outside of the box thinking" and creates default reactions.<sup>6</sup>

A fair view would be that doctrine and training alone do prepare warriors for a change. However, it could also be argued that there is a large challenge that one needs to understand. Without a considerable degree of education, doctrine alone creates learning abilities that are experiential. It also creates the tendency to implement lessons from one sui generis campaign to another. Michael Gordon and Bernard Trainor explain this accurately in their book "Cobra II: The Inside Story of the Invasion and Occupation of Iraq", dedicated to the dynamics inside the military and political environment in the US before the launching of the campaign "Iraqi Freedom".<sup>7</sup> Similarly, Colin McInnes concludes that *"Doctrine and training may constrain the ability to think outside the box, but limit the ability to understand novel situations"*.<sup>8</sup> Even though these authors have provided evidence that supports the thesis for better military education, one could ask (as my practice shows) why do we need this kind of military?

My answer is simple. The operational environment where SEE countries deploy our troops is fluent,

---

<sup>4</sup> Report of the High-level Panel on Threats, Challenges and Change, *A More Secured World: Our Shared Responsibility*, p. 1-4

<sup>5</sup> Charles C. Krulak (1999) *"The Strategic Corporal: Leadership in the Three Block War"*. Marines Magazine. [Air University](#). Retrieved 2006-11-23

<sup>6</sup> John Kiszely, "Post modern Challenges for Modern Warriors" The Shriven ham papers, Number 5, December 2007

<sup>7</sup> Michael R. Gordon & Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*, 2007

<sup>8</sup> Colin McInnes, "The British Army's New Way in Warfare: A Doctrinal misstep? Defense and Security Analyses, 23:2, 127-141, June 2007

unpredictable and messy. As David Kilcullen, the former COIN advisor to the General Petraeus, puts it: *"It is a complex, problematic form of conflict that straddles the boundaries between warfare, government, social stability and moral acceptability"*<sup>9</sup>. Hence, to be able to operate in this environment our young leaders must endorse the capability to make novel decisions, not to react on the previously constructed scenarios and default actions. This doesn't mean that SEE countries should give up training and doctrine development. Quite the opposite. Education should be used as a platform for doctrine and training development, not the other way around. To paraphrase Huntington: "The complex operations demand warriors who are capable of planning, preparing and executing operations with the multi-disciplinary and comprehensive approach, combining a number of lines of operation".

Although many arguments speak about the shift that SEE countries must consider the SEE reality proves that it is much easier to narrowly accept this than to cognitively digest it and implement in practice. The so-called "cultural challenge" like in the rest of the world puts people in the position where they tend to stay in their safe areas. Thomas Khun's theory described in his book "The structure of scientific revolutions" is totally applicable to military wisdom and the strategic leaders in SEE. Accordingly, we are witnessing that military leaders (consciously or sub-consciously) have a desire to prove that their style is superior, and are reluctant to changes.<sup>10</sup> Therefore, if we are about to change something and produce SEE countries must consider finding the right balance between education and doctrine and training, and, thus, avoid the opposite pole. Among other things, education should prepare our future warriors to advise, plan and execute missions for peace while understanding the opponents' and one's own culture.

### **3. Coping with the challenges to current military education, some thoughts for SEE countries' military leadership**

If SEE countries want to achieve more by employing military forces as an instrument of national power they need to design an education system in such a way that will enable future warriors to endorse complex political decisions, technological development and its limitations, cultural perceptions, acting in crisis situations and preventing them, respecting the rules of law and especially human rights.


The complex geopolitical reality produces complex political situations and, accordingly, complex political decisions. As a result, the enemy on the ground could change on a weekly if not on a daily basis. Unlike the politicians the military is usually trained in a way to execute concrete and precise directives and orders. Politicians, which is totally understandable, need more options. They rarely stick to the black and white solutions. Instead, they are more comfortable with practicing politics through the so-called "fifty shades of grey" concept. This is not a critique of both sides. But, rather, introducing the complexity that one needs to understand when preparing future warriors.

Another challenge, which is asymmetrical and confusing, stems from the limits of technology. Practice shows that even though perceived enemies, like non-state actors in the contemporary and future operational environment where future SEE warriors will operate, are technologically inferior, they still effectively oppose the coalition forces. Surely it is trendy to implement new technologies and introduce them to our future leaders on the ground. But we must create a wisdom among these warriors that will enable them to compensate the limits of technology and yet accomplish a desired end-state.

---

<sup>9</sup> David Kilcullen, *"The Accidental Guerilla-Fighting the Small Wars in the Midst of big One"*, Oxford University Press, 2009

<sup>10</sup> See more in: Thomas Khun, *The Structure of scientific Revolutions*, Chicago University Press, 1962



Culture matters a lot. The success is guaranteed to one who understands this. Therefore, we must transfer to our young leaders what Sun Tzu once thought us, i.e., that *if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies, but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.*<sup>11</sup>

One of the effects of the changed security reality is the elevated importance of managing the crisis situations. As prescribed in SEE legislation in the most simple sense this is a situation between peace and war. Contemporary security dynamics among others are shaped by the transition of the military forces and the necessity to catch up with the Euro-Atlantic integrations, necessity to respond to natural disasters and necessity to counter threats to critical infrastructure posed by modern terrorism. Arguably defending the homeland under the Cold War paradigm has created the civil defense system capable to effectively react and defend the homeland in a synchronized and coordinated manner with the overall defense system. However, the changed security reality and the post-Cold War reality dynamics urged a transformation of these systems in SEE.

It is true that many criticize these changes and transition processes, arguing that we were better off in the past. On the other hand, it is also true that these systems were robust, costly and designed for different security and political environments. More or less, today almost all SEE countries have developed crisis management agencies whose missions are to prevent, react, mitigate and manage the consequences of disaster and to bounce back, i.e., to normalize the system and secure continuation of the national system's performance. Most of these agencies or institutions are now out of the defense umbrellas and have developed doctrines and procedures in this context. SEE countries' respective military forces, according to the legislation, should have a supporting role.<sup>12</sup> Therefore, new educational curricula should consider planning, producing and executing missions to support this role and protect critical infrastructures.

Finally, one of the biggest challenges so far in countering asymmetric and unconventional threats is to earn and maintain legitimacy. Respecting the rules of law is a crucial enabler in this context. The fact that General Krulak's thoughts about the three block warfare are relevant the new education curriculum for the SEE warriors of peace must consider wider branches of law. So far, almost all SEE countries have been focusing on the International laws of armed conflict (ILOAC) or as some call it International humanitarian law (IHL). Respecting International Human rights Law and domestic criminal law has been all but neglected. Their relevance is especially important in the post-conflict environment or during a crisis. Thus, although not exclusively, this creates a culture that mocks the humanitarian principles and emphasizes hard power.

It is true though that the complex situations on the ground are frustrating and at odds with the existing doctrines, the tactic and procedures were designed in accordance with the legal principles and standards and approved by the political and democratic leaders. However, it is also true that intrinsic and applicable knowledge of these principles and standards could be conceptualized in a way that follows the logic of the military operations on the ground. If one designs the future military education curriculum in accordance with the previously described incentives from above one increases the chances to better equip the future SEE warriors to cope with contemporary security challenges.

---

<sup>11</sup> Sun Tzu, "The Art of War", Ch-3, Planning offensive

<sup>12</sup> Hadji-Janev, Metodi & Jovanovski Vlatko, (2014), "The Concept of Resilience and Protection of Critical Infrastructure against Natural and Man-made Disasters in Republic of Macedonia\*", in: Collegium Antropologium, 38 (2014) Suppl. 1, Zagreb, Croatia, pp143-155, available at: <http://www.coliantropol.hr/antropo/issue/view/20>

\* Turkey recognizes the Republic of Macedonia with its constitutional name.

## Conclusion

The political and security reality have changed and are still changing. These changes heavily affect the operational environment and create a burden for military leaders. Focusing on the training and doctrine adjustment is a valuable and important process. Doctrine adjustment creates a framework for effective transfer of political guidance to tasks on the ground. Training to create better planners and operators on the ground is also necessary. The problem with this approach, however, is that it creates default solutions. To effectively cope with the security challenges in the operational environment SEE warriors need to be able to produce novel solutions. For this they need education and not training and doctrine adjustment alone. In fact, the education should be a platform for better doctrine and training development.

## References:

1. Charles C. Krulak (1999). "[The Strategic Corporal: Leadership in the Three Block War](#)". *Marines Magazine*. [Air University](#). Retrieved 2006-11-23
2. Colin McInnes, "The British Army's New Way in Warfare: A Doctrinal misstep? Defense and Security Analyses, 23:2, 127-141, June 2007
3. David Kilcullen, "*The Accidental Guerilla-Fighting the Small Wars in the Midst of big One*", Oxford University Press, 2009
4. John Kiszely, "Postmodern Challenges for Modern Warriors" The Shriven ham papers, Number 5, December 2007
5. John J. Mearsheimer, "Why we will soon miss the Cold War", August, 1990, The Atlantic online, at: <https://www.theatlantic.com/past/politics/foreign/mearsh.htm>
6. Metodi Hadji-Janev & Vlatko Jovanovski, (2014), "The Concept of Resilience and Protection of Critical Infrastructure against Natural and Man-made Disasters in Republic of Macedonia\*", in: Collegium Antropologium, 38 (2014) Suppl. 1, Zagreb, Republic of Croatia, available at: <http://www.collantropol.hr/antropo/issue/view/20>
7. Michael R. Gordon & Bernard E Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq, 2007*
8. Report of the High-level Panel on Threats, Challenges and Change, *A More Secured World: Our Shared Responsibility*
9. Seyom Brown, "World Interests and Changing Dimensions of Security", in Michael Klare and Yogesh Chandrani (eds), *World Security: Challenges for a New Century*, 1994, New York: St. Martin's
10. Sun Tzu, *The Art of War*, Ch-3, Planning offensive
11. Thomas L. Friedman, *The World Is Flat, A Brief History of the Twenty-first Century*, Farrar, Straus & Giroux
12. Thomas Khun, *The Structure of scientific Revolutions*, Chicago University Press, 1962

\*Turkey recognizes the Republic of Macedonia with its constitutional name.

## Transition of the Military Education System in Croatia

COL Slobodan Čurčija, Vice Dean of Croatian Defense Academy

1LT Tina Orlović, Executive officer, Office of the Commandant, Croatian Defense Academy

### Croatian Defense Academy

The Croatian Defense Academy is the only institution of higher education of the Croatian Armed Forces. It was established at the very beginning of the Homeland War. Over 36,000 Armed Forces members have attended the CDA courses. The transformation of the Croatian Armed Forces has also included the transformation of the Croatian Defense Academy. By joining Euro-Atlantic and European associations, the Croatian Armed Forces started to prepare for new challenges. Their first step was the harmonization with the standards of national civilian education system and, simultaneously, integration with the European Higher Education Area.

In the academic year 2014-2015 the Croatian Defense Academy introduced two new undergraduate university military study programs: Military Management and Leadership and Military Engineering. They have been developed in cooperation with 11 faculties of the University of Zagreb. The development of military education programs aims to improve the quality of the CAF officer education and education of other Croatian and foreign students attending the CDA courses in which they will not only gain more competencies, but also meet interoperability standards required for cooperation with officers from NATO and European Union member countries. The Basic Officer Course is an integral part of this program.

As defined by the Croatian Armed Forces Long-Term Development Plan, the Croatian Defense Academy is the principal military educational institution whose objective is to integrate into the academic community as an academic and scientific-research institution.

### Current Military Education System

Level	Duration
Basic Officer Course	1 academic year
Advanced Officer Course	1 semester
Command & Staff College	1 academic year
War College	1 academic year

Table 1: Current military education system in Croatia

# COMPENDIUM 2015

Besides the main issue of the lack of integration into the civilian academic education system, the Academy struggles with the resulting absence of academic accreditation of the programs and the student academic titles, as well as the inability to apply the criteria for the selection of academic and school professions. The integration with the civilian academic education system is planned through the adaptation of the existing programs of the CDA's current military education system in close coordination and cooperation with the Universities of Zagreb and Split. The main efforts are being made to develop an appropriate module with a curriculum that would provide support to military strategic goals and satisfy the University accreditation requirements.

The first steps towards full integration of the CDA military education programs into the civilian academic education system have been made by incorporating the Cadet program as an undergraduate university military study program at the University of Zagreb. Starting from the academic year 2014-2015, 11 faculties of the University of Zagreb are participating in this study program, with the Faculty of Electrical Engineering and Computing and Faculty of Political Science as the program coordinators. The development of military-relevant and academically accredited programs will enable cadets to earn 240 ECTS upon graduation and after four years of study they will be commissioned as Second Lieutenants. There are two main curriculums: Military Engineering (ME) and Military Leadership and Management (ML&M). The Military Engineering study program will educate future officers of Armory, Artillery, Engineering, Signals, CBRN Defense and Technical Service to meet the requirements of CAF services.

The Military Leadership and Management study program is aimed at educating the future officers of Infantry, Military Intelligence and Military Police branches.

The general requirements for enrollment into these two programs are prescribed by the University of Zagreb. They include a successful completion of a 4-year high school education program and the results achieved in the state-school leaving exam as well as the grade point average as listed in Table 2.

Subject	ME		ML&M	
	Level	Admission points score	Level	Admission points score
Mathematics	higher	30%	basic	20%
Croatian	higher	20%	higher	25%
English	basic	20%	higher	25%
GPA		30%		30%

Table 2: General enrollment requirements

On the other hand, the Croatian MoD has prescribed specific requirements regarding medical health, the psychophysical status, physical fitness and security. After enrollment, students undergo a preparatory camp with the purpose of acquiring the basic knowledge of military customs and courtesies, such as military regulations, salutations, military ranks, the military profession, etc.

## CURRICULUM

The study programs are comprised of general, political, general military and military vocational subjects.

Non-military subjects		Military subjects	
General	Political	General Military subjects	Military Vocational Subjects
Mathematics	Academic Writing and Research Methods	Military Psychology	Military Combat Systems
Informatics and Programming	Political System of Republic of Croatia	Military Pedagogy	Communication and Information Systems
International Law	Decision Analysis	Military History	Management of Military Logistics Systems
Statistics	Military Sociology and Sociology of War	Military Geography with Topography	Ballistics
Foreign Language		Military Leadership	General Tactics
Physical Training		Military Management	Infantry Tactics

*Table 3: Subjects overview*

The students/cadets enjoy numerous benefits, such as scholarships, free handbooks, personal computers, uniforms, sports gear, free public transport, extra meals, covered travel expenses to the place of residence twice a year, single room accommodation, laundry and hairdressing services, sport facilities, etc. Students mustn't fail their freshman year or they will be excluded from the program, although they can fail their senior year. Upon graduation, cadets are obliged to serve in the military. The length of their service is twice as long as their education, e.g. if the cadet graduates after 5 years, he/she has to serve in the military for 10 years.

## MILITARY TRAINING

Throughout the academic year, cadets undergo military training one working Saturday per month, one working weekend at the military training area per month and they also attend a 2-hour training twice a week. No training is conducted the week before and during the exam period.

Throughout their studies, cadets also undergo military training at the boot camps. The boot camp programs are structured according to the cadets' academic year and knowledge and skills acquired during previous trainings.

The objective of Boot Camp 1 is to acquire basic military skills and get accustomed to future life as part of the military organization. It consists of the Summer and the Winter Boot Camp. The training purpose is to gain knowledge of the military profession and to start acquiring basic military skills. The purpose of the Winter Boot Camp training is to master basic alpine skiing techniques, while the Summer Boot Camp focuses on basic drill procedures, weapons training and marksmanship.



# COMPENDIUM 2015

The objective of Boot Camp 2 is to train team leaders. It is also comprised of the Summer and the Winter Boot Camp. The training purpose is to acquire basic knowledge and skills required to lead a team/group in the execution of small unit tactical tasks. The training purpose of the Winter Boot Camp is to master advanced skiing techniques as well as basic skills and techniques required for successful operations and survival under extreme conditions.

Boot Camp 3 also consists of the Summer and the Winter Boot Camp. The Summer Boot Camp training objective is to acquire basic knowledge and skills required to lead a squad and the purpose of the Winter Boot Camp training is to master advanced techniques, skills and knowledge required for operation and survival under extreme conditions.

Boot Camp 4 is no different from the previous three. It consists of the Summer and the Winter Boot Camp. The Summer Boot Camp training objective is to acquire basic knowledge and skills required to lead a platoon in combat operations, peace support operations and crisis management operations. The purpose of the Winter Boot Camp training is to integrate previously acquired knowledge and skills and apply them during the final exercise.

## **EXPECTED RESULTS**

After their graduation and commission as second lieutenants, junior officers are expected to have mastered basic skills of the military profession, gained specialist military knowledge, basic knowledge of social and humanistic studies and basic technical knowledge. They are also expected to have developed personal and professional skills and characteristics of a leader as well as social skills and characteristics, such as teamwork and communication skills.


## **PROMOTION AND RECRUITING**

The following promotional and recruiting activities have been conducted for the purposes of cadet recruitment and promotion: top young sportsmen and sportswomen have been included in promotional activities; cadets have participated in CAF events open to public and non-military events organized for future students (University of Zagreb Fair, Career Day, Scholarship Fair, Job Fair); high school visits with cadets and pilots have been organized; cadets have participated in radio and TV shows; they have been promoted on social networks and the CDA's web page and info phone lines have been established.

## **FUTURE EFFORTS**

The next step towards integration of the CDA military education programs into civilian academic education system is the development of accredited graduate programs in Military Nautical Studies and Military Ship Engineering in cooperation with the University of Split.

Efforts are being made to develop a new graduate university program from the existing Advanced Officer Course. The desired outcome is a graduate program developed in coordination and



cooperation with the Universities. Upon graduation, students will earn 60 ECTS for a 3-semester course of study.

Further efforts are also being made to accredit the existing War College program as an accredited specialist postgraduate university program.

With complete integration of the CDA as an academic and scientific research institution into the academic community as a desired end-state, the CDA will continue to primarily educate students to meet the requirements of the CAF and other government and security institutions. The achieved level of education and outgoing competences will be comparable and equal to those acquired at other universities in the Republic of Croatia as well as other EU and NATO member states.

## **CONCLUSION**

New challenges arising from continuously changing surroundings are setting up new requirements and the CDA's response is a structured and overall approach to military education, its development and enhancement by establishing cooperation with the highest academic institutions in the Republic of Croatia. The CDA will continue to invest efforts in further development of education that provides knowledge, skills and capabilities required to operate in national and multinational environments. By implementation of new methodological and educational programs and technologies, the CAF plan to develop a military education system recognized in the region.

The overall situation is very promising and the initial results from cadet participation in undergraduate university military study programs are very optimistic. The climate is right and with the current support of the academic and political community, we hope to see other levels of military education at the CDA being developed and accredited by the academic community soon.

## Modelling the European Initial Officers' Education and Training Systems

By Sylvain Paile-Calvo

Senior Researcher, University of Liège

Too often, formally or informally, the "military specificity" *vis-à-vis* the higher education is raised as the main obstacle to the enhancement of mobility. However, this specificity is shared by most of the military institutes responsible for the basic education and training of the officers. One could think, therefore, that nothing prevents exchanges between entities sharing similar characteristics. Possibly, the obstacle could be their difference from other - civilian - entities that play the game with different rules.

In the military higher education, the argument of the "military specificity" is, certainly more than in the civilian higher education, coupled with the argument of a "national specificity". Civilian universities, for instance, mainly educate their students in a somehow similar way across the European Union, despite the differences in the curricula, based on the number of ECTS and duration of study cycles. In the European military higher education there exists a wide diversity of basic education and training models, based on the object of the curricula, their composition or duration, for example. But, also, very often there is a possibility of involvement of more than one institution in the basic education and training of an individual, which is extremely rare in the education of the civilian elites apart when speaking about personal choices. It is more appropriate and more convenient, therefore, to refer to a national frame through the term "system".

Often, the "specificities" of one or the other education and training system, allegedly on the basis of the nationality or the needs of a particular service, are also used as justification for limiting the possibilities of exchanges or the scope of the national or institutional exchange policies. However, one can expect that in the European Union the historical interaction of the Nations and the States gave birth to commonalities in the know-hows in the basic education and training of the military officers. This is a hypothesis the explorer of the military higher education shall consider. These commonalities could in principle remain at the level of simple similarities in the mechanisms, such as the mechanisms established on the basis of the standards of the European Higher Education Area or, crystallised in "models" where and when the systems share similar philosophies and logic. Consequently, these models could be used as the foundation of a further enhancement of the exchanges between the systems of a same or close "family". The possible classifications, if they exist and are valid, may help the explorer identify ways for developing the mobility of the cadets<sup>1</sup> as it stands today.

Efforts to classify have been undertaken by authors and can be found in literature, though this one is limited as it relates to the initial stage of the education and training of the officers. Indeed, there are several attempts at classification that can be proposed to the eye of the explorer and kept in mind with a view to possibly interpret and comment findings. Hence, it is necessary to select in the first place those that concern the capacity to enhance mobility. Since a look at the existing literature does not allow identifying any effort of classification of this kind, the explorer should consider only those that are possibly relevant *vis-à-vis* the existence of "families".

---

<sup>1</sup> One must state, already at this stage, that the exchange of personnel is less - or, rather, not - affected by such a possibility since the conditions of their work do not fundamentally matter here. A teacher, for instance, may in principle teach - or even train - in a host institution of a host system even if these entities do not share any similarities.

The classification that is proposed by professors Kirkels, Klinkert and Moelker<sup>2</sup> is among the first ones to be considered. They made a distinction, indeed, between two traditions already used previously to describe the role of officers with regard to the history of the missions<sup>3</sup>. They analysed the nature of the officer and his/her role in peace construction: the "Spartan" model and the "Athenians" model. The former outlines the need for a military officer to be first of all a soldier and insists, in view of his education and training, on his behaviour in the field of operations. The latter favours the vision of the military officer as being part of an intellectual elite, capable of dealing with the complexity of the social, economic and political aspects of his or her mission. The values attached to this distinction may be summarised as is shown in the following table.

#### Values attached to the Sparta/Athens distinction

"SPARTAN" VALUES	"ATHENIAN" VALUES
Personal austerity and glory	Learning and high culture
Discipline and self-sacrifice	Creative and critical thinking
Science and technology	Philosophy and history
Patriotism and honour	Crosscultural sympathies
Personal heroism	Politically post-heroic

Source: Peter Foot (2006)

Applying this to the basic officers' education and training professors Kirkels, Klinkert and Moelker promoted models which insist that priority be given to academic education in the curricula delivered by military institutions. They relied on five contextual arguments:

- Focusing education on combat training remains necessary but is no longer sufficient;
- An education system essentially focused on the teaching of human values and practical knowledge, as in classical academies, might attract a public not suited to the new missions. Furthermore, it might not be adapted to the political demands emerging in the European context;
- The competency profile of an officer should correspond more to professional capacities than to practical knowledge;
- A growing integration between civilian national higher education and the military education system is more appropriate for flexibility of missions and also allows budgetary consistency;
- Military education should follow university standards and, in order to provide an appropriate study environment, it should be provided in civilian universities. It transposes to the field of the education and training of the military officers the initial level in the first place - the dichotomy of the Spartan and Athenian models of values in the military profession.

Since its focus is on these values, it is possible in principle to apply it to the analysis of the education and training policy of a given institution, *i.e.* the action of this institution in the more global context of the preparation of the officer for his or her profession. However, as the concept of "values" relates to the end of this preparation, it seems that a better echo is achieved when applied to the analysis of the entire basic education and training system. This classification is mainly based on the respective weights of the academic education and vocational training. It is following the idea that, even if they necessarily complement each other as both are needed to train the military elite, these aspects "fight" for being the biggest piece of the cake. In fact, these aspects do coexist in every European Union officers' basic education and training system but they do not always coexist in an institution. Several

<sup>2</sup> Harry Kirkels, Wim Klinkert, René Moelker (eds.), *Officer Education: The road to Athens!*, NL Arms, Netherlands Annual Review of Military studies, 2003.

<sup>3</sup> Peter Foot, "Military Education and the Transformation of Canadian Armed Forces", *Canadian Military Journal*, Spring 2006, p.15.

# COMPENDIUM 2015

institutions may be in charge of different aspects as is the case, for example, in the Republic of Slovenia, Federal Republic of Germany or the United-Kingdom. Owing to the fact that exchanges take place more on the level of institutions than an entire system, therefore, this classification gives interesting indications about the cultural identity of a system but is less relevant with regard to mobility enhancement.

Giuseppe Caforio<sup>4</sup> proposes a second classification, which sensibly implements the Spartan-Athenian dichotomy as well, but at the level of the basic education and training institutions this time. He establishes a distinction between the institutions in which education and training policy and functioning, converge with those of civilian higher education institutions, and the institutions that diverge with them, *i.e.* that are organised on the model of “military academies” understood in a classical way. As a parallel to the previous classification transposed at the level of institutions, one could expect that the converging institutions mainly promote Athenian values and the diverging ones the Spartan values. Naturally, the distribution of the European institutions in this classification by Giuseppe Caforio is more nuanced than that. This classification does not focus on mobility perspectives, either, but primarily touches on the socialisation of the cadets in regards to their future profession. It concentrates its efforts on the institutions, which are the first actors of mobility but it does not take into account the possibility that cadets move very regularly from an institution to another, for training camps *e.g.*, within a period which could be envisaged for inward or outward exchanges. Nevertheless, this classification is highly interesting because it comments on a trend, generally observed in the European Union, of progressive alignment of the military education philosophies with the civilian higher education models.


Another classification could be proposed that goes further than the simple “weights” of the academic education and the vocational training in the curriculum. It is based on the nature of the organisation of these two components<sup>5</sup> within the basic education and training systems. Using the schedules of the curricula, which reflect their contents, the systems could be distributed as follows.

## Classification of the systems according to the organisation of the academic and vocational components in 2014

	Organic separation of the academic / vocational	Intermediate	Alternation academic / vocational	Parallel organisation academic - vocational (and alternation)	Intermediate separation (and parallel)
Army	DK, SL, DE	CZ, SE	AT, BE (+LU), FI, FR (+LU), GR (+CY), HU, NL, RO, SK, RO (engin.), ES	EE, HR, IT (+MT), LT, LV, BG, PT, PL (engin.)	IE (+MT), UK (+MT)
Navy	DK, DE, SL	SE	NL, PT, BE, BG, FR	ES, FI, HR, IT (+MT), LV, RO, EE, GR (+CY), PL	IE (+MT), UK (+MT)
Air Force	DK, DE, SL	CZ, SE	AT, FR (+LU), BE (+LU), HU, IT (+MT), NL, RO, SK, LT, LU, RO (engin.)	BG, EE, ES, FI, GR (+CY), HR, LV, PL, PL (engin.), PT	IE (+MT), UK (+MT)
Gendarmerie			IT	ES, PT, FR, RO	

<sup>4</sup> Giuseppe Caforio (eds.), *The European officer: A Comparative View on Selection and Education*, European Research Group on Military and Society, Edizioni ETS 2000.

<sup>5</sup> See Sylvain Paile (2010), *Op. Cit.*, p. 118-122. It must be noted that this classification did not take into account the regular physical training a cadet is expected to practice all along his or her curricula but that it is considered to be a component of vocational training.



The organic separation is found where institutions, within or outside the military sphere, are dedicated to the academic education of the future officers although others are dedicated to their vocational training, for example in the Republic of Slovenia. The separation between these two is "physical" but the cadets must follow their programmes.

The alternation is found where the curriculum is provided by one main institution which, for organisational reasons, alternates academic semesters and vocational training exercises. This model of organisation is notably followed by inter-service institutions, as they have to "send away" their cadets for the purpose of vocational training since they may not have all the facilities that are needed on their premises.

In-between the two previous categories systems that have different institutions in charge mainly of one or the other aspect but where the students may be called upon to move between them in the course of their curriculum can be found for practical training, notably.

The last main category covers the education and training systems in which the two types of training are conducted in parallel, such as for example in the Republic of Croatia. However, there is no "pure" parallelism insofar as, to be effective, some practical exercises need time especially dedicated to them. Therefore, the defining characteristic of these systems for their classification in this category is that they have at least extended periods during which they conduct both types of training.

In between the "parallel" and the "organic separation" categories exists an intermediate one, which is very specific in the sense that it covers only the British and Irish education systems. The delegation of academic education still exists as a rule, formally (in Ireland) or informally (in the United Kingdom), but the cadets have also theoretical/academic courses in the academies, which do not necessarily lead to a higher education diploma but which can be valued in such a diploma with extra studies. Contrary to the category of "organic separation", the cadets are not obliged to "pass through several institutions and their programmes in order to be commissioned. However, the small proportion of these academic or "theoretical" courses, compared to the amount of vocational training, brings the systems closer to organic separation than real parallelism.

This classification made out of observations of the organisation of time can be an indicator and an element of predictability in the search for exchanges of students. It can be assumed that when an institution looks for an academic exchange in a Member State where the two aspects are organically separated, it will address a given institution depending on whether the object of the exchange is academic or vocational. For systems where the two types of training are alternated, the time organisation involved is the most important criterion to address. Finally, if an exchange is envisaged with a system where the two types of training are conducted in parallel, it may be thought that the sending institution would have to entrust the hosting institution with the training of its students in both vocational and academic aspects. The scope and difficulty of the task is thus different when dealing with systems of different categories. Structurally, however, every military education system can find potential partners. This effort at classification is, therefore, of limited help in view of identifying the characteristics that would suggest that a system or an institution is mature enough for developing further its mobility policy and practices quantitatively and qualitatively. Alternatives or complements must then be investigated.

A possible classification for analysing the European military higher education could also focus on the "military science". The assumption is that the object of the military education and training, already at the initial level, is to spread a "military science" that would go beyond the mere military application of existing sciences. "Military history", for example, can be seen as the application in the military sphere of historical science. On the other hand, the military can also be seen as having invented a leadership science. But the real military specificity according to this classification is that it would completely merge academic education and vocational training in one fully-integrated curriculum. One of the main markers for distributing the systems according to their level of integration would be the organisation of the academic and vocational aspects: the more "parallel" - to use the previous proposition of classification - the organisation is, the more integrated the military science is. Another one would be the credit system: if vocational training is being credited with ECTS this suggests that both aspects are being merged into a "military science", if it is not credited at all the system tends to remain focused on "military sciences". Though it may apply to the education and training policy of an institution, this classification rather addresses the systems.

Another possible classification would be more specific as it could focus on interoperability. One could propose, indeed, to distribute the institutions according to their level of preparation to interoperability they offer. Joint institutions, whose number is currently increasing due to the financial constraints met by the European Union Member States and institutions with an important exchange culture, would be the most "interoperable" ones. However, the purpose is not to promote the merging of institutions into joint ones, as this depends on the national traditions and education and training cultures and mobility would be, in such a classification, a marker and not the objective, as sought by the explorer. But it is equally true that joint institutions have specific advantages in terms of attractiveness and inward mobility.


It is also possible to classify the systems according to the level of academic studies that is required from a newly commissioned officer posted for the first time as a leader. In the European Union, notwithstanding the implementation of the Bologna Process standards, three categories can be defined: the systems that do not officially require particular academic levels at the end of the basic curriculum, the systems that require a bachelor-equivalent level and the systems that require a master level. Due to the phenomenon of academic education being delegated to the civilian sector<sup>6</sup>, the first category can be challenged and, in terms of mobility enhancement, it does not give particular information on how the military specificity is being dealt with.

One could also propose to classify the institutions, this time, according to the level of the implementation of the European Higher Education Area standards and guidelines. Such a classification would highlight their desire to be recognised as European-integrated institutions and their respective readiness for exchanges. However, as has been already concluded, these standards and guidelines are not sufficient to develop mobility to an expected level.

These classifications or possible classifications present different levels of relevance *vis-à-vis* the development of mobility. They reveal that "families" of systems and/or institutions exist within the European Union<sup>7</sup> and the distributions between the families get their meaning from the objective behind the efforts at classification as well as the use of generic markers. Overall, even if they do not

<sup>6</sup> Notably in the United Kingdom officers' basic education and training systems.

<sup>7</sup> And, most probably, can be extended to countries outside the European Union as the exchanges between the military cultures were not and are not limited to the European Union, e.g. NATO countries.



offer the possibility to "systematise" the search for mobility development means, which suggests that the explorer should question the feasibility and desirability of establishing a mobility-tailored method, these classifications can be used as a certain scientific dashboard of the European military higher education.

An ideal classification, focusing on the capacity of mobility development, would address both the institutions and the systems on the same level as to be detailed enough to be useful to the primary mobility actors which are the institutions but also to be curriculum oriented. Such classification should also address both the academic and vocational components of basic education and training. It should not be used as the exclusive criterion but it is too often seen, as has been previously stated, that the number 1 obstacle to the development of mobility are the differences that exist between the curricula which, if the student has not followed them entirely, prevent the recognition at the national level of the validity of the exchange's benefits in the commissioning curriculum. Standardisation is neither realistic nor desirable. However, it may seem legitimate that the institutions expect at least some identity of the content of the parts of curricula that are being exchanged; not an exact match of programmes but a similarity in the balance of the academic and vocational components. Taking all these factors into account, it may be proposed to also base such a classification on the qualifications to be acquired by a future military elite throughout his or her basic education and training. A qualification-based classification would address both the institutions and the systems equally. The drafting of qualifications, indeed, is meant to reflect the "end products". The units of time and duration used for comparing two institution(s) and / or system(s) would not be relevant, therefore. And, with a view to be read through the glasses of mobility, the qualifications constitute the standards for mutual recognition the mobility actors call for. In the framework of the European initiative for the exchange of young officers inspired by Erasmus, the work of defining the European sectorial qualifications framework is on-going. This framework will reflect both the academic and vocational components not as a duality but as being complementary - toward a "military science", prospectively. It is, in a way, an "acceptable" effort of standardisation that is currently taking place since it is based on the inputs of participating institutions themselves and according to a certain "bottom-up" approach: the institutions shared what they implemented in terms of qualifications in their education and training policies and the commonalities were then used for designing the European and joint qualifications. The qualifications and their respective importance in a given timeframe would, in this sense, allow a re-interpreting of the military higher education *vis-à-vis* the objective of mobility development. However, this method of interpretation is only in its conceptual stage as the framework needs first to be established as a legitimate and common language of the European officers' basic education and training systems.

Efforts at classifying and modelling the officers' basic education and training systems and/or institutions, therefore, can support and guide the process of search for possible partners in an exchange or possible mobility opportunities. However, as the process is intimately linked to the personal assumptions and expectations of the searcher as well as the selection of subjectively relevant criteria among an indefinite number of possible ones, it is unlikely that one classification only, as accurate as it may be, can be a universal key for finding "true love".



## **Civil-Military Relations and the Democratic Control of Armed Forces**

Prof. dr. Anton Bebler

Faculty of Social Sciences, University of Ljubljana


E-mail: anton.bebler@fdv.uni-lj.si

The democratic control of armed forces constitutes today the most important principle on which civil-military relations rest in democratic societies. Its forms, quality and intensity vary considerably in the Euro-Atlantic area reflecting the countries' historic experience, political culture and the general state of their representative democracy.

Modern forms of civilian control over the armed forces have originally developed in England from a political compromise in 1688 between two oligarchies - the aristocracy (represented by the Crown and the House of Lords) and the rising middle class (represented by the lower chamber of Parliament - the House of Commons). The initially limited civilian control through the Parliament's passing of the state budget has evolved gradually into a democratic and progressively strengthened instrument in parallel with general political reforms. These reforms transformed oligarchic systems into modern representative democracies featuring notably universal suffrage, ideological pluralism, competing political parties, fair electoral systems, a vibrant civil society, autonomous mass media, etc.

Several models of strict civilian control have developed also in totalitarian (fascist and communist) political systems in XXth century Europe, reflecting the rulers' distrust and fear of the professional military. The main instruments for controlling the armed forces in these states had not been Parliaments which were either disbanded or altogether made into toothless appendices of the regime. Instead, the ruling totalitarian party and the secret police became the main tools of control by civilian dictatorial rulers. The civilian control over the armed forces is thus a necessary but insufficient condition for a democratic system.

The essential features of the British parliamentary oversight of the military were transplanted to and became subsequently internalized in the predominately white British colonies (including the USA, Canada, Australia and New Zealand). Their implementation in other British colonies and protectorates was frequently unsuccessful or very shaky, interrupted by military coups (e.g. Pakistan, Nigeria, Uganda, Egypt, Libya, Sudan, Iraq et al.). There have been a few exceptions from this predominant pattern (India, Sri Lanka, Malaysia, Singapore). The record in the former French, Portuguese, Dutch and Belgian colonies has been even worse, not to speak of the former Spanish colonies where military dictatorships predominated in the XIXth and during several decades also in the XXth century. The British model of civilian parliamentary control has slowly and unevenly spread by emulation to other parts of Northern and Western Europe. After the second World War it was reintroduced in France, Italy, the Netherlands, Belgium, Norway, Finland and Republic of Austria, was imposed by the occupiers on Western Germany (and in Asia on Japan), adopted in several Southern European states from the mid-1970s onwards (Portugal, Spain, Greece) and in the Republic of Turkey from the 1980s onwards. In the 1990s, after the fall of communist regimes civilian parliamentary control became a rule also in East-Central and South-Eastern European states. So the predominance of democratic civilian control over European militaries is, historically speaking, a recent phenomenon.



In South-Eastern Europe there have been social and political obstacles which made particularly difficult the implementation and development of democratic civil-military relations. The principal among them have been: the late and weak (compared with Western Europe) democratic transformation of political systems in general which has been interrupted several times and often only superficial. This obstacle has been due to the strong underbrush of paternalistic and authoritarian values and habits among the, on the average, poorly educated population and also among the political elites. In the last 150 years the political history of the Balkans featured many military coups (in the Republic of Serbia, Albania, Kingdom of Yugoslavia, Greece, Bulgaria, Romania, Republic of Turkey) followed by periods of outright military or military-civilian rule. Practically all Balkan states have experienced in the XXth century several types of authoritarian control over the military - a traditional oligarchic, fascist or semi-fascist and two communist patterns. One of the latter ones was copied from the Soviet-Russian system (in Bulgaria and Romania). The other - the Yugoslav-Albanian system was more original and similar to those in China, Vietnam, North Korea and Cuba.

The former Yugoslav and the smaller but similar Albanian system have developed during the Second World War under the ideological and organizational influence of Soviet communism. However, due to the requirements of guerrilla warfare in territories occupied by better armed, stronger and more professional armies of the Third Reich and Italy both systems deviated significantly from the Soviet Russian blueprint. The fused civilian political and military leadership at the top of the two partisan movements allowed military commanders to enjoy a much greater leeway in making operational, including politically sensitive decisions. After the war the state leaders of Yugoslavia and Albania (J. Broz-Tito and E. Hodzha) often wore military uniforms and top generals wielded considerable political weight, also as members of the highest organs of the ruling party. In former Yugoslavia the Soviet-type of control by the civilian party apparatus and the civilian security service was greatly weakened after 1952. This gap was filled in and partly compensated by President Tito's personal control of and close contacts with the top brass as well as by his regular visits to military districts. The organization of the ruling League of Communists of Yugoslavia was established within the Armed Forces separate from its civilian organizations in six federal units (Republics).

But when Tito died in 1980 and was succeeded by a group of lower caliber Republican barons the civilian grip on the military leadership began to crumble. In the 1980s the general economic and social malaise in Yugoslavia had contributed largely to growing decomposition of the Federation also on the political level. Already in 1981 Federal tank units and special troops were ordered to suppress mass student protests in Kosovo<sup>1</sup> as the Serbian police could not cope with the unrest. Frequent blockades in the highest federal institutions, including the eight-member collective Presidency of SFRY, allowed the Yugoslav military brass to get rid of effective civilian control and even to openly pressure top civilian politicians. The two last Yugoslav Defense Ministers - Admiral Branko Mamula and General Veljko Kadijević (both Serbs from the Republic of Croatia) contemplated actively, discussed with their military colleagues and even with the Serbian civilian leader Slobodan Milošević their plans to stage a military coup to "save Yugoslavia". The unconstitutional High Military Command intended to declare a martial

---


<sup>1</sup> This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence. (In accordance with Arrangements regarding regional representation and cooperation.)

law and carry out numerous arrests of civilian politicians, particularly in the Republic of Slovenia and Republic of Croatia. In mid-March 1991 the Command ordered tanks and armored vehicles to the streets of the federal capital Belgrade in a demonstration of political support to the Serbian civilian leadership. The High Military Command elaborated plans for a military takeover and organized its own, albeit short-lived political party called the "League of Communists - Movement for Yugoslavia". It also tried actively to influence the outcome of the first competitive parliamentary elections by allowing to broadcast pre-election political propaganda on the military-controlled reserve television network (maintained for emergencies). The vacillating Defense Minister General Veljko Kadijević finally desisted from taking over supreme political power in former Yugoslavia. The military leadership's strenuous endeavors to save both the federal state and the one-party rule failed miserably. The Yugoslav People's Army's siding with and its active support to Serbian nationalists increased heftily the bloody toll of several wars on the territory of ex-Yugoslavia in 1991-1995.

The decomposition of SFRY in the 1990s brought down the peculiar Yugoslav communist system of fused civil-military relations. It was replaced in the today's seven separate states by several models of civilian control ranging originally from democratic parliamentarian systems to the authoritarian or semi-authoritarian presidential systems. During the last decade the evolution of political systems in all ex-Yugoslav states has brought considerable progress in strengthening the role of parliaments and in democratizing their systems of civil-military relations. There is still much to do to make this progress irreversible and their systems viable. The assistance of international community and international organizations has helped the region significantly also in this important aspect of its political development.

Since the adoption of the "Charter of Paris for a New Europe" (1990) a functioning democracy became a political obligation for all states participating in the Organization for Security and Cooperation in Europe (OSCE). In addition OSCE adopted in 1994 a "Code of conduct on political-military aspects of security" which i. a. elaborated the requirements for democratic civil-military relations as part of the general commitment for implementing the rule of democracy. Politically binding in the OSCE area since January 1, 1995 this Code prescribed four major principles to be followed in European democracies:

- (1) Primacy at all times of democratic constitutional civilian power over military power (encompassing the military, paramilitary and security forces). The military establishments and particularly professional military personnel must be and must remain politically (party-wise) neutral.
- (2) Subjection of the armed forces to the norms and prescriptions of international humanitarian law. This principle applies to all levels of command, to manning, training and equipment in time of peace as in wartime. All military personnel responsible for serious violations of international humanitarian law, whether commanders or subordinates, must be held accountable for their actions under national or international law.
- (3) Respect for the human rights and fundamental freedoms of the armed forces' personnel. The laws and other regulations should provide for effective protection of human rights of the military, paramilitary and security forces personnel.



(4) The use of armed forces for internal security purposes must remain subject to the rule of law, international law and international humanitarian law as in inter-state armed conflicts. This stipulation requires a constitutionally lawful decision on their engagement, the respect of the rule of law during such operations, the commensurability of the use of force with the needs for the enforcement of law and order and the care to avoid excessive injury to civilians and their property. This principle also prohibits a domestic use of military force aimed at restricting human and civil rights when peacefully and lawfully exercised by unarmed civilians or at depriving citizens of their individual or collective identity. It also prohibits the use of military force against citizens as individuals or as representatives of groups.

The Code also prescribed transparency and publicity when preparing and deciding on defense and military expenditures. Each state is to exercise restraint concerning the level of expenditures which should be commensurate with its real and legitimate needs.

From 1999 onwards all OSCE participating states report on the Code's implementation submitting annually a filled in standardized questionnaire. This report contains ten columns seven out of which are related to the democratic control of the armed forces.

Having been negotiated under the iron law of consensus the Code contains several gaps:

- there is no conceptual linkage established between the Code and the Vienna regime of confidence and security building measures (CSBMs)
- the Code lacks operative provisions for paramilitary forces, such as internal security forces, intelligence services and the police and has no provisions at all for border guards
- the human rights and fundamental freedoms of the armed forces personnel are not specified, such as the right to join political parties, to participate passively and actively in elections and in elected legislative bodies, etc.

In a parallel development and roughly at the same time NATO issued a semi-official document entitled the "Study on NATO enlargement" (1995). The document spelled out NATO's "expectations" (in fact conditions) concerning civil-military relations in future members of the Alliance. According to the document the appropriate norms should include:

- a clear division of authority between the president and the government (prime minister and defense/interior minister) enshrined in a constitution or in public laws;
- effective parliamentary oversight of the military through the control of the defense budget;
- peacetime governmental oversight of the General Staff and military commanders through civilian defense ministers and ministries.

In a contrast with the lenient treatment in the past of several older, Mediterranean members of the Alliance (Portugal, Greece, Republic of Turkey) where these principles were grossly violated during the periods of military rule the Alliance has since 1995 started using much higher democratic standards and strictly applied them when deciding on the membership of former communist-ruled East European states.

# COMPENDIUM 2015

An influential American academic Samuel Huntington differentiated between two kinds of civilian control over the armed forces - the subjective and objective. The subjective control is exercised externally through civilian institutions, in democratic systems through the parliament, executive and judiciary branches of the government and through public opinion. Objective control, on the other hand, rests on developed military professionalism and on democratic values (including the value of civilian supremacy) internalized by the military itself. Several important factors characteristic of the military tangibly constrain and make systemically difficult the implementation of subjective civilian and particularly democratic civilian control. In the first place it is the inevitable authoritarian nature of the military organization itself and its logical influence on the mentality of military professionals. Secondly, the highly complex nature of modern warfare which demands a high degree of specialized expertise and training as well as of solid practical managerial experience among civilians dealing with the military. Thirdly, the regimes of military secrecy. Fourthly, the low level or even complete lack of specialized military knowledge and often also of keen interest in military affairs among civilian elites. Fifthly, the extreme time pressure in times of crisis and particularly in wartime and thus the imperative of making quick operational decisions by military commanders.

Due to these reasons the actual working of both democratic and authoritarian civil control over the military differs greatly between normal peacetime conditions and wartime. For example, during the Second World War in democratic Switzerland extraordinary discretionary powers were bestowed for the duration of the war by the Federal parliament on the appointed professional General (Commander-in-Chief). Similarly, in authoritarian states the degree of civilian control drops appreciably under extraordinary circumstances, for example, due to grave external threat, deep political rifts in the country, threats of secession or to greatly internally weakened civilian rule. For example, in Poland these circumstances led to the imposition of martial law and military government in 1981 which lasted for eight years.

Although legally prescribed the real quality of democratic control depends on a number of objective circumstances. Among them figure prominently the general state of democratic institutions (including their functionality, the degree of political consensus among civilian elites on security-related issues, the intellectual quality of civilian political leadership and of parliamentarians, the strength of the civil society, the predominant social values related to the military and the quality and degree of professionalism of military personnel. Obviously, unlawful behavior, abuse of office and corruption among civilian politicians and among the military could entirely debase proper civil-military relations. The maintenance of effective civilian control over the armed forces is a never ending story even in old democracies. It requires attention, constant efforts and broader social support.

## Flood Risk Management in Lower Austria

Experiences and conclusions about the Danube floods in 2002 and 2013

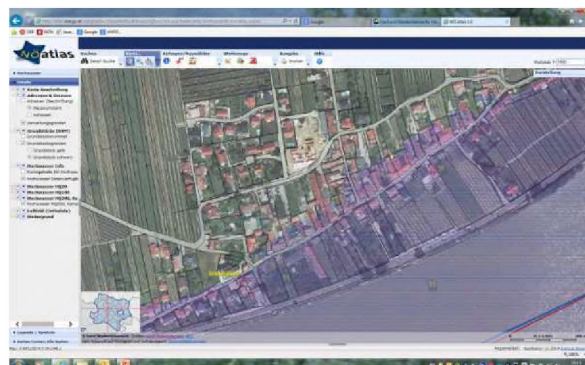
Dipl.-Ing. Martin Angelmaier  
Deputy head of department  
Department of Water Management  
Government of Lower Austria

In the recent years Lower Austria was affected by several floods. Especially the flood disaster in 2002 caused disastrous damages. Because of the experiences from 2002 the Provincial Government of Lower Austria started a new strategy of flood risk management encompassing comprehensive measures. The Danube flood in 2013 showed that these measures have been successful: although the Danube floods in 2002 and 2013 reached similar water levels, the damages in 2013 were significantly lower than in 2002. In 2002 the damages amounted to roughly € 950 mio, in 2013 around € 100 mio only. Even if the damages in 2002 were not only caused by the Danube but also by some other rivers, the difference in damage losses is the result of the comprehensive flood risk management which started after the flood disaster in 2002.

### Flood Hazard Maps

Flood hazard maps are an important base for flood risk management. At the moment in Lower Austria these maps exist for almost all river sections at relevant settlement areas. All in all they have a total length of about 3.000 km. They were elaborated by using digital elevation models and hydraulic simulation models. The flood endangered areas were detected for three scenarios: 30-, 100- and 300-year floods. The maps are available on the website of the Provincial Government of Lower Austria:

[http://www.noel.gv.at/Umwelt/Wasser/Hochwasserschutz/Hochwasser\\_Hochwasseranschlaeslinien\\_Niederosterreich.html](http://www.noel.gv.at/Umwelt/Wasser/Hochwasserschutz/Hochwasser_Hochwasseranschlaeslinien_Niederosterreich.html). Via this website everybody is able to find information about his own flood risk in an easy way.



Flood hazard map available on the website of  
[www.noel.gv.at](http://www.noel.gv.at)  
(© Provincial Government of Lower Austria)

## Spatial Planning

Flood hazard maps are an import base for spatial planning. The Lower Austrian law for spatial planning takes into account also flood risk management. The main aim is a strict separation of settlement areas and areas of inundation. Therefore, it is forbidden to dedicate new building land in areas which are endangered by 100-year floods.

## Flood Protection Systems

In the Republic of Austria there is no statutory obligation for anyone to build structural flood protection systems. It is always a voluntary measure. Usually the municipalities decide to build a protection system. That means that the municipalities are the promoters of the flood protection projects, that they are the owners of the protection buildings and that they are responsible for their operation. The projects are co-financed by the Federal Government and by the Provincial Government. The grants depend on the type of the river and the type of protection system. Usually the municipalities have to cover about 15% to 33% of the total costs.

Since 2002 in Lower Austria 430 projects have been realized. The total costs are around € 700 mio. In the following 10 years further investments of around € 750 mio. are in store. The costs of maintenance of existing flood protection systems are increasing year by year. Lower Austria estimates maintenance costs in the amount of € 115 mio. during the next 10 years.


The flood protection systems of the region "Wachau" are a special case in Lower Austria. It is a 40 km long section of the Danube valley which has been a UNESCO world heritage site since 2000. Because of the sensitive landscape and the standards of UNESCO it is not possible to build flood protection systems in the form of permanent concrete walls or dikes. Therefore, a decision was made to build mobile flood protection systems. They consist of aluminium components which are up to 5 m high. These systems are designed for a 100-year flood. In case of floods they are mounted with the help of volunteer firefighters, which lasts about 12 to 24 hours. If necessary, the firefighters are supported by the Austrian Armed Forces.



*Mobile flood protection during the Danube flood in 2013  
(© Provincial Government of Lower Austria)*



*Aluminium components up to 5 m high  
(© Provincial Government of Lower Austria)*



A cost-benefit analysis shows that this kind of flood protection system is economically successful. Let's take the example of the city of Ybbs: the city was flooded in 2002 and the damage losses were about € 39 mio. The flood protection system was finished in 2012. The costs of the flood protection system have been around € 24 mio. and could completely prevent the flood damage in the city of Ybbs during the flood of 2013.

### Flood Forecasting

After 2002 the Provincial Government of Lower Austria started to improve the flood forecasting systems. In 2002 Lower Austria had a forecasting system only for the Danube which could predict floods for only 12 hours. Now Lower Austria has already 84 gauging stations all over the country which can be found on the website:

<http://www.noel.ov.at/Externeseiten/wasserstand/static/4.m.html>.

At these gauging stations the current water levels and the current discharges are shown. Nineteen of these gauging stations are used to predict floods. The forecasting period is now about 48 hours for the Danube river and 24 hours for other rivers. Close cooperation with the neighbouring regions of Upper Austria, Bavaria and the Czech Republic is very important. They also provide basic data for the forecasting systems.

### Disaster Management

Floods cannot be prevented. Therefore in case of floods efficient disaster management is needed. The Republic of Austria has a highly developed fire fighter service which has also an important function in flood risk management. The special feature is that Austrian firefighters are mostly volunteers organized and only exceptionally organized as professional brigades. In Lower Austria the firefighter service is organized in 1,700 fire brigades with approximately 76,000 firefighters. During the flood in June 2013 about 26,000 voluntary firefighters were in action and had a performance of about 467,000 man-hours.

Because of the fact that the firefighters are mostly volunteers they cannot stay in action for a long time. In such cases the Austrian Armed Forces are deployed. They can support the commitment with the military engineers and with their special equipment, for example with the Black-Hawk S-70 helicopters. The military support is able to stay in action during disasters for a long time with high man power.

The municipalities are committed to elaborate disaster management plans. The main content of such plans are the inundation areas in case of flooding or in case of dike breaks. Furthermore, the areas where people should be evacuated are outlined as well as the so-called „second lines of defense“, where provisional flood protection might be built with sandbags or similar equipment. A further important topic is the position of oil tanks, because broken oil tanks cause most serious pollutions in case of floods.

In the recent years joint trainings of civil authorities, fire fighter services and armed forces were intensified in order to improve cooperation in case of floods. As a base for cooperation common guidelines for the operational management of dikes and a technical manual about monitoring and defence of dikes were published. Both are available on the following website:

[http://www.noel.ov.at/Umwelt/Wasser/Hochwasserschutz/Hochwasserschutz\\_Dammverteidigung.html](http://www.noel.ov.at/Umwelt/Wasser/Hochwasserschutz/Hochwasserschutz_Dammverteidigung.html)



# COMPENDIUM 2015

## Disaster Recovery Subsidy

In the Republic of Austria there is a disaster recovery subsidy. The subsidy is available for private persons and business. The grants mostly amount to 20% of damage loss and up to 50% in special cases. The grants are financed by a federal disaster fund. In case of floods the municipalities evaluate the damages. The Provincial Governments pay out the grants. For example in 2013 about 2,900 cases of disaster recovery subsidy have been reported in Lower Austria.

## EU Flood Directive

During the first step of the implementation of the EU Flood Directive the areas of potential significant flood risk (APSF) were identified. In Lower Austria these areas have a total length of 505 km which is about 5.8% of the total water body surface. In a second step flood hazard maps and flood risk maps were elaborated. At the moment the flood risk management plans are being prepared. They should be published in December 2015. As a base for the management plans all 573 municipalities in Lower Austria were asked about their further flood protection needs. The survey showed that further costs of about € 1,5 billion are to be expected.



The EU co-financed the project CEFAME for coordinated flood risk management (© Lower Austrian Government)

One of the main objectives of the EU flood directive is a close transnational cooperation in joint river basins. An example of such multinational cooperation is the project CEFAME which was led by the Provincial Government of Lower Austria and was co-financed by the EU. In this project the authorities of the Republic of Austria, the Czech Republic, Slovakia and Hungary elaborated coordinated flood risk management for the joint river basins of the rivers Danube, Thaya, Morava and Leitha. The main outputs of the project are the harmonized maps of flood endangered areas, a documentation of current flood management, estimation of potential flood damages, common strategies for flood risk management, an emergency handbook and, last but not least, a Memorandum of Flood Protection with which the project partners declared their further strategic cooperation and to improve flood protection in the joint river basins. More information on this is available at: <http://www.ceframe.eu/>



## The Position of the Female Service Members in the Slovenian Armed Forces

Janja Vuga, PhD, Assistant professor  
Faculty of Social Sciences (University of Ljubljana)  
Kardeljeva ploščad 5, 1000 Ljubljana, Republic of Slovenia,  
[janja.vuga@fdv.uni-lj.si](mailto:janja.vuga@fdv.uni-lj.si)

Ljubica Jelušič, PhD, Full professor  
Faculty of Social Sciences (University of Ljubljana)  
Kardeljeva ploščad 5, 1000 Ljubljana, Republic of Slovenia,  
[ljubica.jelusic@fdv.uni-lj.si](mailto:ljubica.jelusic@fdv.uni-lj.si)

### ABSTRACT

Republic of Slovenia gained its independence in 1991 and Slovenian national armed forces were established based on the former Territorial Defence. Until 2003 when conscription was abolished a small portion of non-commissioned officers and officers was employed in the SAF and an even smaller share of those employed were women, however, the social representativeness in the Slovenian Armed Forces has improved by transiting to the professional army. From then on, all positions within the SAF were open to women. Further on their participation in international operations and missions grew. Nowadays the Slovenian Armed Forces are among the most “feminine” considering the share of female service members (15 percent in 2012). The result of our analysis shows the following: 1) the position of women in the Slovenian Armed Forces has improved over the years, however, they still occupy so-called less important posts; 2) the abolition of the conscription had a positive effect on the posts occupied by women in the Slovenian Armed Forces; 3) women have proven to be as efficient in the international operations and missions as men; 4) the public support of women in the Slovenian Armed Forces (in all positions and all units) has increased over the years.

**KEYWORDS:** Slovenian Armed Forces, male-oriented values, feminization of armed forces, all-volunteer forces, international operations and missions

### 1. INTRODUCTION

Within a national army based on male universal military service, the issue of its social representativeness and legitimacy may arise, since the number of women included in such an army is only symbolic (Jelušič 1995: 5). This issue was addressed in the Slovenian defense system from its very beginning in 1991 while the institutions of the newly independent state were being formed.

The purpose of this article is to provide an overview of the gender structure of the Slovenian Armed Forces (SAF). We will focus mainly on the evolving gender mainstreaming inside the SAF through the past two decades, on the share of female members of the SAF and the positions they occupy within the SAF and on international operations and missions. We will conclude this chapter by presenting the Slovenian public attitude towards the entrance of women into a military organization.

## 2. THE PROCESS OF "FEMINISATION" OF THE SAF

### 2.1. Constitution of an independent country

The emphasis on the representation of women in the SAF at the time of the constitution of an independent country was more a symbolic token than an expression of a real need for a female workforce. Despite that, women were accepted as equals, since many had proven themselves during the ten-day war, and it was important to show women off, even obtaining high military ranks (although they were not being promoted in a regular rank-by-rank career), in order to highlight the distinction between the anti-women culture of the former Yugoslav People's Army and the liberal openness of the military culture of the new Slovenian Armed Forces (Jelušič 2002: 9). Moreover, these women served as proof that the SAF were capable of contributing to the general social emancipation of women.

Further on, at the end of 1993, the Resolution on the Foundations of the National Security of Slovenia gave official voice to Slovenia's aspiration to realize its external security in NATO for the first time. This meant that the military organization had to be built to be compatible with the forces of NATO member states. At first glance it may seem strange to speak of NATO in connection with the issue of women since there were quite a few countries in this organization in 1993 whose forces, in spite of their much greater size (that of Federal Republic of Germany and Republic of Italy at least), contained fewer women than Slovenia's (Jelušič 2002: 10). The question of NATO compatibility opened up the issue of professional soldiers. The recruitment of professional soldiers is a question for the labor market, in which women may also apply as suitable candidates.


The issue of the representation of women in the SAF thus takes on a new dimension after 1995. Military service was increasingly regarded as an institution that discriminated against men rather than as an institution of male social domination due to their mastery of military knowledge (Jelušič 2002: 10-12). Hence the issue of the greater representation of women in the army came to be regarded as proof of a greater fairness in the division of social burdens. In April 2002, the government's proposal to the parliament to abolish the military service and the reserve military service was a watershed in the history of women's inclusion in the SAF (Bric 2002).

### 2.2. An abolition of the military service

After the abolition of military service, it was no longer possible for the army to continue with its tradition of a male-centered culture. From that moment onwards, the army became as socially representative as its internal military culture allowed it to be by letting various social groups join with a view to carry out a military occupation. If in relation to conscripts we can still claim that a small number of women represent a perfectly normal state of affairs, since women are not subject to obligatory military service, the institution's real reasons for or against women will surface when it comes to the all-volunteer force (AVF). Furthermore, the gender balance of the AVF demonstrates to what extent are women really prepared to take part in military activities.

The number of women in a professional army depends in part on their personal readiness for such work, in part on the willingness of the army to accept them, and in part on the public's view of how useful they will be on military assignments.

Immediately following the changes in the employment regime of the Slovenian military in 2003 women represented 13 percent of the total military corps, which placed the SAF among the most feminized armies in the world, alongside the US and Canada (Jelušič 2002: 11). The growing demand for equality



of the genders in the wider civilian environment has played a key role in the decision of the military forces to open its doors. A lack of male recruits has led most societies, under internal or external pressure, to lift bans on the employment of women in the armed forces (Harries-Jenkins 2001: 1).

The data for 2000, when the SAF was still recruited by conscripts, shows that the share of female officers was 2.5 percent while the share of NCOs was 4.7 percent. Due to conscription no female rank and file existed at that time. Prior to the suspension of conscription women rarely occupied leading positions. At that time, the highly specialized units employed the least women, whilst the administrative and financial sectors employed the most (Pešec 2002: 139-140).

The situation with female promotions to more competitive positions changed after the introduction of the AVF. Women work at various levels and occupy different positions in the chain of command; they serve as commanding officers, deputy commanding officers, in various staff functions and other different positions within the military structure at home and in Slovenian units deployed abroad.

### 2.3. New military assignments

We have used the expression 'feminized armies' (see Jelušič 2002: 12) but we have to take into account the fact that women have a long way to go before they are represented in armies at least to the same extent as in other public sectors, or in line with the fact that they constitute half of the world's workforce. The road to a feminized army, that is to say, a state of affairs where women form a majority in military employment, is probably a centuries-long process, or maybe even impossible. Whilst some professions which only a century ago were exclusively male domains have become feminized (e.g. teaching, the health profession), we predict that the army, due to the loss of social prestige, will be forced into greater feminization (Jelušič 2002). We can also conclude that the new tasks and roles of the armed forces have contributed to a larger number of women entering the military (Jelušič 2002; Valenius 2007). Men dominated the armed forces when the job of the armed forces was primarily one of defending the home country or occupying a foreign country. With the establishment of international operations and missions which primarily focus on providing peace and humanitarian tasks following natural disasters, the number of women soldiers has also increased. New assignments, often carried out in post-war environments or even in environments where there is no military threat allow more women to take part. There are two basic reasons for this (Jelušič 2002: 12-13).

Firstly, these assignments do not demand great physical strength or the use of weapons, but, on the contrary, a heightened ability to negotiate, to understand different cultures, to empathize with the civilian population in the area of the operation. Secondly, international operations and missions (IOMs) represent a source of quick and considerable income, particularly in the case of the poorer service members.

Feminization may not only refer to a larger number of women in the army. A proportion of women greater than 10 percent also brings about certain qualitative changes to the institution that is to say, the establishment of a minority culture within the majority culture. Women are no longer a minority which has to adapt to the majority culture, but a group whose values have to be taken into account by the majority culture. More specifically, the feminization of the army presupposes a re-conceptualization of maleness, something which has already happened in wider society. Feminism has brought about changes in the identity of the genders and in the relations between them, so that the acceptability of the concept of maleness as a capability and readiness for violent action has dramatically fallen.

The presence of women has led to a more rational approach to some well-established but emotional

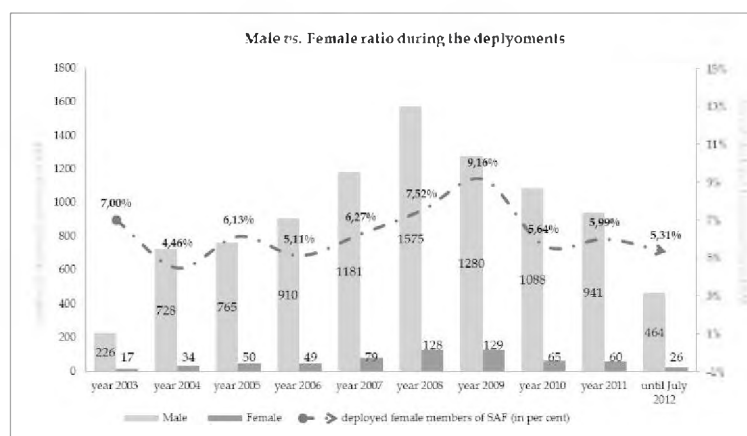
methods of training. The execution of military tasks that may result in death is regarded as more acceptable when men rather than women are sent home in coffins. Precisely these consequences of the feminization of armies bother some military experts, who maintain that women lower the efficiency of the army and must therefore be excluded from combat tasks. Black (2001: 10) even argues that, in combat, where there is no basic front line, where the battle ground is everywhere, the exclusion of women from combat necessarily leads to their complete exclusion from the army as it is no longer possible to determine precisely which areas are combat areas and which are behind the lines. This consideration particularly applies to new wars taking place within a country.

Black's thesis is one of the most radical theses on the consequences of the feminization of the army. He argues that armies containing a large number of women will be used in combat less frequently and that society as a whole will be less inclined to send its military into combat because of the feminization of the army, and less willing to engage in war (Black 2001: 9-10). A Slovenian expert in the sociology of genders has expressed the hope that 'we may assume that the feminization of the armed forces can mean the first step towards the changing of the patterns of everyday life in the direction of reducing violence as the means of ensuring mutual coexistence' (Jogan 2001: 79). However, it should be noted that Slovenian public opinion shows the convergence of opinions among both genders regarding the acceptance of risk, namely, whilst in the past women were more vocal in their opposition to any kind of high risk or combat activities of the SAF, today there appears to be no significant difference between genders anymore (Vuga 2013). The opinions of both men and women indicate a high risk-aversion to combat.


### 3. FEMALE MEMBERS OF SAF IN INTERNATIONAL OPERATIONS AND MISSIONS<sup>2</sup>

During the early years of Slovenia's participation in IOMs, women were rarely found among peacekeepers and in cases when they were deployed it was always on a voluntary basis. That changed in 2003, when whole units were deployed, therefore being deployed was no longer voluntary. The average share of women deployed to IOM between 1997 and 2012 is 8.04 percent.

The numbers in graph 1 demonstrate that the share of women deployed in IOMs has been slowly but steadily rising, reaching its peak in 2009. Since then it has declined.



Graph 1: Male and Female Members of the SAF 2003 - 2012<sup>3</sup>



In the initial years of Slovenia's participation in international peace and security endeavors, the deployed SAF contingents were small and rarely occupying rank and file positions. Therefore, the positions occupied by female members of the SAF were mostly opened to officers or NCOs that volunteered to be deployed in a certain IOM. Due to the suspension of compulsory military service a broader spectrum of positions within the SAF was opened to women and some traditionally male units (e.g. the motorized battalion, reconnaissance platoon, artillery, etc.) were no longer exclusively male. By 1999, the first female officer had been promoted to the position of deputy commander and in 2000 to the position of a commander of the Slovenian contingent in Cyprus. Female SAF members have subsequently assumed other high ranking positions, such as commander of the Slovenian contingent, commander of a task force, senior representative of the contingent, chief of the Information Operations Division, deputy commander of the contingent, commanders of companies, staff positions in multinational headquarters, etc. The first female commander of a motorized battalion took post in November 2011.

Beginning in 2005, the share of female rank and file increased rapidly and, in the period from 2007 until 2009, they outnumbered the previously prevalent officers and NCOs. The data gathered from the SAF shows that deployed women are usually in their mid-thirties; it, therefore, could be presupposed that they are more experienced. A more detailed data analysis reveals that in 2007 the number of female members of the SAF rose to 6.69 percent and in the next two years even to 10.08 percent.

The geographical dispersion reveals that in certain IOMs no female members of the SAF have been deployed so far (e.g. UNIFIL; closed IOMs: NTM-I and EUFOR Tchad/CAR). The highest number of women was deployed to KFOR in Kosovo<sup>1</sup>.

The share of female members deployed in IOMs (approx. 8 percent) remains lower than the share of women in the SAF (approx. 15 percent). There are several reasons for this disproportion in the structure of the IOMs: (1) the maternity role of female members of the SAF creates certain limitations; (2) the deployment to certain positions in the IOM depends on the position the service member occupies in the SAF and women are rarely found at high positions in the SAF structure especially in combat units which are dominantly being deployed to IOMs; (3) the prevailing masculine values and high entering standards limit the possibility for women to integrate within certain units (e.g. the Special Forces Unit).

The interviews conducted with members of the SAF (Vuga 2012) highlight that in the IOM gender relations are an issue, since there are usually few if any joint IOM rules that would regulate such relations. Consequently, the rules of individual AFs apply, regulating gender relations in light of each country's own experience and their prevailing cultural norms.

#### **4. PUBLIC ATTITUDE REGARDING THE GENDER STRUCTURE OF THE SAF**

The gender structure ranks the SAF among the armed forces with the highest share of women (15 percent) who enjoy access to all positions and this has been one of the sources of SAF's legitimization.

---

<sup>1</sup> This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence. (In accordance with Arrangements regarding regional representation and cooperation.)

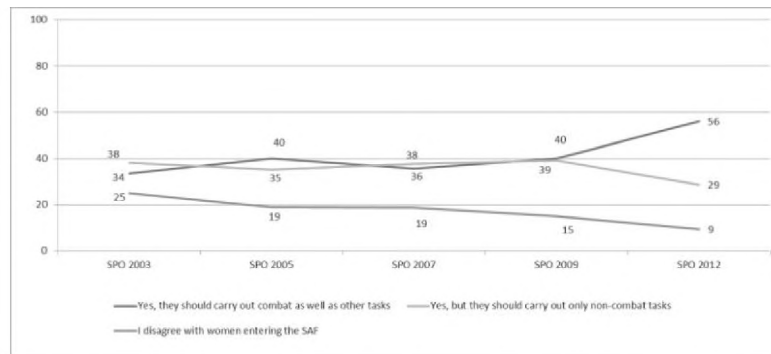
# COMPENDIUM 2015

76 percent of the public believes the share of women in the SAF is appropriate or even too small (see table 1) and a similar share of the public believes that women should have equal career opportunities. This reveals the Slovenian national character's inclination towards equal opportunities and a feminine culture (see Hofstede, 2001).

There are approx. 15 percent of women in the SAF. In your opinion, does that number signify that...	SPO 2007	SPO 2009	SPO 2012
there are too many women	13.20 %	11.80 %	10.90 %
there are not enough women	15.90 %	16.30 %	17.20 %
the share is appropriate	53.80 %	57.10 %	58.70 %
don't know, n.a.	17.10 %	14.80 %	13.20 %


*Table 1: Public Attitudes towards the Current Gender structure in the SAF*

If the gender-based differences had been significant through the previous measurements, they became almost nonexistent in the latest measurement in 2012. Therefore, the attitude towards the feminization of the SAF and female participation in the SAF as well as in the IOMs is relatively uniform and supportive. Even previously divided opinions regarding the type of tasks women should be allowed to perform has become more uniform, since the majority of the population supports the idea of women entering combat units and performing high-risk tasks (see graph 2).



*Graph 2: Public Attitudes towards Women Entering the Military Organization (percentage)<sup>4</sup>*

According to the findings of some authors (Kotnik 2002), women should not be in combat units, because the death of a woman weakens the morale of a unit much more than the death of a man. De Konink (2000) explains that male soldiers perceive their female colleagues as their mothers, sisters, wives, etc. and, therefore, losing a female soldier in battle is much harder to cope with than losing a male soldier. Furthermore, the analysis of the general public's opinion shows that women are traditionally less inclined to support high-risk operations because they perceive soldiers as their sons. It was assumed by Vuga (2011: 89-90) that this works both ways: namely men also perceive female



soldiers as their daughters (a factor which did not play an important role when the military organization was an exclusively masculine organization).

## **5. CONCLUSION**

The military organization is characterized by prevailing male-oriented values (Cohn 1993; Dunivin 1994; Carreiras 2010). Despite the changing nature of the tasks related to intense participation in IOMs, this value system remains present as a result of the predominantly male structure and women's tendency to adopt male behavioural patterns in order to escape the stereotypes (Trompenaars and Hampden - Turner 1998: 227). This statement is also valid for the SAF.

During the ten years of professionalization of the SAF, the presence of women opened up many of the known issues, related to the feminisation of the armies in general. As the Republic of Slovenia has not had any victims due to the cooperation in IOMs yet, we are not able to prove the thesis of less acceptable female victims to the public. We still have to rely upon the abstract view of the public on this issue, or we may make some conclusions on the basis of more indirect events (see Vuga 2013).

The improving position of female SAF members in IOMs was proven by their presence in higher staff and commanding positions in the international headquarters of IOMs, but less so in the SAF structure; namely, the first female officer was appointed a brigade general (officer six in NATO terminology) in 2011. However, it should be added that even though that there have been some cases of promotion of female service members to high positions of power in the SAF, it is the women's prevailing opinion that they still occupy so-called less important positions and the real power of decision making is rarely handed over to a woman. As some of the high ranking female service members in the SAF concluded, women are much more self-critical than men and they more often decline an offer to a certain position because they are either not sure about their own competence or they have worries about balancing their family and paid work.

Female members of SAF have proven themselves with the quality of their work and have received a credit by members of various AF in multinational environments. As one of the female service members said .../'in some cases women are even better leaders, since they are more sensitive and curious, ask about other people's feelings more often and, therefore, establish more genuine contacts with their co-workers'. This leads to the conclusion that women can be added value to the military organization by keeping their values and their way of "doing the job" instead of adapting to the male-oriented military culture.

## **ACKNOWLEDGMENT**

The extended version of this article has been published as part of the book *Small, but smart?: the structural and functional professionalization of the Slovenian Armed Forces*. Baden-Baden: Nomos, 2015.

Authors would like to take this opportunity to thank all the female and male service members of the SAF who contributed to our research findings by participating in various research projects over the past years.



## 6. REFERENCES

<sup>1</sup> Statistically, women are not the greatest problem in relation to military readiness and efficiency. Judging by the results of research in professional armies, the integration of women into the army had very limited effects on military readiness, cohesion and morale. Much more decisive for this are command, training and the amount of work being carried out in a unit (Rand Research Brief 1999).

<sup>2</sup> The data regarding gender based structure of deployments of SAF in IOM used in this chapter was gathered by the Slovenian Armed Forces; namely the General Staff (Liliana Brožič, PhD and her team) and Forces Command (LtC Marko Prvinšek and his team). Due to different methodologies of registering deployed members of SAF and various data bases there is a possibility of some slight deviations in numbers.

<sup>3</sup> The numbers presented include officers, non-commissioned officers, rank and file and other military personnel.

<sup>4</sup> The question posed was "Do you agree with women entering the Slovenian Armed Forces?"

## 7. LITERATURE

**Black, Jeremy** (2001). *War in the New Century*. (London and New York: Continuum.)

**Bric, Roman** (2002). *Naborniki še do leta 2004 (Conscripts until 2004)*. Slovenska vojska, Vol X, 13, 12 July 2002; 13-20.

**Carreiras, Helena** (2010). *Gendered Culture in peacekeeping Operations*. *International Peacekeeping* 17(4): 471-485.

**Cohn, Carol** (1993). *Wars, Wimps and Women: Talking Gender and Thinking War*. In Miriam Cooke and Angela Woollacot (eds). *Gendering War Talk*. New York: Princeton University Press: 227-246.

**De Konink, Marjike** (2000). *Women's Empathy, Men's Victory?* In Marjan Malešič (ed). *International Security, Mass Media and Public Opinion*. Ljubljana: FDV: 212-232.

**Dunivin, Karen** (1994). *Military Culture: Change and Continuity*. *Armed Forces & Society* 20 (4): 531-547.

**Harries-Jenkins, Gwyn** (2001). *Women in Extended Roles in the Military: The Legal Issues*. Paper at Biennial International Conference of Inter-University Seminar on Armed Forces and Society, October 19-21, 2001.

**Hofstede, Geert** (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*. London and New Delhi: Sage Publications.

**Jelušič, Ljubica** (1995). *Ženske in oborožene sile (Women and the Armed Forces)*. In Zorica Bukinac (ed). *Zbornik študij*. Ljubljana: Ministrstvo za obrambo RS (Ministry of Defense of the Republic of Slovenia).

**Jelušič, Ljubica** (2002). *Feminization of the military organization*. In Ljubica Jelušič and Mojca Pešec (eds). *Sexism in the Military Uniform*. Ljubljana: FDV.

**Jogan, Maca** (2001). *Seksizem v vsakdanjem življenju (Sexism in Everyday Life)*. Ljubljana: Znanstvena knjižnica, Fakulteta za družbene vede.

- Kotnik, Igor (2002). *Preoblikovanje oboroženih sil sodobnih evropskih držav*. Ljubljana: FDV.
- Pešec, Mojca (2002). Women in Slovenian Armed Forces. In Ljubica Jelušič and Mojca Pešec (eds). *Sexism in the Military Uniform*. Ljubljana: FDV: 138-142.
- Rand Research Brief, **Military readiness: Women are not a Problem**.  
<http://www.rand.org/publications/RB/RB7515/> 22.1.1999.
- Slovenian Public Opinion 2005/2: National and International Security and International Electoral Survey [data file]**. Jelušič, Ljubica / Malnar, Brina et al. Slovenija, Ljubljana: Faculty of Social Sciences, Defense Research Centre, Centre for Public Opinion Research and Mass Media [execution], 2005, Ljubljana: University of Ljubljana, Faculty of Social Sciences, Archive of Social Data. [distribution], 2009.
- Slovenian Public Opinion 2007/1: Opinions about National and International Security; Military Profession [data file]**. Malešič, Marjan et al. Slovenia, Ljubljana: Faculty of Social Sciences, Defense Research Centre, Centre for Public Opinion Research and Mass Media [execution], 2007, Republic of Slovenia, Ljubljana: University of Ljubljana, Faculty of Social Sciences, Archive of Social Data. [distribution], 2010.
- Slovenian Public Opinion 2009/2: Opinions about National and International Security [data file]**. Malešič, Marjan / Malnar, Brina / Toš, Niko et al. Republic of Slovenia, Ljubljana: Faculty of Social Sciences, Centre for Public Opinion Research and Mass Media [execution], 2009, Republic of Slovenia, Ljubljana: University of Ljubljana, Faculty of Social Sciences, Archive of Social Data. [distribution], 2010.
- Slovenian Public Opinion 2012/1: Opinions about National and International Security [data file]**. Malešič, Marjan / Malnar, Brina / Toš, Niko et al. Republic of Slovenia, Ljubljana: Faculty of Social Sciences, Centre for Public Opinion Research and Mass Media [execution], 2009, Republic of Slovenia, Ljubljana: University of Ljubljana, Faculty of Social Sciences, Archive of Social Data. [distribution], 2012.
- Trompenaars, Fons in Hampden-Turner, Charles (1998). *Riding the Waves of Culture* (second edition). New York: McGraw-Hill.
- Valenius, Johanna (2007). A Few Kind Women: Gender Essentialism and Nordic Peacekeeping Operations. *International Peacekeeping* 14(4): 510-523.
- Vuga, Janja (2011). *Public Perceptions of Casualties in Peace Operations: The Effects of Potential Casualties on Public Support in Case of Slovenia*. In Marjan Malešič in Gerhard Kummel (eds). *Security and Military between Reality and Perception*. Baden-Baden: Nomos Publishers: 79-93.
- Vuga, Janja (2012). *Cross cultural cooperation in multinational operations and missions: case of the Slovenian Armed Forces*. Doctoral thesis. FDV. Available at:  
[http://dk.fdv.uni-lj.si/doktorska\\_dela/pdfs/dr\\_vuga-janja.PDF](http://dk.fdv.uni-lj.si/doktorska_dela/pdfs/dr_vuga-janja.PDF) (Retrieved 14 June 2013).
- Vuga, Janja (2013). *Safety bubble vs. risk awareness: Casualty aversion among the Slovenian public*. *Armed Forces & Society*, first published on March 7, 2013.  
doi:10.1177/0095327X12465814.
- Women, Peace and Security**. 2002. Available at:  
<http://www.un.org/womenwatch/daw/public/eWPS.pdf> (Retrieved 5. April 2012).

## **International and Regional Cooperation with Focus on Euroatlantic Integration**



## Civil-Military Relations in the Protection and Rescue Field

Col Slavko Angelevski Phd<sup>a,1</sup>

<sup>a</sup> Military Academy "General Mihailo Apostolski" - Skopje, MK

### ABSTRACT

The article addresses three basic questions concerning civil-military relations in the protection and rescue field: *Why, When and How* the military should be involved in disaster response. In a crisis situation causing widespread damage the response need is far greater than the response available and this is why the military should be involved in the protection and rescue field or, generally, in disaster response. This article explores Civil-Military Co-Operation (CIMIC) as a military function through which a commander links to civilian agencies and addresses key documents explaining it. Also, it suggests that the military is not an instrument of first resort in humanitarian response but supports civilian relief agencies. Military actors are likely to seek to establish relationships with the civilian population and in many cases attempt to provide them with assistance because the military forces can provide useful resources and support to the affected country or region, population or humanitarian actors.

**KEYWORDS:** Disaster, Crisis, Civil-Military Co-Operation, Host Nation Support, Military capabilities, Support operations.

### Introduction

If we look in the dictionary we can find different definitions of the word "disaster." These are just a few: an occurrence causing widespread destruction and distress; a catastrophe; a grave misfortune; or, informal - a total failure. Generally, we can define disaster as a crisis situation causing widespread damage which far exceeds our ability to recover. It can be man-made or natural, but in any case a key element in this situation is that a response need is far greater than the response available. This means that in a response to crisis situations we have to engage all available resources, including the military.

It seems that when disasters occur, either natural or man-made, governments often turn to the military for help as the military has certain resources immediately at hand, such as food, medicine and fuel as well as transport and human assets with which to distribute them. This is the answer to the question why the military should be involved in the protection and rescue field or, generally, in disaster response. The way how to coordinate these activities is connected with the term "civil-military co-operation" or with the well known acronym CIMIC.

---

<sup>1</sup> Corresponding Author: Col. Slavko Angelevski, Ph.D., Associate professor at the Military Academy "General Mihailo Apostolski" - Skopje, Str. Vasko Karangeleski b.b., 1000 Skopje, MK; E-mail: angel@va.edu.mk

## Civil-military co-operation (CIMIC)

Civil-military co-operation (CIMIC) is the military function through which a commander links to civilian agencies active in a theatre of operations. It is concerned with coordination and joint planning with civilian agencies in support of the mission. Through the CIMIC functions the provision of any of a variety of forms of assistance (expertise, information, security, infrastructure, capacity-building, etc.) to the local population is considered in support of the mission.

The key document explaining the NATO CIMIC doctrine is "Allied Joint Publication 9"<sup>2</sup>. This document constitutes one level in the hierarchy of NATO documents covering CIMIC policy and doctrine as well as tactics, techniques and procedures (TTPs). It reflects the NATO Military Policy for CIMIC and is coherent with the guidance for Allied joint doctrine. The document focuses primarily - but not entirely - on the operational level.

Civil-military cooperation, as a military capability and as a theoretical idea was conceptualized, developed and applied for the first time in its present form by NATO in the context of its commitment in the Balkans. This development was originally triggered by an operational-level reorientation of the deployment of forces in significantly changing conflict scenarios after the end of the Cold War. The main objective was the creation of a military tool for analysis and action that would integrate the "civil dimension" in an effort to meet the challenges posed by unclear confrontation patterns between opposing forces, changing geographical conditions, political and ethnic considerations and domestic and international factors.<sup>3</sup>

There are a number of associated activities within this spectrum which, although different, are either closely associated with CIMIC or can be confused with it. Principal among these associated activities are:

- *Military Assistance in Humanitarian Emergencies (MAHE)*. In the broadest sense CIMIC is primarily concerned with co-operation with rather than support or assistance to civilian bodies, although at the practical level support will, of course, take place. MAHE, for example, in the context of disaster relief, can take place nationally or internationally. In both cases a national or multinational military force is called upon to carry out specified tasks for finite periods under the direct auspices of a civilian authority. That authority may be national or international in nature.
- *Civil Emergency Planning (CEP)*. CEP is concerned with the protection of and support to domestic populations, usually in the context of disasters or war. In the current security environment, a core function of CEP is to remain responsive to military planning in both Article 5 and non-Article 5 operations. This includes planning for civil support such as strategic logistic and communications facilities.
- *Host Nation Support (HNS)*. HNS seeks to provide the NATO Commander and the sending nations with support available in the form of material, facilities and services including area security and administrative support in accordance with negotiated arrangements between the sending nations

---

<sup>2</sup> AJP-9 "NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE", June 2003.

<sup>3</sup> Hans-Jürgen Kasselmann, "Civil-Military Cooperation - eine militärische Notwendigkeit und Fähigkeit zur Lösung von komplexen Krisenlagen," in: *Neue Formen und Instrumente der Entwicklungszusammenarbeit*, ed. Rainer Öhlschläger and Hartmut Sangmeister (Baden-Baden, Germany: Nomos Publishing, 2012).

and/or NATO and the host government. As such, HNS facilitates the introduction of forces into an area of operations by providing essential reception, staging and onward movement support. HNS may also reduce the extent of logistic forces and material required to sustain and re-deploy forces that otherwise would normally be provided by the sending nations. CIMIC will normally be employed to facilitate the execution of HNS.

The dissolution of the traditional border between civilian and military crisis management, mainly by deliberate efforts to introduce hybrid, civilian/military crises management operations, has been one of abandonment of the concept at the EU level, though EU member states have used it at the national level. The limits of CIMIC for a comprehensive coordination between civilian and military sides of ever more complex EU crisis management operations are seen in the fact that the concept has been derived from a military perspective primarily concerned with force protection and the reason for cooperation with non-military actors is subordinated to that aim.<sup>4</sup>

## Civil-Military Relations in the Protection and Rescue Field

Discussions about the most effective, efficient and sustainable approach to resolving complex crisis situations have a long historical tradition, even if ongoing debates among politicians and researchers may suggest otherwise. However, an analysis of relevant publications in military and security policy or social science over the last few years clearly shows that different perspectives prevail. From a military viewpoint, the focus is typically on determining the right tactical approach and the broader debates are only tangentially helpful. By contrast, the civilian side emphasizes that the resolution of complex crisis situations should primarily be obtained through civilian tools.<sup>5</sup>

The military is not an instrument of first resort humanitarian response but supports civilian relief agencies. The military may be involved when:

- The military provides a unique service
- Civilian response capacity is overwhelmed
- Civilian authorities request assistance


When the military does become involved, then the military mission should be clearly defined; the risks should be minimal and core military missions should not be affected (military missions have priority). We should always follow the principle "LAST IN, FIRST OUT".

In immediate/serious situations commanders in the field may take action when conditions and time do not permit approval from higher authorities to: save lives, prevent human suffering and mitigate great property damage. In those situations they must inform the regional planning agent and the national chain of command and also disengage as soon as possible.

---

<sup>4</sup> Khol, R., 2006, 'Civil-Military Co-Ordination in EU Crisis Management', In: Nowak, A. (ed.), *Civilian Crisis Management: The EU Way. Chaillot Paper No. 90* (June 2006), page 124.

<sup>5</sup> Hans-Jürgen Kasselmann, "Civil-Military Cooperation - eine militärische Notwendigkeit und Fähigkeit zur Lösung von komplexen Krisenlagen," in: *Neue Formen und Instrumente der Entwicklungszusammenarbeit*, ed. Rainer Öhlschläger and Hartmut Sangmeister (Baden-Baden, Germany: Nomos Publishing, 2012).



In the last few decades engagement of the military is more focused on deterring war, resolving conflict, promoting peace and supporting civil authorities in response to domestic crises. In this context the phrase Military Operations Other Than War and the acronym MOOTW was coined by the United States military during the 1990s, but it has since fallen out of use. More recently, we are talking about "Support operations" that employ army forces to assist civil authorities, foreign or domestic, as they prepare for or respond to crisis and relieve suffering. The key document explaining this kind of operations is FM 3-0.<sup>6</sup>

In June 1998 a Euro-Atlantic Disaster Response Coordination Centre (EADRCC) was established at the NATO Headquarters and it's operational on a 7/24 basis. Since its launch, the EADRCC has been involved in a great number of different operations around the world ranging from coordination of relief supplies to refugees, aid to flood, hurricane and earthquake victims, fighting forest fires and other forms of assistance to different countries.

As the EU's crisis management activities demonstrate, it is especially the doctrinal and operational need to consolidate civil-military coordination. Increasingly, EU crisis management missions are operations that combine military and civilian aspects which need to be built into the plan in a holistic way and executed seamlessly. It is for this reason that a number of specialized bodies have been erected and transformed within the EU and the Lisbon Treaty to further this process. In respect of decision-making structures relevant for EU crisis management, the Helsinki European Council established three new permanent political and military bodies within the Council: Political and Security Committee (PSC), the Military Committee (EUMC) and the Military Staff (EUMS). The PSC's role in crisis management is aimed at the political control and strategic direction of the operation. Also, the PSC is set to send guidelines to the EUMC, a body composed of the Chiefs of Defense. The EUMC's responsibility towards the PSC has been the provision of military advice and recommendations. In regard to the EUMS, it takes military direction from the EUMC and its function has been the production of Military Strategic Options (MSOs) and conduct of EU-led military crisis management operations. 'Once the MSOs have been produced, the EUMC prioritizes them and the PSC decides on the preferred course of action'.<sup>7</sup>

The standard guide for civil-military relations in the protection and rescue field is "Civil-Military Coordination Officer Field Handbook"<sup>8</sup>. It is the essential dialogue and interaction between civilian and military actors in humanitarian emergencies that is necessary to protect and promote humanitarian principles, avoid competition, minimize inconsistency and, when appropriate, pursue common goals. Basic strategies range from coexistence to cooperation. Coordination is a shared responsibility facilitated by liaison and common training.

In most humanitarian emergencies (complex and natural) the UN agencies and the members of the international humanitarian community responding to the disaster will encounter armed actors. Now, more than ever before, there are likely to be multiple types of forces, including foreign, international or multinational forces. When such actors are present there are significant coordination challenges in the realms of security, medical evacuation, logistics, transport, communications, information management and others. The challenges include such issues as ensuring that humanitarians have the access they require, but at the same time do not become a target. Other challenges include minimizing the

---

<sup>6</sup> Field Manual FM 3-0 "OPERATIONS", Headquarters Department of the Army, Washington DC, 27 February 2008, p. 1-15-16.

<sup>7</sup> Simón, L., 2010, 'Command and Control? Planning for EU Military Operations', *EU/ISS Occasional Paper* No. 81, January 2010, page 13.

<sup>8</sup> Civil-Military Coordination Officer Field Handbook, Version E 1.0, Presented to the Consultative Group on the Use of MCDA in Geneva on 29 November 2007.



competition for scarce resources such as ports, supply routes, airfields and other logistics infrastructure.

In addition, most of these armed actors are likely to seek to establish a relationship with the civilian population and in many cases attempt to provide them with assistance. In some cases, the military forces can provide useful resources and support to the affected country or region, population or humanitarian actors. In other cases, the perceived association with the armed actors can compromise the humanitarian efforts and may pose an additional security threat. Dealing with these challenges requires training, appropriate experience and in some cases dedicated staff.

Military capabilities can support the civil environment directly on a subsidiary basis or in the event of an ethical-moral obligation. This can be achieved through civil-military cooperation in the implementation of projects and measures, but also as direct assistance administered by available military forces. There are multiple possibilities, as military contingents usually have capabilities in their force posture that can be adjusted to support civilians in an emergency. Examples include medical support for the population, logistic transportation support and the use of military engineering equipment for civilian purposes. The main focus here is on the direct and immediate involvement of the local administration and government institutions, as well as the integration of the population.

To face the new challenges associated with the coherent implementation of a comprehensive approach in all civil-military relations, including within NATO, major adaptation is required in terms of concepts, capabilities and administration. To achieve the desired optimization of cooperation in complex crisis situations, it is necessary to break the isolation of CIMIC at the tactical implementation level, which, as a rule, consists of national troop contingents assigned to NATO. Capabilities must be provided cohesively in a top-down approach at all levels, ranging from the politico-strategic level, the crucial planning conducted at the operational level down to the theater level.

## References

- [1] AJP-9 "NATO CIVIL-MILITARY CO-OPERATION (CIMIC) DOCTRINE", June 2003.
- [2] Hans-Jürgen Kasselmann, "Civil-Military Cooperation - eine militärische Notwendigkeit und Fähigkeit zur Lösung von komplexen Krisenlagen," in: *Neue Formen und Instrumente der Entwicklungszusammenarbeit*, ed. Rainer Öhlschläger and Hartmut Sangmeister (Baden-Baden, Germany: Nomos Publishing, 2012).
- [3] Khol, R., 2006, 'Civil-Military Co-Ordination in EU Crisis Management', In: Nowak, A. (ed.), *Civilian Crisis Management: The EU Way. Chaillot Paper No. 90* (June 2006).
- [4] Field Manual FM 3-0 "OPERATIONS", Headquarters Department of the Army, Washington DC, 27 February 2008.
- [5] Simón, L., 2010, 'Command and Control? Planning for EU Military Operations', *EU/ISS Occasional Paper No. 81*, January 2010.
- [6] Civil-Military Coordination Officer Field Handbook, Version E 1.0, Presented to the Consultative Group on the Use of MCDA in Geneva on 29 November 2007.



## **Cyber Security Strategy as a “Must” for South-East European Countries**

Associate Professor **Metodi Hadzi-Janev**, Colonel  
Military Academy “General Mihailo Apostolski Skopje”,  
University “Goce Delcev” - Stip  
e-mail: metodi.hadzi-janev@ugd.edu.mk

**Keywords:** national cyber security strategy, cyber crime, cyber defence, civilian cyber defence

### **ABSTRACT**

Information and telecommunication technologies play a crucial role in social, economic and political activities in the region of South East Europe (SEE). However, the growing dependence on these technologies in SEE has not been matched by a parallel focus on security. This article argues that SEE governments must create concrete strategic guidance for cyber security, i.e. cyber security strategies. In order to be effective the future cyber security strategies produced by the SEE governments must have a “whole-of-government” approach. To accomplish these future cyber security strategies they must address cyber crime, cyber defence, cyber intelligence and counterintelligence, critical information infrastructure protection and crisis management and cyber diplomacy and cyber governance.

### **Introduction**

Complex geopolitical dynamics and the advance in technological development have affected security in a unique way. On the one hand, they have brought progress and success. On the other hand, these processes have brought serious challenges to security. Today, most of the social, political and economic activities are taking place in the so-called “cyber world”. Exploiting the challenges that stem from the cyberspace state and non-state actors (groups and individuals) with negative agendas they have started to pose serious threats to our security.

South East European countries depend on the development of safe and secure cyberspace. The cyberspace security risks have not, however, been addressed through strategic guidance. Thus, effective cyber security strategy is a must for the region itself. The main hypothesis is that while building the future cyber security strategy SEE governments need the “whole-of-government” approach. This approach must establish an appropriate balance between security on the one hand and social, political and economic needs on the other hand.

### **1. Global security trends in the context of South East European security**

The fall of communism has rapidly changed the political landscape in the region of South-Eastern Europe (SEE). Along with the process of democratization the environment in SEE had brought forth many new opportunities to the socialist- oriented societies. Parallel to this, the global trend of

technological development has improved the means of communication and opened many new opportunities. At the same time the transition to democracy has erased the government-controlled vertical corporations. Hence, the new and flattened environment has dismantled the geographical, political and cultural boundaries.<sup>1</sup>

The Euro-Atlantic integration processes have also influenced SEE. By holding in high esteem liberal and democratic values and virtues SEE governments, among others, have introduced the freedom of movement of goods, money, services and people. The new political set-up has introduced capitalist-based corporate systems that have begun to run everyday life in the SEE countries. These systems and services that they provide are run by private, non-state actors. As in the rest of the world, both systems and services are interlinked and go beyond national borders. Global processes run through such systems and services bring a fundamental shift in the spatial scale in human social organizations that link distant communities and expand the reach of power.<sup>2</sup>

The information and communication technology (ICT) and the use of cyberspace play a crucial role in the region of SEE. The pursuit of modernization, the Euro-Atlantic integration and the necessity of foreign investments, among others, have urged SEE countries to invest in the development of ICT and cyberspace. Thus, although virtual, cyberspace has become the dominant place for social, economic and political activities in the region of SEE. These activities have brought on both positive and negative effects.

The geographical position and Euro-Atlantic aspirations of its populace and political elites urge SEE countries to seriously consider the current political and security dynamics. It is obvious that in order to ensure their stability SEE governments must follow current trends in the cyber domain. This is why many have invested in the development of the so-called "informatics society".<sup>3</sup>

As Brian Forst concludes, globalization and technological development have *introduced many side effects by scrambling everything and thus affecting the previously designed international order*.<sup>4</sup> Thus, the new flattened environment in general introduced the so-called hybrid security threats.<sup>5</sup> The new non-state adversaries are a mix of terrorists, criminals, insurgents and religious extremists. By relying on modern technology (especially information technology) and (ab)using modern processes these hybrid adversaries pose asymmetric and unconventional threats to SEE. At the same time, none of the SEE governments at the moment of writing of this article have a cyber security strategy.

## 2. Do SEE countries need a Cyber Security Strategy?

Economic, political and security reasons urge SEE governments to consider a national cyber security strategy. Political reasons for such an effort stem from security dynamics and Euro-Atlantic

---

<sup>1</sup> Friedman, L. Thomas, *The World is Flat*, Farrar, Straus & Giroux, 2005


<sup>2</sup> McGrew, Anthony, "The Globalization of World Politics", in ed. J Baylis; S. Smith and Patricia Owens, "An Introduction to International Relations", 5th. ed. Oxford, 2010, pp. 14-31.

<sup>3</sup> Government of the Former Yugoslav Republic of Macedonia\* - Ministry of Informatic Society, "National Strategy for e-Government 2010-2012", January 2010, Original: „Национална стратегија за е Влада, 2010-2012“)

\* Turkey recognizes the Republic of Macedonia with its constitutional name.

<sup>4</sup> Brian Forst, *Terrorism, Crime and Public Policy*, Cambridge University Press, 2009, p. 86

<sup>5</sup> The U.S. Department of defense, "Quadrennial Defense Review", Report 8, (2010)



aspirations. Both the revised NATO Policy on Cyber Defense of 8 June 2011<sup>6</sup> and the Chicago Summit Declaration of May 2012<sup>7</sup> have stressed the importance of cooperation with partner nations in order to achieve greater cyber security. Although a “storm cloud still emerges from the European Union's cyber security strategy”<sup>8</sup> regarding its lack of clarity to protect cloud computing this document clearly confirms the importance of addressing cyber security too.

Cyber security challenges pose serious security threats that could directly and indirectly undermine the peoples' trust in the system when the former is incapable to provide effective protection. It could be argued, though, that to some extent this is understandable since cyberspace has not been designed with legal and security considerations in mind. The Internet and the concept of “national security” were developed along separate and divergent paths. After the Cold War these paths are converging in a way that makes the Internet problematic and even threatening to national security.<sup>9</sup>

Technical considerations regarding cyberspace represent a serious challenge to the SEE countries' national securities too.<sup>10</sup> Thus the “paradox of modernity”<sup>11</sup> in the context of cyber security also affects SEE. The more we depend on modern technology the more vulnerable we are. Therefore, if SEE governments are about to ensure economic development they need to invest in a safe and secure environment. Achieving such an environment requires measures, instruments and mechanisms that will convince clients, investors, consumers and citizens about cyber security too.

There are general and specific based cyber threat vectors that urge SEE countries to consider the cyber security strategy. Last year, for example, Jose Pagilery reported that in a “massive hack” more than 2 million Facebook, Gmail and Twitter users suffered from password takeover.<sup>12</sup> Among the compromised data were 41,000 credentials used to connect to File Transfer Protocol (FTP, the standard network used when transferring big files) and 6,000 remote log-ins. The 2014 Symantec report shows that 2013 was a year of a mega breach; Targeted Attacks Growth; increased Zero-day Vulnerabilities and Unpatched Websites; Facilitated Watering-Hole Attacks; Social Media Scams and Malware Flourish on Mobile; Ransomware attacks and the year where attackers turned into the internet of things.<sup>13</sup> Along with the global trends the region of SEE is not immune to the negative effects coming from cyberspace.

According to the local SEE and world news, recent reports and studies, many SEE countries are facing experienced cyber activists but the awareness of these threats is not promising. The news reports, back in May of 2013, for example, informed that three Romanian nationals were caught taking part in a multimillion dollar cyber fraud ring that specifically targeted U.S. consumers and the trio ended up

---

<sup>6</sup> NATO Public Diplomacy Division, “Defending the Networks, The NATO Policy on Cyber Defence”, June 8, 2011

<sup>7</sup> NATO Homepage, Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, retrieved (May 3, 2013 from: [http://www.nato.int/cps/en/natolive/official\\_texts\\_87593.htm](http://www.nato.int/cps/en/natolive/official_texts_87593.htm))

<sup>8</sup> European Union, “The cybersecurity strategy “An Open, Safe and Secure Cyberspace””, The European Commission and High Representative of the Union for Foreign Affairs and Security Policy, February 7, 2013, retrieved May 5 from: <http://www.eda.europa.eu/info-hub/news/2013/02/08/european-union-strategy-for-cyber-security>

<sup>9</sup> Gary Chapman, *National Security and the Internet*, The 21st Century Project, LBJ School of Public Affairs, July 1998, p 5

<sup>10</sup> See in depth discussion in: Weber H. Rolf, “Internet of Things New security and Privacy challenges”, *Computer Law & Security review* 26, 2010, pp 23-30

<sup>11</sup> For a more general discussion on this topic see: Anthony Giddens, *The Consequences of modernity*, Stanford University Press, 1990

<sup>12</sup> Jose Pagilery, “CNN Money”, November, 2013

<sup>13</sup> Symantec, “Internet Security Threat Report”, Volume 19, 2014

making off with more than \$2 million.<sup>14</sup> Although not a regional trend per se, the mysterious disappearing of a cyber crime writer in Bulgaria in 2010 and 2011 shows that actions in SEE cyberspace have significant influence on security.<sup>15</sup> Although reports misinterpreted the information, a young hacker from The Former Yugoslav Republic of Macedonia<sup>16</sup> back in 2012 was detained due to cyber crime allegations (i.e., attempting to penetrate illegally several security websites in the US).<sup>17</sup> These and similar reports attest why SEE countries need to consider cyber challenges in a more organized, systematic and professional manner.

### 3. Building a national cyber security strategy as a “Must” for the SEE countries' leaderships

Addressing cyber security challenges is a complex task. Modern and complex threats that stem from the interconnected and interrelated environment have urged strategic thinkers around the globe to shift the approach to overall national security. In general, while addressing their own national security strategy many states have moved from a few specific threats based on a strategic approach to mitigate the myriad risk strategic approach. In this light, while building their national security strategies, states have started to mention the term cyber security more often than before and have dedicated a broader focus to it.

Australia, for example, published its First National Security Statement to its Parliament in 2008.<sup>18</sup> In the Federal Republic of Germany until 2008 the term 'Sicherheitspolitik' was analogous to the English term 'national security'. This trend continued and in 2011 the Federal Republic of Germany launched its Cyber strategy. In this document the German government focuses on preventing and prosecuting cyber-attacks and also on the prevention of coincident IT failures, especially where critical infrastructures are concerned. According to the French government documents, 'cyber defence' aims to protect the security of France's 'critical information systems' according to 'information assurance measures'.<sup>19</sup>

Development of the national cyber security strategy must be understood as a tool that will help the society to reach a desired state of affairs. It is not an end in itself. Therefore, SEE countries' leaderships need to recognize the emerging problem and set forth goals and adequate strategic framework to address it.

Current cyber security threats straddle the boundaries between different public sectors. These include (but are not limited to) law-enforcement, national defence, crisis management, economic efficiency and public diplomacy and governance. Furthermore, current practice shows that cyber security threats could be interconnected and interlinked affecting different social sectors at a specific the time.

---

<sup>14</sup> Amaruso John, "Romania Global Center for Cyber Crime in USA", USA Today, (January 14, 2014), retrieved 22 March 2014 from: <http://guardianlv.com/2014/01/romania-global-center-for-cybercrime-in-u-s/>


<sup>15</sup> Leavitt Lydia, "Cybercrime writer mysteriously disappears in Bulgaria", January 25, 2011,

<sup>16</sup> Turkey recognizes the Republic of Macedonia with its constitutional name.

<sup>17</sup> \_\_\_\_\_, (November 20, 2012), "FBI Arrested Young Hacker from Struga" Press 24 retrieved on 22 Sept. 2013 from: <http://star.press24.mk/story/poznato/foto-fbi-uapsi-miad-haker-od-struga-sin-na-poznata-struzhanka>

<sup>18</sup> Australian Prime Minister, The First National Security Statement to the Australian Parliament (Canberra: Australian Government, 2008)

<sup>19</sup> French Secretariat-General for National Defence and Security, Information systems defence and security. France's strategy (Paris: French Network and Information Security Agency, 2011)



Thus, while considering cyber security threats the SEE leaderships must balance the economic, legal and social importance of free flow of information with the security needs of the government, industry and citizens. Hence, the national cyber security strategy should span more than five cornerstone areas. These cornerstone areas are: countering cyber crime; cyber defence addressed by cyber military specialists; intelligence and counterintelligence; critical infrastructure protection and crisis management and cyber diplomacy and cyber governance.

Effective response to cyber security threats thus must be comprehensive and highly coordinated among all stakeholders. Consequently, this will require a response from different stakeholders (public and private sectors included). So far, all of these areas have been addressed by the specific documents in the broader national security context, separate from cyber threats. Therefore, nesting the cyber challenges under current national (SEE countries) security strategic documents requires careful analyses of the existing legislature regarding leading national authorities in different areas.

Future strategists must avoid establishing defaults or just copies of the concepts that are suitable for different societies that have a different history, traditions and culture. Although well intended Euro-Atlantic integration processes might cause complex confusion, especially when security responses need to be implemented in practice on an operational or tactical level. More precisely, if a nation fails to develop an appropriate security concept that will be followed by all responsible stakeholders. Moreover, this concept should be vertically (top-down and bottom-up, from the strategic through the operational to the tactical level) and horizontally (between different institutions) harmonized.

Hence, if guidance of security concepts isn't carefully and, under a coordinated mode, transferred into practice they could create "separate worlds" on the operational and the tactical, responsive level. Finally, such mistakes will result in the development of different standardization processes (including, but not limited to, risk assessment, resilience building, the overall consequence management, etc.). Such discrepancies will be evident not just in defence or law enforcement, but also in other cornerstone areas, i.e., crisis management and critical infrastructure protection, intelligence and counterintelligence, cyber governance and cyber diplomacy.

Finally, given the complexity which the future cyber security strategy must address, it is clear that the overall approach (i.e., developing a national cyber security strategy) must rely on the "whole-of-government" approach. Nevertheless, future strategies must design guidance that will develop centralized planning and decentralized execution. Thus the strategy will help avoid one of the biggest challenges that these processes produce, i.e. the lack of coordination.

## Conclusion

Contemporary security dynamics have urged many countries and organizations to consider cyber security as a top priority when it comes to security. Marching toward modernity and following their own ambitions in view of the Euro-Atlantic integration, SEE countries have, among others, invested serious efforts to improve their own information and communication technologies. The growing interdependence of these technologies and cyberspace in SEE, nevertheless, has not been matched by a parallel focus on security.

While building their national cyber security strategies SEE countries must address several areas. These areas are: countering cyber crime; cyber defence; intelligence and counterintelligence; critical infrastructure protection and crisis management and cyber diplomacy and cyber governance. To avoid potential miscommunication future strategists must consider centralized planning and decentralized execution.

# COMPENDIUM 2015

## References

1. **Australian Prime Minister**, The First National Security Statement to the Australian Parliament (Canberra: Australian Government, 2008)
2. **Chapman Gary**, *National Security and the Internet*, The 21st Century Project, LBJ School of Public Affairs, July 1998
3. **Giddens Anthony**, *The Consequences of modernity*, Stanford University Press, 1990
4. **European Union**, "The cybersecurity strategy - "An Open, Safe and Secure Cyberspace"", The European Commission and High Representative of the Union for Foreign Affairs and Security Policy, February 7, 2013
5. **Forst Brian**, *Terrorism, Crime and Public Policy*, Cambridge University Press, 2009
6. **French Secretariat-General for National Defence and Security**, Information systems defence and security. France's strategy (Paris: French Network and Information Security Agency, 2011)
7. **Friedman L. Thomas**, *The World is Flat*, Farrar, Straus & Giroux, 2005
8. **John Amaruso**, "Romania Global Center for Cyber Crime in USA", USA Today, (January 14, 2014), retrieved on 22 March 2014 from: <http://guardianlv.com/2014/01/romania-global-center-for-cybercrime-in-u-s/> Jose Pagilery, "CNN Money", November 2013
9. **Leavitt Lydia**, "Cybercrime writer mysteriously disappears in Bulgaria", January 25, 2011
10. **McGrew Anthony**, "The Globalization of World Politics", in ed. J Baylis; S Smith and Patricia Owens, "An Introduction to International Relations", 5th. ed. Oxford
11. **NATO Public Diplomacy Division**, "Defending the Networks, The NATO Policy on Cyber Defense", June 8, 2011
12. **NATO Homepage**, Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012
13. **National Strategy for development of Information Society with action plan** (2005) available at: [http://www.mio.gov.mk/files/pdf/dokumenti/Strategija\\_i\\_Akcionen\\_Plan.pdf](http://www.mio.gov.mk/files/pdf/dokumenti/Strategija_i_Akcionen_Plan.pdf).
14. **Symantec**, "Internet Security Threat Report", Volume 19, 2014
15. **The UN "E-Government Survey 2008: From E-Government to Connected Governance"**, New York, 2008
16. **The UN, "E-Government Survey 2012: E-Government for the People"**, The UN New York, 2012
17. **Weber H. Rolf**, "Internet of Things - New security and Privacy challenges", Computer Law & Security review 26, 2010
18. \_\_\_\_\_, (November 20, 2012), "FBI Arrested a Young Hacker from Struga" Press 24 retrieved on 22 September 2013 from: <http://star.press24.mk/story/poznato/foto-fbi-uapsi-mlad-haker-od-struga-sin-na-poznata-struzhanka>



## **Building a Cyber-Resilient Society by Forging a Partnership in SEE: An Important Task for Future SEE Strategists**

Associate professor **Metodi Hadji-Janev**, Ceolonel  
Military Academy "General Mihailo Apostolski Skopje",  
University "Goce Delcev" - Stip  
e-mail: metodi.hadzi-janev@ugd.edu.mk

### **Abstract**

Information and communication technologies play a crucial role in our everyday lives. These technologies bring many positive effects in almost all spheres of the society. However, they bring negative effects too. The main argument of this article is that South East European Societies need to change the woefully inadequate approach to cyber security. Given that zero risk is almost impossible to achieve in the cyberspace, among others, the SEE governments need to focus on building cyber resilient societies. One way to achieve this is to forge a partnership and cooperation. This cooperation needs to focus on several areas of SEE governance.

### **Introduction**

The rise of the information and communication technologies (ICT) in the globalized world introduced many changes. Many saw these changes as positive. However, these changes brought about many negative effects too. General changes after the end of the Cold War have significantly changed the power distribution. Using modern ICT some States, groups and individuals have gained strategic power. Hence, they have become able to multiply their effects and accomplish political agendas in an unconventional manner and under different rules and concepts.

The region of South East Europe (SEE) is not immune to these changes. In fact, as in the rest of the World, new waves in geopolitics have affected SEE countries too. Among others these changes have brought about new security challenges. Although modern ICT are necessary for the SEE countries' progress these technologies have brought many security challenges to these countries' societies. Given that these technologies ensure a competitive edge in the region of SEE and thus are necessary for the prosperity of these societies, SEE countries must ensure that societies are ready to meet the negative effects from cyberspace and these technologies and extract benefit from their everyday use. Hence, SEE countries need to build cyber resilient societies ready to cope with all challenges and multiply the benefits that cyberspace and ICT have to offer. Nevertheless, if they are about to do so in the age of globalization they need to forge a partnership among themselves which must be a strategic imperative for SEE's leadership.

The article will first explain the general security challenges that cyberspace and modern ICT pose to the societies around the globe and specifically in the region of SEE. Then, it will explain why SEE countries must build cyber resilient societies by explaining the concept of resilience. Finally, it will provide some incentives as a guidance that future strategies could consider in building cyber resilient societies.



## 1. Meeting the global security trends

The world we knew is gone forever. The walls that keep the East and West apart have disappeared. The technological boom in the new flattened environment resulted in interconnectivity and interdependence. The ICT is everywhere and represents an important part of our everyday lives. Networks of services and infrastructures built by these technologies and embedded within move people, goods, energy, money and information at a higher volume and greater velocities. As a result, our way of living has changed.

The new environment, in which ICT dominates and that is based on the principles of globalization, is changing fast. In their research study on the mankind progress Ray Kurzweil & Chris Meyer claim that "the 21st century will be equivalent to 20,000 years of progress at today's rate of progress".<sup>1</sup> In this context one might ask how all of these affect the region of SEE?

The evaporation of the walls and the dominance of the liberal democracy over the communism in the region of SEE changed the general concept of statehood functioning. Free flow of capital, people, goods, energy, money and information have begun to equal free market and foreign investments. At the same time all of these processes, more or less, today depend on ICT. The connectivity and interdependence designed to equal market economy principles, efficiency and commodity created a network. This network could easily be described as a system of systems. In fact, this system of systems enables a flow of capital, people, goods, energy, money and information. Even though these processes and changes brought many positive aspects seen from the perspective of security they have brought forth many challenges.

The paradox that SEE countries face is similar to the rest of the World. The main challenges stem from the fact that modern systems create the challenge by the way in which they were built. The problem is that these systems of systems were built without a political and security consent. The only considerations while establishing them were commodity, efficiency and wellbeing. Analyzing similar processes in the US from the perspective of security Stephen Flynn notes that these networks of systems that we depend upon are extremely vulnerable. According to him, it makes national security vulnerable too. The main reason behind this vulnerability according to his observation comes from the fact that architects of these networks did not factor in security variables when they built them. Security considerations have been widely perceived as annoying speed bumps in the process of achieving their goals. The only consideration while these systems and networks were built were profit, efficiency and commodity.<sup>2</sup>

Hence, these changes and dynamics have produced many side effects on the geopolitical level. The rise of ICT in the flattened environment after the Cold War and in the age of globalization has caused the governments to lose the monopoly of power. As a result non state actors corporations, groups and individuals have gained strategic power like never before. A network of system of services that were built to serve economic efficiency, wellbeing and commodity with their horizontal connections challenge many security concepts that were designed for a hierarchical order (where states and international organizations were the main actors). Finally, the development of the ICT resulted in improved communications and digitalization of our everyday activities. On the global level many see these changes as challenging. For example, addressing the Aspen security forum the former US Joint

<sup>1</sup> Ray Kurzweil & Chris Meyer, *Understanding the Accelerating Rate of Change*, May 2003, at: <http://www.kurzweilai.net/understanding-the-accelerating-rate-of-change>

<sup>2</sup> Flynn, Stephen (2004), *America the Vulnerable*, New York: Harper Collins, p. x

Chief of Staff, General Martin Dempsey observed that although globalization and new ICT are good when put in the context of Security, they are game changer.<sup>3</sup>

## 2. Understanding the South East European Cyber security trends

Although many doubt that SEE countries face cyber security challenges of the rest of the World, a closer view will lead one to conclude that these doubts are not quite right. During the Kosovo\*\* campaign, for example, NATO has arguably experienced the first ever organized cyberattacks.<sup>4</sup>

According to many serious reports Ramnicu Volcea in Romania represents a hotbed for cybercrime. The news reports, back in May of 2013, stated that three Romanian nationals were caught taking part in a multimillion dollar cyber fraud ring... And that the trio ended up making off with more than \$2 million.<sup>5</sup> General cybersecurity trends, however, are not the only challenge that comes from cyberspace alone.

The influence of the cyberspace activity has started to have a serious impact in the physical world too. Although not a regional trend per se, mysterious disappearing of a cybercrime writer in Bulgaria in 2010 and 2011 speaks that actions in SEE cyberspace have a significant influence on security.<sup>6</sup> According to these reports Danco Dancev refused to speak about what happened to him but he latently admitted that he was a victim due to his cyberspace engagement. The cyber security trends do not end here.

Some hackers from the region have tried to enter foreign governments' official websites in order to take control of their information sharing. A young hacker from The Former Yugoslav Republic of Macedonia\* back in 2012 was detained due to the cybercrime allegations of this kind. According to the allegation he attempted to penetrate illegally several security websites in the US, including that of the US FBI.<sup>7</sup>

Other reports speak about regional SEE based hackers' global involvement. Individuals from Great Britain, the US, Bosnia and Herzegovina, Republic of Croatia, The Former Yugoslav Republic of Macedonia\*, New Zealand and Peru established a virtual network whose primary objectives were the committing of cybercrime activities. The group was arrested in an operation carried out with the assistance of Facebook and international law enforcement agencies.<sup>8</sup>

<sup>3</sup> Martin Dempsey's Remarks at the Aspen Security Forum, July 25, 2014, retrieved from: <http://www.usatoday.com/media/cinematic/video/13145943/>

\* Turkey recognizes the Republic of Macedonia with its constitutional name.

\*\* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence. (In accordance with Arrangements regarding regional representation and cooperation.)

<sup>4</sup> Michael Aaronson, Avere Diessen, Yves de Kermabon, Mary Beth Long and Michael Miklaucic, (2012), "NATO Countering the Hybrid Threat", Prism 2, No 04, p.112-113

<sup>5</sup> Amarusio John, (January 14, 2014), Romania Global Center for Cyber Crime in USA", USA Today, retrieved on 22 March 2014 from: <http://guardianiv.com/2014/01/romania-global-center-for-cybercrime-in-u-s/>

<sup>6</sup> Leavitt Lydia, (January 25, 2011), "Cybercrime writer mysteriously disappears in Bulgaria", retrieved 24.04.2014 from <http://www.today.com/security-features/53558-cybercrime-writer-mysteriously-disappears-in-bulgaria>

<sup>7</sup> \_\_\_\_\_, (November 20, 2012), "FBI Arrested Young Hacker from Struga" Press 24 retrieved 22.09.2013 from: <http://star.press24.mk/story/poznato/foto-fbi-uapsi-mlad-haker-od-struga-sin-na-poznata-struzhanka>

<sup>8</sup> \_\_\_\_\_, (December 13, 2012), "10 arrested in cyber-crime probe", Express UK, retrieved 24.03.2014 from: <http://www.express.co.uk/news/world/364435/10-arrested-in-cyber-crime-probe>

The problems that loom large, however, are some concerning reports about the trend in Eastern Europe. Authors of these reports claim State involvement in providing cover for cybercriminals. In this context, for example, respected security researcher Nart Villeneuve has controversially declared that Eastern European cybercriminal gangs are responsible for the 2014 attacks on Target and other major retailers and that they are relatively safe from arrest and prosecution from their State authorities.<sup>9</sup>

Terrorist use of a cyberspace is another general trend that is also present in the Region of SEE. Websites such as the "Way of Islam" (*stazomislama.com*), Ensarije Serijata ("Partisans of haria") [http://www.geocities.ws/ensarije\\_serijata/index-2.html](http://www.geocities.ws/ensarije_serijata/index-2.html)); News of the Community" (*vijestiummeta.com*) and the Sandžak Wahhabi website *kelimetul-haqq.org* are known as promoters of electronic jihad.

In sum, it could be argued that almost every aspect of the cyber based threats is in one or another way present in the SEE cyberspace. The influence of the cyberspace on SEE societies has an emotional, societal, economic, political, safety and security aspect. Therefore, if SEE countries are about to cope with the global trends and effectively mitigate negative effects from many double edged sword based trends like cybersecurity trends and challenges, among others, they need to build cyber resilient societies.

### 3. The concept of resilient society in the cyber era

A logical question that one might ask at the very beginning is why focus on resilience? As we saw rapid changes in the age of globalization and technological development in two general trends is important for our point of perception. Firstly, these trends have resulted in the decrease of the lifespan of our organizations. Secondly, the increasing demands from key stakeholders, to effectively address the combined issues of security, preparedness, risk and survivability. These stakeholders include, but are not limited to, Boards, Governments, Regulators, Shareholders, Staff, Suppliers and Customers.

At the same time cyberspace and modern ICT were not designed under the national security concept's logic. Analyzing the development of the internet compared to national security Gary Chapman comes to very interesting conclusions. In short, according to him, while the Internet and the concept of "national security" share common roots in history, they developed along separate and divergent paths.<sup>10</sup> In this line, unlike national security which is organized according to the top down principle, cyberspace has vertical and horizontal effects-it depends on end users. Therefore, security is shaped by these users, not by the Government alone per se. These observations, nevertheless, raise serious concerns.

A fair view would be that cyberspace today could be described with the famous Latin phrase: *hic sunt leones* - here lie the Dragons. This was a phrase that ancient Roman legions used to explain the area that they did not know and was behind the borders of the Roman Empire. The danger from cyberspace comes and maybe also well explained if one uses Antony Giddens' observations about the "consequence of modernity".<sup>11</sup> Put differently, the more we depend on modern technology the more vulnerable we are.

<sup>9</sup> \_\_\_\_\_, (February 04, 2014), "East European cyber criminals protected from prosecution", SC Magazine UK, retrieved on 08 May 2015 from: <http://www.scmagazineuk.com/east-european-cyber-criminals-protected-from-prosecution/article/332548/>

<sup>10</sup> Gary Chapman, *National Security and the Internet*, The 21st Century Project LBJ School of Public Affairs, July 1998

<sup>11</sup> Anthony Giddens, "The Consequences of Modernity", Cambridge University Press, 1999

From all of the above a logical risk averted approach would be to disconnect from the cyberspace. The problem with this approach is that it is at odds with the aspiration to cope with modernity and create efficiency, commodity and wellbeing. Thus, to disconnect is not a solution for SEE countries.

Common wisdom dictates that if SEE countries are about to ensure economic development they need to invest in a safe and secure environment. Achieving such an environment requires measures, instruments and mechanisms that will convince clients, investors, consumers and citizens in cyber security too. In fact if we are about to keep the commodity, welfare and benefits from cyberspace, we need to build effective and cyber resilient societies.

One of the problems with building cyber resilient societies is that the definition matters. For different actors and different people resilience has a different meaning. The 2009 US National Infrastructure Advisory Council's study on resilience had identified challenges with the definitions of resilience in this direction.<sup>12</sup> Similarly the 2010 US DHS's Study on resilience distilled that there are about 109 definitions of resilience.<sup>13</sup> Therefore, having a conceptual definition is an important precondition that must be considered. James Sterbenz from Kansas University led a team that worked in developing a framework definition usable for national institutions. The final product of their project ReiliNets was a framework approach to resilience of the government and organizations. Later this framework was adopted by ENISA and Department of Homeland Security.<sup>14</sup>

To be able to approach in an appropriate manner the threats from cyberspace SEE countries need to change the woefully inadequate approach to cyberspace. The general attitude in SEE societies is that cyberspace is a business for IT professionals. Although this is true for most parts of cyberspace, to leave cyberspace alone to the IT world is like leaving nuclear proliferation or other Weapons of mass destruction to the technologists, physicians and chemists. Yes, they play a crucial role in developing these weapons like IT experts do in the IT world. But, to build cyber resilient societies we need the "whole-of-government" approach and a multidisciplinary approach that will look into different aspects of everyday lives where cyberspace has influence. There are several reasons for this.

Chris Valasek & Charlie Mille presented their project in which they showed how they can remotely access the Toyota speedometer.<sup>15</sup> If one knows what this can cause by tricking the computer than it would be clear that this technique could be used as a weapon. Chenda Ngak gives astonishing examples of how Sochi Olympic Games were hacked.<sup>16</sup> Jared Howe claimed a similar thing about the Brazil World Football championship, where hackers were using hotspots from the free wifi and stole data from consumers.<sup>17</sup> The fact that ICT affects our life from different angles maybe is best described by David Jacobs' personal experience. In the article "How I hacked my home" he describes the challenges of using new technology that creates the so called internet of things enigma.<sup>18</sup>

<sup>12</sup> The US National Infrastructure Advisory Council (NIAC), "Critical infrastructure resilience", 2009 retrieved from: [http://www.dhs.gov/xlibrary/assets/niac/niac\\_critical\\_infrastructure\\_resilience.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf)

<sup>13</sup> The US DHS, (February 2010) " Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland", retrieved: May 10, 2015 from: [http://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf)

<sup>14</sup> James PG Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, Paul Smith, *Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET)*, vol.54 iss 8, June 2010, pp 1245-1265

<sup>15</sup> Chris Valasek & Charlie Miller, Adventures in Automotive Networks and Control Units, at: [http://www.ioactive.com/pdfs/IOActive\\_Adventures\\_in\\_Automotive\\_Networks\\_and\\_Control\\_Units.pdf](http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf)

<sup>16</sup> Chenda Ngak, (February 7, 2014), Sochi 2014: Privacy and hacking at the Olympic Games, at: <http://www.cbsnews.com/news/winter-olympics-2014-privacy-hacking-sochi-olympic-games/>

<sup>17</sup> Jared Howe, (June 16, 2014), Hackers at the World Cup: Beware the Risky Free WiFi in Brazil's Soccer Stadiums, at: <http://www.privatewifi.com/hackers-at-the-world-cup-beware-the-risky-free-wifi-in-brazils-soccer-stadiums/>

<sup>18</sup> David Jacoby (August 21, 2014), "How I hacked my Home", at: <https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my->

These and many other similar examples clearly attest that we need to build cyber resilient societies. In this process we need to change the approach to cyber security in a manner that our security system could cope with the challenge. Precisely our systems need to be able to withstand the attack or failure; maintain an acceptable mode of operation; manage the consequences in a careful and timely manner; mitigate negative effects and fight back effectively while operating in the shared network of networks. To be able to effectively achieve this state SEE countries must consider cooperation and partnership as one of the important tools in achieving the desired end-state i.e. cyber resilient societies.

#### 4. Forging partnership in SEE as strategic imperative

Global threats need a global response. The best way to implement this is through regional cooperation. This cooperation must be developed in a way that will support several sectors in the national systems. These sectors are:

- Law enforcement
- Defense
- Crisis management and critical infrastructure protection
- Intelligence and countering intelligence, and
- Cyber governance and cyber diplomacy.


Cooperation in cyberspace has political importance for SEE countries. All SEE countries have pledged their national agendas under the framework of the Euro-Atlantic integrations. In this line, both the revised NATO Policy on Cyber Defense of 8 June 2011 and the Chicago Summit Declaration of May 2012 stressed the importance of cooperation with partner nations in order to achieve greater cyber security. Considering the threat from cyberspace as real NATO decided to build up cyber-defense rapid reaction teams. Similar guidance comes from the European Union cyber security strategy too.

The future cooperation must focus on several areas that will equally be implemented in the above mentioned sectors of the national systems. SEE countries must cooperate in finding the right balance between:

- Economic development vs. improved national security
- Modernization of infrastructure vs. critical infrastructure protection
- Private sector vs. public sector needs and priorities
- Private sector vs. public sector, and
- Individual freedoms vs. public safety.

A partnership must ensure an exchange of best practices and cooperation in the following areas:

- Assurance (including engineering, certification and insurance)

- 
- Integrated data-centric and system-centric views
  - Secure execution environment, with secure devices for everybody
  - Establishing of privacy-enhancing technologies and digital identities
  - Managing the complexity of systems (including risk assessment and management)
  - Trust management
  - User-centricity
  - Standardization and interoperability
  - Education and awareness

All of these recommendations, however, must be implemented carefully and through research in order to avoid mistakes from previous experience.

### Conclusion

Global Cyber Security Trends urge SEE societies to seriously consider cyber security threats. As we have seen cybersecurity affects societies from different angles and in different ways. Therefore, building cyber resilient societies must be a strategic imperative for the strategists in SEE countries. Cooperation and partnership in achieving the strategic end with cyber resilient societies in SEE is a must for all SEE countries. This cooperation should be built in several sectors across the governance level. They need to consider sharing of best practices and experience and to focus on raising awareness, education and building capacities among the SEE societies.

### References:

1. **Amaruso John**, (January 14, 2014), Romania Global Center for Cyber Crime in USA", USA Today, retrieved on 22 March 2014 from: <http://guardianlv.com/2014/01/romania-global-center-for-cybercrime-in-u-s/>
2. **Anthony Giddens**, "The Consequences of Modernity", Cambridge University Press, 1999
3. **Chenda Ngak**, (February 7, 2014), Sochi 2014: Privacy and hacking at the Olympic Games, at: <http://www.cbsnews.com/news/winter-olympics-2014-privacy-hacking-sochi-olympic-games/>
4. **Chris Valasek & Charlie Miller**, Adventures in Automotive Networks and Control Units, at: [http://www.ioactive.com/pdfs/IOActive\\_Adventures\\_in\\_Automotive\\_Networks\\_and\\_Control\\_Units.pdf](http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf)
5. **David Jacoby** (August 21, 2014), "How I hacked my Home", at: <https://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home//>

# COMPENDIUM 2015

6. Flynn, Stephen (2004), "America the Vulnerable", New York: Harper Collins, p. x
7. Gary Chapman, National Security and the Internet, The 21st Century Project LBJ School of Public Affairs, July 1998
8. James P.G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, Paul Smith, Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET), vol. 54 iss. 8, June 2010, pp.12451265
9. Jared Howe, (June 16, 2014), Hackers at the World Cup: Beware the Risky Free WiFi in Brazil's Soccer Stadiums, at: <http://www.privatewifi.com/hackers-at-the-world-cup-beware-the-risky-free-wifi-in-brazils-soccer-stadiums/>
10. Leavitt Lydia, (January 25, 2011), "Cybercrime writer mysteriously disappears in Bulgaria", retrieved on 24 April 2014 from <http://www.tgdaily.com/security-features/53558-cybercrime-writer-mysteriously-disappears-in-bulgaria>
11. Martin Dempsey's Remarks at the Aspen Security Forum, July 25, 2014, retrieved from: <http://www.usatoday.com/media/cinematic/video/13145943/>
12. Michael Aaronson, Averre Diessen, Yves de Kermabon, Mary Beth Long and Michael Miklaucic, (2012), "NATO Countering the Hybrid Threat", Prism 2, No. 04, p.112-113
13. Ray Kurzweil & Chris Meyer, Understanding the Accelerating Rate of Change, May 2003, at: <http://www.kurzweilai.net/understanding-the-accelerating-rate-of-change>
14. The US National Infrastructure Advisory Council (NIAC), "Critical infrastructure resilience", 2009 retrieved from: [http://www.dhs.gov/xlibrary/assets/niac/niac\\_critical\\_infrastructure\\_resilience.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf)
15. The US DHS, (February 2010) "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland", retrieved: May 10, 2015 from: [http://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf)
16. \_\_\_\_\_, (November 20, 2012), "FBI Arrested Young Hacker from Struga" Press 24, retrieved on 22 September 2013 from: <http://star.press24.mk/story/poznato/foto-fbi-uapsi-mlad-haker-od-struga-sin-na-poznata-struzhanka>
17. \_\_\_\_\_, (December 13, 2012), "10 arrested in cyber-crime probe", Express UK, retrieved on 24 March 2014 from: <http://www.express.co.uk/news/world/364435/10-arrested-in-cyber-crime-probe>
18. \_\_\_\_\_, (February 04, 2014), "East European cyber criminals protected from prosecution", SC Magazine UK, retrieved on 9 May 2015 from: <http://www.scmagazineuk.com/east-european-cyber-criminals-protected-from-prosecution/article/332548/>



## Technical Aspects of Resilience in Cyberspace with Emphasis on Water Supply Critical Information Infrastructure

Mitko BOGDANOSKI<sup>a</sup>,  
Marjan BOGDANOSKI and  
Zoran ANGELOV

<sup>a</sup> *Military Academy "General Mihailo Apostolski",  
Goce Delcev University*

### Abstract:

National infrastructure for drinking water is vital for protecting public health and safety, but it also supports business, industry and national economy. This paper outlines the challenges of the physical and cyber security on national infrastructure for public drinking water and presents existing security gaps. The paper also presents security measures which need to be taken in order to eliminate (mitigate) these gaps and achieve resilient cyberspace. Furthermore, the paper gives an overview of the situation regarding cyber (in)security infrastructure of drinking water, currently known threats to SCADA (Supervisory Control and Data Acquisition) systems and potential threats and countermeasures that should be carefully analyzed. The purpose of this paper is to make a realistic assessment of a potential terrorist attack against public drinking water systems and possible solutions for achieving resilience.

### Keywords:

Water supply, Cyber attack, Terrorism, SCADA, Critical infrastructure, Industrial Control Systems

### Introduction

Although defining the term critical infrastructure is a complex task, according to the United States Government Accountability Office (2007) the critical infrastructure includes all physical or virtual systems and assets which are so vital for the nation that their incapacity or destruction of such systems and assets would have caused great damage to the national and economic security, public health and security.

These systems and assets, such as power supply, transportation, water treatment facilities, etc. (Figure 1) are essential for the economy and government operations.

Generally speaking, water infrastructure systems include surface and underground water resources of raw water for municipal, industrial, agricultural and domestic needs; dams, reservoirs, aqueducts and pipes that contain and transmit raw water; plants for water treatment which eliminate impurities and pollution of raw water; final water reservoirs; systems that distribute water to consumers and facilities for collection and treatment of the waste water (Fig. 2 and 3).



# COMPENDIUM 2015



Figure 1. Critical Infrastructure

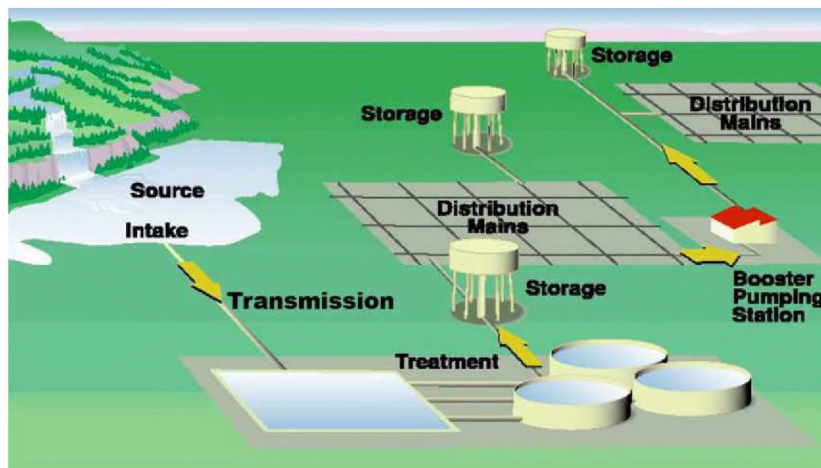


Figure 2. Water purification system

The water supply is one of the most critical elements of infrastructure for any nation that is not critical in itself, but has a lot of influence on other systems and tools included in the category of critical infrastructure (energy, transport, emergency services, critical industries, etc.).

Considering the importance of water infrastructure in all domains of life, it has been targeted thousands of years ago<sup>1</sup>.

<sup>1</sup> Copeland C., and Cody B., "Terrorism and Security Issues Facing the Water Infrastructure Sector", CRS Report for Congress, May 2006, [fpc.state.gov/documents/organization/68790.pdf](http://fpc.state.gov/documents/organization/68790.pdf).



Figure 3. Water treatment plant

In general, the public water supply systems are vulnerable to three types of attacks, namely, the following:

- Contamination (chemical, biological and radiological)
- Physical damage, and
- Damage of the SCADA (Supervisory Control And Data Acquisition) systems.

Although water poisoning is very difficult to do, mainly because of the required physical access to the water supply facilities, it is possible. During the chemical, biological and radiological (CBR) contamination of the water, the following criteria must be considered<sup>2</sup>:

- Weaponized, meaning it can be produced and disseminated in quantities large enough to cause the desired effect.
- Water threat, meaning it is infectious or toxic to drink water.
- Stability, meaning the agent maintains its structural and virulent effects in water.
- Chlorine resistance.

The list of CBR which would probably cause mass casualties is not that long. Only a few agents can cause such effects. This attack can be used in combination with some other attacks. For example, in combination with the contaminations of water the attackers can physically destroy communications, which would prevent an emerging response to the poisonous attack and awareness of the potential victims about this attack.

Lately, the fear of exploitation of these water vulnerabilities by terrorist groups is becoming greater. The cache of electronic and handwritten materials seized during the killing of the Osama bin Laden

---

<sup>2</sup> McNabb J., *Cyberterrorism & the Security of the National Drinking Water Infrastructure*, DEFCON 18, July 31, 2010, <https://www.defcon.org/images/defcon-18/dc-18-presentations/McNabb/DEFCON-18-McNabb-Cyberterrorism-Drinking-Water.pdf>.

# COMPENDIUM 2015

includes numerous hallmark al Qaeda plots for mining dams and poisoning the drinking water in the United States (Figure 4)<sup>3</sup>.

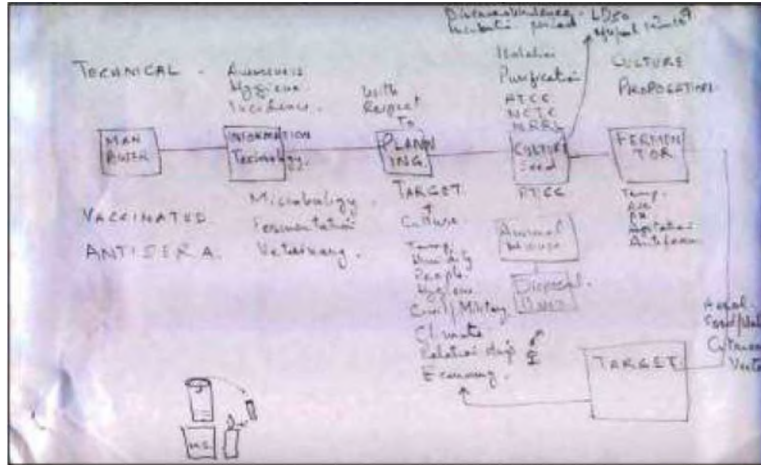


Figure 4: Al-Qaeda's plan for poisoning a water supply facility in the U.S.

Although Al Qaeda and other terrorists organizations use the Internet extensively in order to realize their goals (organizing, propaganda, stealing money, etc.), there is still no valid information to confirm that they have used the cyberspace to realize cyber terrorism, which does not mean that this will not happen in the future.

Unlike other attacks on water infrastructure that existed for thousands of years, cyber-dependent attacks are very recent and the reason for this is their nature and the necessary resources for these type of attacks (Table 1).

Year	Attack
1994	A hacker penetrated into the computer system of the Salt River Project in Phoenix, Arizona, USA.
2000	Former consultant in a wastewater treatment plant in Maroochy Shire, Queensland, Australia, hacks into the sewage system and releases over a million liters of raw sewage into the coastal waters.
2006	A foreign hacker penetrated security systems of the water filtering plant in Harrisburg, Pennsylvania, USA and planted malicious software capable of affecting the plant's water treatment operations and entered into the system for cleaning water, Pa., through which he could operate the plant for filtering water.
2007	A former employee of a federally-owned canal system in Tehama Colusa in California, USA was charged with installing software that damaged a computer used to divert water out of a local river.
2009	According to RISI (Repository of Industrial Security Incidents), the cyber attacks on water facilities increased by 30%.
2011	Hackers attacked SCADA systems of the water supply facilities in Springfields, Illinois, USA.

Table 1: Shortlist of cyber attacks on water infrastructure

<sup>3</sup> ABC World News, "Osama Bin Laden Raid: Al Qaeda 'Playbook' Revealed 6", May 2011, <http://abcnews.go.com/Blotter/osama-bin-laden-raid-al-qaeda-playbook-revealed/story?id=13544154#T7bEmkUtg3A>.

The scope of this paper covers the cyber threats on water utilities' SCADA systems. The following sections give a brief description of the operation of these systems, the threats against these systems and possible responses against these threats.

### 1. Use of SCADA Systems in the Water Supply Systems

In the past, SCADA primarily had only a supervisory function, i.e., the SCADA system was understood as a system that collects and sends information to remote locations. Today this function is extended and one of the main functions of these systems, apart from the monitoring function, is the controlling of the industrial and manufacturing processes and facilities.

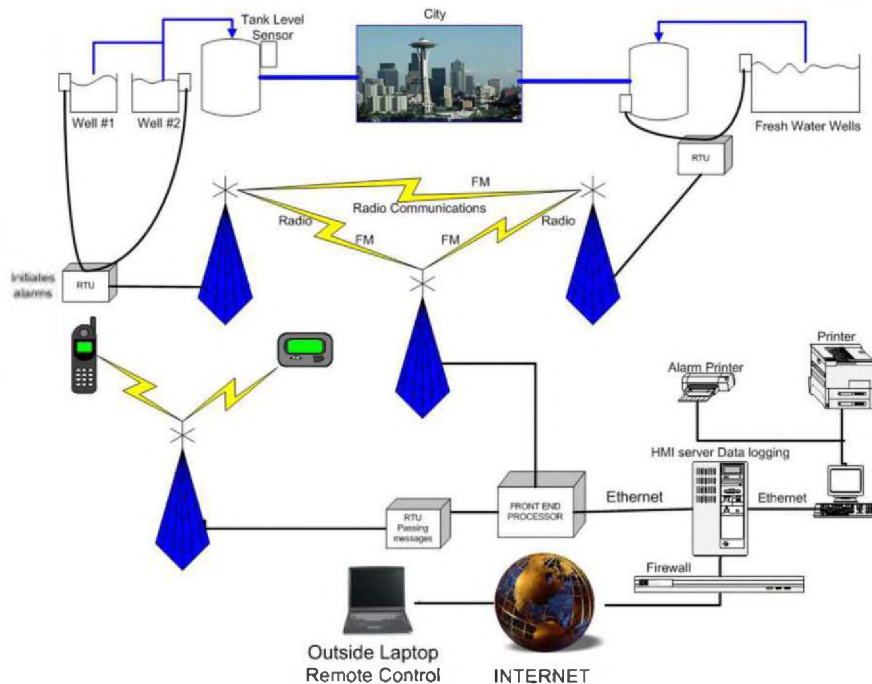


Figure 5. Components of a Control System in a Water Treatment and Distribution Facility

SCADA systems are able to communicate using a variety of transmission media. This makes them especially useful for collecting and sending information and controlling a variety of other digital systems. Using different protocols, SCADA systems are able to communicate via telephone lines, UHF / VHF radios, Ethernet, microwave systems, satellite systems and optical cables. A typical SCADA system consists of a master unit - MTU (Master Terminal Unit) and one or more remote units - RTU (Remote Terminal Unit). A Master unit can be a personal computer (or network of computers) on which a SCADA software with a graphics operator and control function are installed, or it consist of a hardware module that acts as a data collector for another digital system. As a remote unit a specialized hardware

unit for SCADA systems can be used, such as RTU or a PLC (Programmable Logic Controller) device. Communication between MTU and RTU is in principle master - subordinate (Figure 5).<sup>4</sup>

Most of the water supply facilities in the developed countries already implemented a system for automatic control and monitoring - SCADA - as support for better water distribution. This system allows operators and controllers to inspect the condition of the facilities, operating parameters and potential problems at any time. This allows rapid response in case of malfunction of the installed equipment, early detection of anomalies in the water supply system (high level of consumption, uncontrolled leakage, etc.), and possibility to analyze historical data of the systems' working parameters (Figure 6).<sup>5</sup>

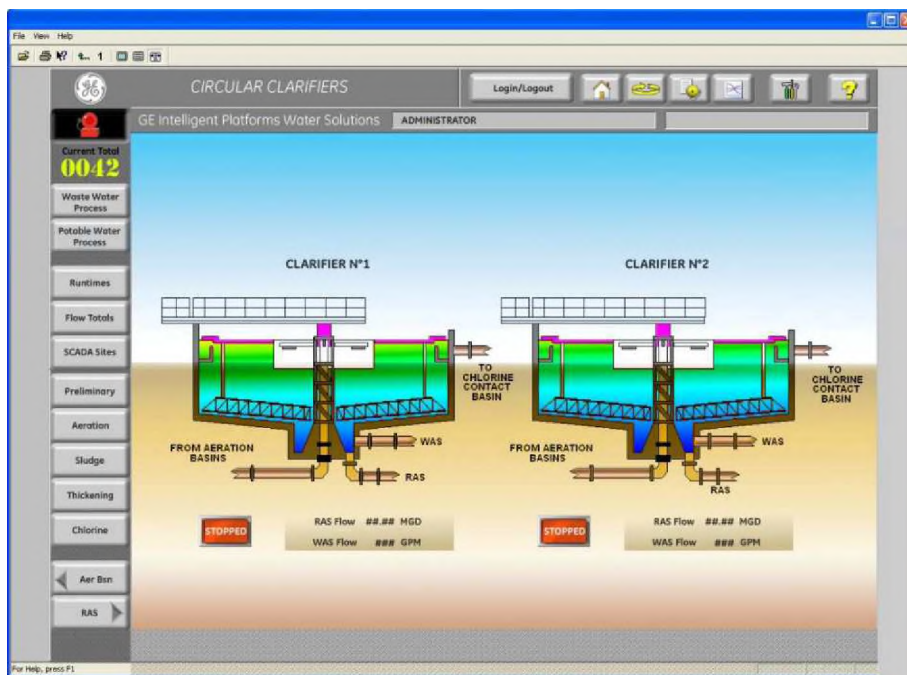


Figure 6. Resource management through the remote monitoring and remote management system


Although the primary objective of the SCADA system is to improve water supply and to allow better control over the complete resources of the company, it can be a potential target for malicious users who can misuse the automatic control method of this system in order to perform malicious actions.

## 2. Lessons Learned from the Previous Cyber Attacks on the SCADA Systems

It is anticipated that in the future almost all branches of the industry will be based on the usage of SCADA systems. The water supply is not exception.

<sup>4</sup> Tuneski, A. and Zaev, E., "HEP regulation and atomization", Mechanical Faculty Skopje, 2008.

<sup>5</sup> Boulos, P. F., and Wiley, "A. N., Can We Make Water Systems Smarter?", Opflow Online, Vol. 39, Issue 3, p.20, March 2013.



On the other hand, most of the systems that fall into the category of SCADA controlled systems are also vulnerable to attacks such as traditional water supply systems. These systems use interfaces, softwares, operating systems and protocols that are generally not well known outside of the industries in which they are being implemented. In theory, if the attacker wants to penetrate into these systems he must either have a great knowledge of the design of the concrete and probably unique system (intruder or someone who is well informed) or spend a lot of time to get access to them and learn how they operate.

The recent cyber attack on water facilities in Springfield, Illinois, USA prompted considerable concern about the vulnerability of the critical infrastructure. The attack destroyed a pump when (a) malicious user(s) using a computer with an IP address based in Russia gained access to a SCADA system that controlled the pump.

Experts in industrial control systems (ICS) explain that, although the attack caused no major consequences, it can be a precursor to more sophisticated and destructive attacks that may be expected in the near future.

The main lessons from this incident, which is still under investigation, are<sup>6</sup>:

### **2.1. Lack of information sharing**

Although in the initial report by the Statewide Terrorism and Intelligence Center of Illinois this incident is called cyber intrusion on the water supply system, the Department of Homeland Security (DHS) and other agencies that share information on such incidents are relatively silent about this one<sup>7</sup>. This was the main reason that a lot of speculations about the nature of the attack appeared, about how serious it was and what the motive behind this attack was. Some even wonder if there might be an outage in a way that the report about the incident is published.

It is assumed that the water pump in Springfield was blighted after attackers used their access to the SCADA system and started turning it on and off continuously. According to LW Brittan<sup>8</sup>, who is a consultant for SCADA systems and a training expert, there is no chance that the pump itself was damaged due to the fast rotation of the big motor pump. On the other hand, the rapid and continuous turning on and off of the pump can overheat it, but in this case the temperature and pressure control mechanisms that are built into the pump should be activated and the pump safely disconnected.

According to Brittan, the SCADA system can be accessed through the Internet so that any malicious user can run the pump and can use on and off commands in a few seconds, but, according to him, the malicious user would not be able to access to the overload relay which protects the motor from overload and burning out. Even if the malicious user had access to the control mechanisms of the SCADA system, he is not confident that he can approach the security mechanisms. Because of this more details about the attack were requested, which were not presented to the public, which is the main reason why the problem with the pump in Illinois still remains unclear.

### **2.2. Braking the SCADA systems**

Most of the systems used to control critical equipment at places like power stations, nuclear plants

---

<sup>6</sup> Jalkumar V., "4 lessons from the Springfield Ill. SCADA cyberattack", November 22, 2011  
[http://www.computerworld.com/s/article/9222113/4\\_lessons\\_from\\_the\\_Springfield\\_Ill\\_SCADA\\_cyberattack?taxonomyid=17&pageNumber=2](http://www.computerworld.com/s/article/9222113/4_lessons_from_the_Springfield_Ill_SCADA_cyberattack?taxonomyid=17&pageNumber=2)

<sup>7</sup> Hurst R. W., "Circuit breaker & Switchgear Handbook, Volume 3", Published by The Electricity Forum, 2007.

<sup>8</sup> Homeland Security, "ICS-CERT Information Bulletin - Illinois Water Pump Failure Report", November 23, 2011,  
[www.us-cert.gov/control\\_systems/pdf/ICSB-11-327-01.pdf](http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf)

and facilities for water treatment are unsafe. In many cases, anyone with logical access to the industrial control system or programmable logic controller can update their firmware, without the need for authentication. Systems' passwords are often hardcoded. Many systems have administrative "backdoors" and contain many basic errors due to buffer overload.

Such flaws were acceptable for a long period of time. The reason for this was that the SCADA systems were not connected with the outside world. The attacker usually needed physical access to the SCADA system to perform the attack.

Over the last few years this conclusion changed. A growing number of SCADA systems are connected to the Internet, which makes them more susceptible to attack from external sources. An example of this is the recent attack by hackers identified as "pr0f" claiming that they penetrated into a SCADA system of water supply resources in South Houston by breaking a three-character password used to protect the system.

According to Ralph Langner, a German expert on control systems security who worked on Stuxnet analysis, the problem is that most users of these systems do not actually realize that the security of these systems is almost non-existent.

So far, the two best-known malwares that are used to attack SCADA systems or, more precisely, to attack the "Natanz" nuclear plants for uranium enrichment in Iran<sup>9</sup> are Stuxnet (2010) and Duqu (2011). The Natanz attacks are followed by several other attacks on SCADA systems conducted using different malwares which are basically are very similar to Stuxnet.

### ***2.3. Increased number of malicious users who want to penetrate within the SCADA systems***

It is expected that the number of attacks on SCADA systems in the future will increase. Special interest for the attacks on these systems appeared after the discovery of the Stuxnet malware<sup>10</sup>. People who in the past did not know anything about SCADA are now finding various types of security vulnerabilities in SCADA products. In 2011, there were more than 200 vulnerabilities discovered in products by different manufacturers, which is much more compared to 2010 when there were only 10 vulnerabilities discovered. In 2012 even more vulnerabilities were discovered, and 2013 broke the records one more time<sup>11</sup>.

## **3. Fixing the SCADA Systems Vulnerabilities and Increasing Resilience**

After Stuxnet, experts are making great efforts to find and fix the vulnerabilities of the SCADA systems. Great emphasis is placed on the front end of the system, i.e. the part that is connected to Windows-based Human Machine Interface (HMI) systems that are used to interact with the SCADA systems. However, the manufacturers are not too much focused on the embedded control systems' vulnerability. ISA Security Compliance Institute in 2010 launched a program for testing and certification of the vulnerabilities of the industrial control systems products. So far only a few companies have certified their product under this program.


Utilities also often lack the resources needed to strengthen the security of their control systems. This

---

<sup>9</sup> Bogdanoski M., Risteski A., and Bogdanoski M., "Cyber Operation a Permanent Part of the Global Terror", Handbook, LAP Lambert Academic Publishing, Germany, January 2014.

<sup>10</sup> Byres E., "SCADA and CIP Security in a Post-Stuxnet World - The Future of Critical Infrastructure Security", AIC - Seminar on Cyber Security, Milano, Lombardia, Italy, October 24, 2011, <http://www.tofinosecurity.com/downloads/477>.

<sup>11</sup> Byres E., "SCADA and ICS Cyber Security: Facing the Facts", Tofino, May 03, 2013, <http://www.tofinosecurity.com/blog/scada-and-ics-cyber-security-facing-facts>.



problem is known when speaking about the smaller suppliers, as was the case with the recent intrusion in Springfield. According to Dale Peterson<sup>12</sup>, CEO of Digital Bond, a consulting agency that specializes in security control systems, smaller utilities have greater difficulties in securing their SCADA and DCS (Distributed Control Systems), because they do not have enough trained IT staff or other resources required to deal with such threats. According to him, in some municipalities, the entire process of maintenance of all information, network and control resources is being handled by only two or three IT people who cannot cope even with the basic needs of the enterprises, not to mention the establishment of certain security policies which will protect systems from malicious users and achieve resilience in the cyberspace.

If it is a well-known fact that the critical infrastructure should be safe and secure, this means that the owners and operators should be aware that their control systems nowadays are targets of sophisticated attacks and adjusting their programs according to the latest security threats is needed. Specifically, the security programs should<sup>13, 14</sup>:

- Consider all possible pathways of infection and have strategy that aims to reduce these pathways, rather than focusing on a single path, such as, for example, the infection via external USB thumb drives
- Recognize that there is no perfect security solution and take steps to aggressively segment the control networks to limit the compromise consequences
- Install ICS - appropriate technologies for intrusion detection to detect attacks and to increase the warning level when the equipment is compromised or it is on at a risk of being compromised
- Deploy, operate and maintain ICS - appropriate security technologies and practices with maximum efficiency, including firewalls, antivirus programs and white lists designed for SCADA/ICS, in order to make a sophisticated malware attack more difficult,
- Look beyond the traditional firewalls on a network layer and focus on the firewalls that are capable of deep packet inspection in key SCADA and ICS protocols
- Focus on securing critical systems, particularly safety integrated systems (SIS)
- Incorporate security assessments and testing as a part of system development and periodic maintenance processes
- Identify and reduce potential vulnerability, which reduces the likelihood of a successful attack, and
- Aim to improve the culture of industrial security among management and technical teams.

These changes must be urgently implemented in order to improve the security of the industrial control systems. Waiting for next Stuxnet-like malwares may be too late.

## Conclusion

The water sector is often identified as one of the critical infrastructures and key resources that are essential for nation's security, public health and safety, economic vitality and way of life. Atomization of the water supply offers better water purification and distribution and at the same time higher quality of life. On the other side site, protecting the water supply infrastructure and achieving resilience in the

---

<sup>12</sup> Peterson D. G., "Luigi Vulnerabilities II", Digital Bong, September 2011, <http://www.digitalbond.com/2011/09/14/luigi-vulnerabilities-ii/>.

<sup>13</sup> Bogdanoski M., Risteski A. and Bogdanoski M., "Cyber Operation a Permanent Part of the Global Terror", Handbook, LAP Lambert Academic Publishing, Germany, January 2014.

<sup>14</sup> Byres E., "SCADA and ICS Cyber Security: Facing the Facts", Tofino, May 03, 2013, <http://www.tofinosecurity.com/blog/scada-and-ics-cyber-security-facing-facts>



# COMPENDIUM2015

cyberspace has become more challenging as control systems, SCADA networks, IT networks and business systems become more interconnected, increasing the threat of cyber attack, and making the fear from possible threats to this part of the critical infrastructure reasonable.

In order to avoid the attacks against SCADA-based critical infrastructure used in water supply systems and to ensure the availability and reliability of these systems in the future it is necessary to take appropriate action by all involved in the design and operation of these water supply control systems.

## References

- [1] **United States Government Accountability Office**, "Critical Infrastructure Protection - Multiple Efforts to Secure Control, Systems Are Under Way, but Challenges Remain", Report to Congressional Requesters, September 2007, [www.gao.gov/assets/270/268137.pdf](http://www.gao.gov/assets/270/268137.pdf)
- [2] **Copeland C, and Cody B.**, "Terrorism and Security Issues Facing the Water Infrastructure Sector", CRS Report for Congress, May 2006, [fpc.state.gov/documents/organization/68790.pdf](http://fpc.state.gov/documents/organization/68790.pdf)
- [3] **Kroll D.**, "Aqua ut a Telum - Water as a Weapon", 2010, <http://hachhst.com/technical-library>
- [4] **McNabb J.**, **Cyberterrorism & the Security of the National Drinking Water Infrastructure**, DEFCON 18, July 31, 2010, <https://www.defcon.org/images/defcon-18/dc-18-presentations/McNabb/DEFCON-18-McNabb-Cyberterrorism-Drinking-Water.pdf>
- [5] **ABC World News**, "Osama Bin Laden Raid: Al Qaeda 'Playbook' Revealed 6", May 2011, <http://abcnews.go.com/Blotter/osama-bin-laden-raid-al-qaeda-playbook-revealed/story?id=13544154#.T7bEmkUtg3A>
- [6] **Tuneski, A. and Zaeve, E.**, "HEP regulation and atomization", Mechanical faculty Skopje, 2008
- [7] **Boulos, P. F., and Wiley**, "A. N., Can We Make Water Systems Smarter?", Opflow Online, Vol. 39 Issue 3, p. 20 March 2013
- [8] **Jaikumar V.**, "4 lessons from the Springfield, Ill. SCADA cyberattack", November 22, 2011 [http://www.computerworld.com/s/article/9222113/4\\_lessons\\_from\\_the\\_Springfield\\_Ill.\\_SCADA\\_cyberattack?taxonomyid=17&pageNumber=2](http://www.computerworld.com/s/article/9222113/4_lessons_from_the_Springfield_Ill._SCADA_cyberattack?taxonomyid=17&pageNumber=2)
- [9] **Hurst R. W.**, "Circuit breaker & Switchgear Handbook, Volume 3", Published by The Electricity Forum, 2007
- [10] **Homeland Security**, "ICS-CERT Information Bulletin - Illinois Water Pump Failure Report", November 23, 2011, [www.us-cert.gov/control\\_systems/pdf/ICSB-11-327-01.pdf](http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf)
- [11] **Bogdanoski M., Risteski A., and Bogdanoski M.**, "Cyber Operation a Permanent Part of the Global Terror", Handbook, LAP Lambert Academic Publishing, Germany, January 2014
- [12] **Byres E.**, "SCADA and CIP Security in a Post-Stuxnet World - The Future of Critical Infrastructure Security", AIIIC - Seminar on Cyber Security, Milano, Lombardia, Italy, October 24, 2011, <http://www.tofinosecurity.com/downloads/477>
- [13] **Byres E.**, "SCADA and ICS Cyber Security: Facing the Facts", Tofino, May 03, 2013, <http://www.tofinosecurity.com/blog/scada-and-ics-cyber-security-facing-facts>
- [14] **Peterson D. G.**, "Luigi Vulnerabilities II", Digital Bong, September 2011, <http://www.digitalbond.com/2011/09/14/luigi-vulnerabilities-ii/>
- [15] **Byres E., Ginter A., and Langil J.**, "How Stuxnet Spreads A Study of Infection Paths in Best Practice Systems", 22 February 2011, <http://abterra.ca/papers/How-Stuxnet-Spreads.pdf>



## **Protecting Civilians from Activities Related to Cyber Conflict While Respecting the International Human Rights Law Principles**

Ljubica Pendaroska

PhD candidate in International Law and International Relations

Personal Data Protection expert

Cyberspace presents new opportunities and new challenges for states and the international community as a whole, while creating policies in different areas of social life, including human rights and freedoms, national defense, security, communication, etc. The threats from cyber adversaries are continuing to grow in scale and sophistication. Public and private organizations in various sectors worldwide now openly acknowledge that cyber attacks are one of the most prevalent and high impact risks they face. Staying protected against cyber-security threats requires that all users, ranging from children and their parents to the most sophisticated users, be aware of the risks and improve their security practices on an ongoing basis. But for international lawyers it also presents cutting-edge issues of international law, which aim at a very fundamental question: how do/can we apply old laws to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?

It is an undeniable fact that cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.<sup>1</sup> Furthermore, in the opinion of most of those whose specialty this subject-matter is, but also, according to the official position of most of the countries in the world, international law principles do apply in cyberspace. This view has not necessarily been universal in the international community, however. In the opinion of several countries existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task and that we need new treaties to impose a unique set of rules on cyberspace.

### **I. Circumstances and conditions affecting the human rights legal framework related to cyberspace activities**

Prior to acceding to the international framework for the protection of human rights that is relevant in terms of cyber activities, it is necessary to indicate the circumstances and events that affect: 1) the process of creation and content of the legal framework; 2) the implementation of the existing legal framework, and 3) the process of amending and adapting the states' system solutions. This fact, logically, leads one to the question: How the geo-political environment, the security trends themselves and human rights influence the creation of national and international legislation for the protection of

---

<sup>1</sup> In particular, because the tools of conflict are constantly evolving, one relevant body of law - international humanitarian law, or the law of armed conflict - affirmatively anticipates technological innovation and stipulates that its existing rules will apply to such innovation. Certainly, new technologies raise new issues and thus, new questions. Developing common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area. See more: International Law in Cyberspace: remarks, Harold Hongju Koh, USCYBERCOM Legal Conference.

# COMPENDIUM 2015

human rights and freedoms? It should be borne in mind that finding the right balance between the protection of the human rights and national security in the age of fast and enormous technological development, rapid development of forms of communication and exchange of information is a serious challenge.

In that spirit, special attention should be given to the following phenomena, which are characteristic of contemporary life:

- Globalization as a process - Thanks to globalization and technological development, many non-state actors (groups and individuals), but also some states, have gained strategic power;
- Redefinition and redistribution of power - especially considering the economic aspect of redefinition of power, in the sense that tectonic changes in the world inevitably have led to a situation where a huge part of the largest economies in the world are now corporations, as well as countries with an annual budget lower than the annual sales of some powerful companies.<sup>2</sup> Similarly, Al Gore said that "More money is allocated by markets around the world in one hour than by all the governments on the planet in a full year."<sup>3</sup>

All those processes (globalization, redefinition and redistribution of power) are causing changes in security challenges, creating modern security threats that are hybrid and composed of: some states, terrorists, criminals, insurgents, religious extremists. The challenge posed by this kind of threats is that only a few security concepts could partially be applied to counter them. All this highlights the need to review the content and composition of a new legal framework to guarantee and protect the human rights and freedoms.

This change has been initiated after World War II, when Geneva Conventions and codification of principles of war fighting were adopted.

One of the most important benefits of the adoption of the Geneva Convention is represented by the fact that it determines a list of human rights articulated in the Convention. Its title reveals that the main focus was on the protection of civilian persons and their humane treatment. The very decision to dedicate the Fourth Geneva Convention to persons and not to Governments signified a growing awareness in International law about the idea that people are not merely the resources of states, but rather that they are worthy of being subjects of International law.<sup>4</sup>

General principles of International Law are nowadays accepted by a vast majority of scholars as a normative source of law-framework and a legal platform for states in producing mechanisms for preventive protection of civilians and their property.


Moreover, whenever talking about the system of protection of human rights in the context of cyber activities ahead one should examine the bigger picture, which includes the domestic law of states and international law, with all their mutual interactions and dependencies.

---

<sup>2</sup> In his 2011 article, Jason Soul argued that "fifty-one of the world's one hundred largest "economies" are now corporations. He also stated that "in 2007 Finland's budget was about 40 billion euros, 20% less than Nokia's annual sales. Jason Soul, February 2011, Corporations are more powerful than Governments, Skoll World Forum on social entrepreneurship

<sup>3</sup> [http://www.nytimes.com/2008/03/business/worldbusiness/11iht-gore.4.10942634.html?\\_r=2&](http://www.nytimes.com/2008/03/business/worldbusiness/11iht-gore.4.10942634.html?_r=2&)

<sup>4</sup> This was concluded by Eyal Benvenisti in his book titled "The International Law of occupation", Princeton University Press, 1993, p.104.



Everything that was said so far in relation to the framework for protecting human rights and freedoms should be considered in the direction of understanding the applicability of Human rights law to cyber space activities.

Overall, issues related to the application of the principles of international human rights law in the field of cyber activities will be presented through the following segments: International Law on Human Rights in Cyberspace: What we know and International Law on Human Rights in Cyberspace: Challenges and Uncertainties.

## II. International Law on Human Rights in Cyberspace

### 1. What we know?

Although at first it seems that the international humanitarian law is the only body of international law that applies in cyberspace, it is not the only international law that applies in cyberspace. Obviously, cyberspace has become pervasive in our lives, not just in the national defense arena, but also through social media, publishing and broadcasting, expressions of human rights and expansion of international commerce, both through online markets and online commercial techniques.

International law, among others, is connected to protecting civilians related to cyber space activities. It consists of:

- 1) Human Rights Law<sup>5</sup>
- 2) Refugee Law<sup>6</sup>
- 3) International Humanitarian Law<sup>7</sup>
- 4) International Disaster Relief laws<sup>8</sup>

Although provisions of International Humanitarian Law don't specifically mention cyber activities, that doesn't mean that such activities and operations are not subject to the rules of IHL. Namely, IHL provisions are broad enough to accommodate all forms and kinds of methods, activities and weapons, including cyber activities as well.

The main obligations of human rights law derive from sources such as:

- The Universal Declaration of Human Rights<sup>9</sup>
- International Covenant on civil and political rights<sup>10</sup>
- International Covenant on economic, social and cultural rights<sup>11</sup>

---

<sup>5</sup> A set of international rules on the basis of which individuals and groups can expect and/or claim certain behavior or benefits from governments.

<sup>6</sup> Law addressing rights of refugees and the obligations of states to protect those rights.

<sup>7</sup> A set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict.

<sup>8</sup> The laws, rules and principles concerning the access, facilitation, coordination, quality and accountability of international disaster response activities in times of non-conflict related disasters, which include preparedness for imminent disaster and the conduct of rescue and humanitarian assistance activities.

<sup>9</sup> Adopted by the United Nations General Assembly on 10 December 1948, ratified on 16 December 1949. For more see: <http://www.un.org/en/documents/udhr/index.shtml#a19>.

<sup>10</sup> Adopted and opened for signature, ratification and accession by the General Assembly 1966. For more see: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

<sup>11</sup> <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>.

# COMPENDIUM 2015

- Regional treaties, including the European and American conventions on human rights
- A large set of authoritative and influential sources interpret or elaborate existing documents and agreements.<sup>12</sup>

The European Commission established the *Cyber security Strategy of the EU: An Open, Safe and Secure Cyberspace* in 2013, which outlines the EU's vision in this domain, clarifies the roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment more safe. The EU vision presented in this strategy is articulated in five strategic priorities, such as: (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy; (iv) developing the industrial and technological resources for cyber security and (v) establishing a coherent international cyberspace policy for the EU and promoting the core EU values.

Cyber-communication is increasingly becoming a dominant mode of expression nowadays. Most of the time, people express their views by blogging, tweeting, commenting or posting videos and commentaries. But, even though the circumstances have changed a lot, the Universal Declaration of Human Rights (adopted more than 70 years ago) was forward-looking in anticipating these trends. According to the Declaration "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This means that human beings are entitled to certain rights, whether they choose to exercise them in a open agora or on the internet.

Besides the above mentioned legal acts and other documents that touch upon issues of human rights and freedoms, in the sphere of cyberspace activities it is very important to emphasize that in 2012 the UN Human Rights Council adopted a Resolution according to which "The same rights that people have offline must also be protected online, in particular the freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."


In essence, human rights are natural, universal and limited in two ways - in terms of respecting the rights of other people and in terms of ensuring public safety. Hence, they should be set or adjusted precisely, so as to be somewhere "in the middle" to avoid any of the two possible extremes - tyranny or anarchy. This is particularly important in modern times of intense globalization and the Internet, a virtual world that essentially "knows no borders"!

The most endangered human rights and freedoms as a consequence of the activities in the cyberspace are the following ones: freedom of expression and information, privacy, the right to protection of personal data, the right to express oneself and to seek information, Intellectual property rights, the freedom of association, communication and correspondence, the right to political participation and all other human rights and peace may be endangered or injured through illegal activities in cyberspace.<sup>13</sup> Two rights enumerated in the International Covenant on Civil and Political Rights may be relevant to the cyber domain. Article 17 (protecting privacy and reputation) might be

---

<sup>12</sup> Including notably the jurisprudence of the European Court of human rights, the General Comments of the Human Rights Committee, Findings and Reports of UN Special Reporters, the UN General Assembly Resolutions, Important statements of non-official expert bodies (for instance: Johannesburg Principles on National Security, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights).

<sup>13</sup> See more Rikke Frank Jørgensen, "Human Rights in the Global Information Society, MIT Press, June 16, 2006.



relevant to cyber operations intended to harm the reputation of an individual for example, by falsifying computer-based records about transactions in which he or she had engaged or to uncover private information about an individual (potentially constituting a provocation prior to conflict if the individual is prominent or politically influential). Article 19 (protecting rights to seek information) might be relevant to cyber attacks intended to prevent individuals from obtaining service from the Internet or other media. A number of other rights, such as the rights to life, to health and to food, may be implicated as well depending on the nature and targets of the cyber activities.<sup>14</sup>

Talking about the relation between human rights and cyberspace it is interesting to point out that in a number of states, the right to access the Internet is guaranteed as a fundamental human right in their societies, which means that actions curtailing or preventing the access to Internet violate that human right!<sup>15</sup>

## 2. International Law on Human Rights in Cyberspace:

### Few challenges and uncertainties

The main dilemma still persists: how far has the international community come in applying established law to new facts and explaining the positions to those who are not included in the process. Inter alia, another interesting question is: How can a use of force regime take into account all of the novel kinds of effects that States can produce through the click of a button?

There remain many other difficult and important questions about the application of international law of human rights to activities in cyberspace for example, about the implications of sovereignty and neutrality law, enforcement mechanisms and the obligations of States concerning "hacktivists" operating from within their territory. Legislative efforts are not just in the areas of cyberconflict, but also in many other cyber areas: cybersecurity, cybercommerce, fighting child pornography and other forms of cybercrime, stopping intellectual property piracy, as well as promoting free expression and human rights.

Policymakers and commentators are debating whether "rules of the road" should be established for behavior in cyber space.<sup>16</sup>

Finally, there remain some questions to think through, that so far lack response: How to find the right balance between human rights and security? Do we need a Global Treaty on Cybersecurity and does/how its implementation will contribute to a higher level of protection of human rights and freedoms?

---

<sup>14</sup> Herbert Lin, "Cyber conflict and International Humanitarian Law", *International Review of the Red Cross*, Volume 94, No. 886, 2012, 515-531.

<sup>15</sup> For instance, the right to access the Internet is guaranteed as a human right in France, where the top court declares that internet access is a "basic human right"; in Finland, where the 1Mb Broadband access is a legal right; in Estonia and Spain as well.

<sup>16</sup> For more see William Hague, "Security and freedom in the cyber age - seeking the rules of the road", Munich Security Conference, February 2011.

## International Law of State Responsibility: Unlawful Orchestration *Versus* the Omission of the Duty to Prevent the Unlawful Cyber Operation

Andraz Kastelic\*

As much as the orchestration of the unlawful interstate cyber operation constitutes a violation of international law,<sup>1</sup> so does the deliberate failure to take 'appropriate'<sup>2</sup> or 'effective'<sup>3</sup> measures, to 'deploy adequate means, to exercise best possible efforts, to do the utmost'<sup>4</sup> to prevent cyber operations 'contrary to the rights of other States'.<sup>5</sup> In spite of the wide recognition of the need for international cooperation in the cyber era, States remain the rational, selfish actors of the international legal order.<sup>6</sup> In a world where 'the tendency for those in power to achieve their ends through private or non-State actors, thereby avoiding attribution'<sup>7</sup> is prominent, the doctrine of due diligence offers a viable instrument for the invocation of the State responsibility and, consequently, allows the employment of legal self-help measures.

While it may be beyond the scope of this text to address the possible legal reactions of self-help, the following lines outline the international law of State responsibility for the unlawful, unforceful cyber operations, indicate the issue of the traditional understanding of this legal framework in the new environment and draw attention to the principle of due diligence. Lastly, the article escapes the purely doctrinal nature by proposing some of the implementation methods available to national States to assume the role of a diligent neighbour and respect the obligations imposed by the existing international legal regime.

### 1. How the attribution standards of the traditional concept of the international law of State responsibility rendered law useless

The invocation of State responsibility in the existing legal regime requires two fundamental conditions to be met - the cyber operation must constitute a breach of international obligations and should be attributed to a State.<sup>8</sup>

\* PhD candidate, Sheffield University Law School, MA, University of Nottingham. I am grateful to Dr Russell Buchan for his useful comments on a draft version of this article.

<sup>1</sup> See, for example, Jan E. Messerschmidt, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' 52 (2013) *Columbia J of Transnational L* 275

<sup>2</sup> ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities II (part two) (2001) *Ybk of the Int L Commission arts 3, 11*. See also Pierre-Marie Dupuy, 'Overview of the Existing Customary Legal Regime Regarding International Pollution' in Daniel B Magraw (ed), *International Law and Pollution* (University of Pennsylvania Press 1991) 61

<sup>3</sup> *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda) [2005] ICJ Rep 168 253.

<sup>4</sup> *Responsibilities and Obligations of States Sponsoring Persons and Entities With Respect to Activities in the Area* (Advisory Opinion) 34 [2011] ITLOS Rep 1034

<sup>5</sup> *Corfu Channel* (United Kingdom of Great Britain and Northern Ireland v Albania) (Merits) [1949] ICJ Rep 22

<sup>6</sup> Scott Shackelford and Andraz Kastelic, 'Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity' (forthcoming) *New York University J of Legislation and Public Policy*

<sup>7</sup> Gordon A Christenson, 'Attributing Acts of Omission to the State' 12 (1990) *Michigan Journal of International Law* 312, 313

<sup>8</sup> *Responsibility of States for Internationally Wrongful Acts* (2001) *Ybk of the International Law Commission* (vol II, Part Two) (ARSIWA) art 2

The developing legal scholarship points at a number of legal obligations interstate unforceful cyber operations may violate; they may, *inter alia*, amount to the internationally prohibited use of force<sup>9</sup>, constitute unlawful act of coercion<sup>10</sup>, a violation of the State sovereignty<sup>11</sup> or a breach of international contractual obligations such as the Vienna Convention on Diplomatic Relations<sup>12</sup>.

Secondly, the cyber operation must be directly or indirectly attributed to a particular (group of) State(s). This is where the cyber sphere and international law seem to collide. The responsibility by attribution has attracted an extensive legal debate<sup>13</sup> and the evolution of legal standards pertaining to State responsibility has been anything but painless.<sup>14</sup> Modern technical means of imitating and concealing the origins of cyber operations rendered the factual attribution unreliable<sup>15</sup> and the application potential of corresponding overall and effective legal control standards questionable.<sup>16</sup> Routing and spoofing techniques as well as the clandestine nature of cyber operations prevents the injured State to present 'clear and convincing'<sup>17</sup> or 'fully conclusive'<sup>18</sup> technical proof to tie the origin of the attack to any State through the traditional overall and effective control standards recognised by international law.<sup>19</sup> Specifically, there is a clear deficit of substantial technical evidence showing that the perpetrators 'acted in complete dependence'<sup>20</sup> on a certain State or that any State 'provided a support and had a role in organizing as well as coordinating'<sup>21</sup> the perpetrators.<sup>22</sup> All technical means for the direct attribution of a cyber attack 'are inherently limited [and] include attribution delay, failed attribution and misattribution'.<sup>23</sup> In effect, the problem of cyber attacks attribution remains 'one of the most significant challenges'<sup>24</sup> in the attempt to establish State responsibility.

<sup>9</sup> Stuxnet serves as an example. See Michael Schmitt (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (CUP 2012) 56

<sup>10</sup> Note, for example, Buchan's argument, submitting 'these attacks crossed the threshold of exerting influence and amounted to the intentional application of coercion against the Estonian government, seeking to force it to reverse its policy to relocate the statue of the Bronze Soldier'. Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) J of Conflict & Security L 211, 226

<sup>11</sup> Michael N Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law Virginia J of Intl L 54(3) (2014) 705

<sup>12</sup> Consider RedOctober virus. The attackers were after documents of various diplomatic establishments. The act was in violation of the inviolability of the archives and documents pertaining to the diplomatic mission, as codified by the Vienna Convention on Diplomatic Relations (Vienna, 18 April 1961) (VCDR) art 24. See also Kaspersky Labs Global Research & Analysis Team, 'The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies' (Securelist, 14 January 2013) <<http://goo.gl/yUjNqu>> accessed 3 May 2015

<sup>13</sup> For example, Antonio Cassese, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' European J of int Law 18 (4) (2007) 649-668

<sup>14</sup> International law scholarship is not united on the attribution control standards. Note the different understanding of the concept found in two influential international judicial decisions: ICTY arguing for the overall (Prosecutor v Duško Tadić (Judgement) IT-94-1-A (15 July 1999) 4951) and ICJ (Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Merits) [1986] para 105115) for the effective control standard. On the development of attribution control standards see also, for example, James Crawford, State Responsibility: The General Part (CUP 2013) 141-161

<sup>15</sup> '[D]igital attribution regardless of motive can be extremely difficult': Dan Holden, 'Estonia, six years later' (Arbor Networks, 16 May 2013) <<http://www.arbornetworks.com/asert/2013/05/estonia-six-years-later/>> accessed 5 May 2015

<sup>16</sup> See for example, Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17(2) J of Conflict and Security L 229; Norwegian Institute of International Affairs, 'Multinational Experiment 7 Outcome 3 Cyber Domain Objective 3.3 Concept Framework (Version 3.0, 3 October 2012) 8; Scott Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' in C Zossek and K Podins (eds), Conference on Cyber Conflict Proceedings 2010 (CCD COE Publications 2010)

<sup>17</sup> Andreas Zimmermann et al (eds), The Statute of the International Court of Justice: A Commentary (OUP 2012) 1265 as found in Lake Lanoux Arbitration (France v Spain) [1957] Arbitral Tribunal 127.

<sup>18</sup> Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment of 26 February 2007) [2007] ICJ Rep para 208, referring to the Corfu Channel (n 5) 17

<sup>19</sup> Both standards would require technical element of the attribution. This is not available. Revisit Holden (n 15)

<sup>20</sup> Shackelford (n 16) 5 referring to the standards found in ICJ Nicaragua and ICTY Tadić cases.

<sup>21</sup> *ibid*

<sup>22</sup> This dilemma of attribution and the pertaining State control standards may be already witnessed in Case Concerning Military and Paramilitary Activities in and Against Nicaragua (n 14)

<sup>23</sup> David A Wheeler and Gregory N Larsen, 'Techniques for Cyber Attack Attribution' (DA Paper P-3792, US Government Institute for Defense Analyses, 2003) 66

<sup>24</sup> Norwegian Institute of International Affairs (n 16) 8



## 2. Rethinking the breach: doctrine of due diligence in cyberspace

While this may be true, looking beyond the traditional understanding of State responsibility as codified by the International Law Commission<sup>25</sup> may be part of a solution. Think of a cyber operation violating the due diligence principle of international law.

The aforementioned principle prohibits an omission of the diligent behaviour or 'good neighbourliness'.<sup>26</sup> Obligation of due diligence is not an obligation of result and as such does not require the States to prevent or stop the unlawful cyber operation. It does, however, impose the obligation of conduct.<sup>27</sup>

It is a well-established principle of international law; contemporary roots may be found in the Corfu Channel Case, where the International Court of Justice held that State is responsible for failure to take all necessary steps to prevent the internationally wrongful act of Albania.<sup>28</sup> The court reiterated the obligation in the Tehran Hostages case, where Iran was found responsible for making 'no apparent effort to deter or prevent the demonstrators from seizing the [US] Embassy's premise'<sup>29</sup>, an act in clear violation of the international diplomatic law. Since the attribution of unlawful cyber operations seems to be an impossible task, due to the fact that unlawful acts are orchestrated by the individuals with no apparent connections to the governmental, judicial or legislative authority,<sup>30</sup> one must appreciate the excerpt from the Trail Smelter Arbitration, where the tribunal concluded that a 'State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction'.<sup>31</sup> Further international judicial decisions substantiate the existence of the due diligence obligation.<sup>32</sup>

Accordingly, there are two elements of due diligence. Firstly, a State has to deliberately fail to act, specifically instruct inaction to the responsible entity<sup>33</sup> or fail to take 'appropriate measures'<sup>34</sup>, all with the intention to prevent or stop the unlawful act. In other words, there needs to be a clear link between State (in)action and the damage consequential to the cyber operation.<sup>35</sup> The state, however, shall not be accused of negligence if it had no knowledge of the unlawful event taking place.<sup>36</sup> This is a second building block of due diligence.

Note, however, that when establishing whether the State<sup>37</sup> met the conditions of the diligent behaviour, one must consider the economic standard of the State as well as the technical capabilities<sup>38</sup> to prevent the unlawful cyber operations.

<sup>25</sup> ARSIWA (n 8)

<sup>26</sup> Duncan French and Tim Stephens, 'ILA Study Group on Due Diligence in International Law' (First Report, 7 March 2014) 4

<sup>27</sup> Gerhard Hafner and Isabelle Buffard, 'Obligations of Prevention and the Precautionary Principle' in James Crawford, Alain Pellet, and Simon Olleson, *International Law of State Responsibility* (OUP 2010) 521

<sup>28</sup> *Corfu Channel* (n 5)

<sup>29</sup> *Case Concerning United States Diplomatic and Consular Staff in Tehran* (United States of America v Iran) [1980] ICJ Rep 12

<sup>30</sup> Apparent connection would constitute a direct attribution. See ARSIWA (n 8) art 4

<sup>31</sup> *Trail smelter case (United States v Canada)* [1937/1941] RIAA vol III 1905, 1963

<sup>32</sup> See; *Alabama Claims Arbitration* (United States/Great Britain) [1872] 29 RIAA 125, 129; *Case Concerning Gabčíkovo-Nagymaros Project* (Hungary v Slovakia) [1987] ICJ Rep

<sup>33</sup> See *Martin v. Republic of South Africa*, 836 F.2d 91 (2d Cir. 1987), where the State agent, the responsible entity was a hospital.

<sup>34</sup> ILC (n 2)

<sup>35</sup> *Christenson* (n 7) 361-363

<sup>36</sup> *Corfu Channel* (n 5) 18

<sup>37</sup> ILC (n 2) art 3 cmt 13

<sup>38</sup> *ibid* art 4 cmt 5

### 3. Attribution of the non-diligent behaviour and the standard of proof in the cyber realm

The abovementioned two elements of due diligence deserve further attention in the context of attribution. This leads to the standard of proof,<sup>39</sup> which, as explained above, is the burning issue of the attribution utilising the traditional State responsibility doctrine.

While a mere control over the internet infrastructure (directly or indirectly through the Internet Service Providers (ISPs)) located on the territory of one State does not prove the State was indeed aware of the unlawful act,<sup>40</sup> it doesn't constitute prima facie State responsibility either. The ICJ, referring to the existing legal practice, allowed for more liberal standard of proof. Circumstantial proof, one that is 'drawn from inferences of fact'<sup>41</sup>, was allowed when considering whether Albania was aware of the minelaying operation in the Corfu channel.<sup>42</sup> With this in mind, it would be acceptable to infer that States with an extensive history of internet censorship and monitoring, States that 'constantly [keep] a close watch over the'<sup>43</sup> ISPs<sup>44</sup> and internet traffic in general do indeed possess the knowledge of the malicious cyber activity using the internet infrastructure under its jurisdiction. Additionally, the implied knowledge of the malicious interstate cyber operation would have been apparent when the national legalisation requires ISPs to report such incidents to one of the organs of the State. Technology is not a limitation here, particularly not in the case of DDoS attacks; computer science scholarship ensures that ISPs can indeed spot not only the incoming but also an outgoing DDoS attack.<sup>45</sup>

Secondly, the injury caused by the unlawful cyber operation must be consequential to a deliberate State inaction or insufficient action.<sup>46</sup> To illustrate: if, for example, a State knew of but neglected an ongoing cyber operation or made no apparent effort to prevent it, one could argue that the State in question is responsible for the omission. But, putting well-connected national intelligence agencies aside, democratic societies transferred most of the internet regulation powers to the ISPs. In this case, the injured State must establish a clear connection between the ISP and the State. It must provide that inaction of ISP was consequential to the insufficient actions or complete inaction of the State. In this case, the international legal practice dictates<sup>47</sup> that the injured State is not aided by the low(er) threshold of proof as 'the most exacting standards of [...] proof of official inaction before attributing an omission to the State'<sup>48</sup> are required. While this may prove to be an impossible task for an injured State,

<sup>39</sup> Some authors went as far as to propose that there is no general burden on a claimant to prove attribution of an omission. See, for example, Ian Brownlie, *System of the Law of Nations: State Responsibility* (Clarendon Press 1983) 16465. Since this cannot be particularly useful in the context of State responsibility invocation for the purpose of self-help remedies employment, the present text omits further discussion on the potential burden of proof shift.

<sup>40</sup> *Corfu Channel* (n 5) 18

<sup>41</sup> *Corfu Channel* (n 5) 18

<sup>42</sup> Mind that the circumstantial proof must 'leave no room for reasonable doubt': *ibid* 19

<sup>43</sup> *ibid*

<sup>44</sup> Including mobile internet service providers. If the speed may still be an issue and the reliability is still not on a par with the cable internet providers, the mobile internet may soon allow for the orchestration of the cyber attack.

<sup>45</sup> See, for example, Tao Peng, Christopher Leckie and Rotagiri Ramamohanarao, 'Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring' in Nikolas Mitrou et al, *Networking 2004 - Lecture Notes in Computer Science* (vol 3042, Springer 2004) 771-782; Jelena Mirkovic, Gregory Prier Peter Reiher, 'Attacking DDoS at the Source' *Network Protocols 2002* (Proceedings 10th IEEE International Conference); Brant Rowe et al, 'The Role of Internet Service Providers in Cyber Security' (research brief, Institute for Homeland Security Solutions, 2011). Outgoing DDoS attack is the one that involves the agent in control of the command and control server of the attack.

<sup>46</sup> *Christenson* (n 7) 361363

<sup>47</sup> The Iran-United States Claims Tribunal refused the attribution of the omission to control the perpetrating private party without a proof of direct link between the perpetrators and the government or a conscious governmental decision not to protect. See *Yeager v Islamic Republic of Iran* [1987] 17 Iran-US CTR 92; William L. Pereira Assoc., *Iran v Islamic Republic of Iran* [1984] 5 Iran-US CTR 198

<sup>48</sup> *Christenson* (n 7) 366

inaction of the allegedly perpetrating State could be a result of the absence of the appropriate domestic legislation. Nevertheless, due diligence 'requires a State to keep abreast of technological changes and scientific developments'<sup>49</sup>, to 'inform itself of factual and legal components'<sup>50</sup> and, specifically, formulate appropriate policies 'expressed in legislation and administrative regulations and implemented through various enforcement mechanisms'<sup>51</sup>.

Under these circumstances States must recognise the obligations of due diligence in their strategic policies and implement them in their respective legal frameworks. For instance, the national legislation and policy instruments could impose the obligation on ISPs, gatekeepers of the internet access, to report and prevent any potential malicious behaviour utilising a specific infrastructure.

In summary, cyberspace made the attribution of the unlawful cyber operation orchestration close to impossible. In particular, modern spoofing techniques rendered the standards of attribution and proof within the context of traditional international law of State responsibility unattainable. However, as much as it is deemed unlawful to orchestrate a cyber operation, neglecting or ignoring such an act may rightfully be labelled as internationally wrongful. States are not only responsible for the orchestration of unlawful cyber operations but also for failing to prevent them. Attribution of an omission of the diligent behaviour in cyberspace is possible. Firstly, international legal practice allows for circumstantial proof when it comes to attributing the knowledge. Secondly, the lack of appropriate national legislation may be the root of the injuries caused by the unlawful cyber operation. Therefore, it is crucial for the States to recognise due diligence and respond with the appropriate domestic legislation. One that, for example, puts an obligations on ISPs to report any outgoing unlawful cyber operations, may just do the trick.

---

<sup>49</sup> ILC (n2) art3 cmt 11

<sup>50</sup> *ibid* art3 cmt 10

<sup>51</sup> *ibid*



## **Contemporary Trends and Challenges in Cyber Security Legal, Operational and Technical Aspects**

**Antun Matija Filipović**

Contemporary trends in the field of cyber security point to the fact that the already wide influence of information-communication technologies is becoming ever stronger and is starting to encompass almost all areas. Accordingly, numerous security threats to information systems have become a daily phenomenon. Security threats appear in the form of computer frauds, espionage (intelligence or technology based), sabotage (intentional or accidental), vandalism, fire, floods and many other increasingly innovative forms.

More than a million people are affected by the consequences of cyber-crime daily and every second there are around twelve new cyber-crimes taking place, which points to the fact that the dynamics in the field of cyber security are great and complex. Thus, cyber security is a never-ending process that we must learn from, making decisions based on knowledge, thereby frequently changing our customary ways of thinking and managing risks. Innovativeness of the transgressor can be beaten only if we use our own innovativeness in defence.

Recent events in the context of global relations are extremely interesting. Russia and China signed a cyber-security pact (an agreement on mutual nonaggression) on 9 May 2015, which indicates how big forces perceive the problem. Moreover, cyber-attacks basically not motivated by financial but various activist reasons are becoming more frequent.

Three such interesting attacks that occurred this year have been motivated by ecological reasons (in the case of hacking the web site of the controversial Maun Kea telescope), the Baltimore police conduct (in the case of publishing user accounts and passwords of workers' e-mails) and xenophobia (in the case of hacking the web site of the Mauthausen Nazi concentration camp). Attacks such as these can be expected to become more frequent, which does not mean that the financially motivated ones will disappear or decrease in intensity. Along these lines, a specific case has been recorded this year in which Tiversa, a company specialized for cyber safety has staged a security incident in order to extort money from its clients.

Information-communication technologies (applying computers and communication equipment for storing, transfer and management of data) are ubiquitous and have thoroughly changed the functioning in the area of work, fun, buying and paying, as well as the methods of eavesdropping, cheating, stealing and leading wars.

Information is an extremely important and frequently the most expensive resource, and as a valuable asset, it must be protected so that we can avoid various disturbances. It is precisely on these grounds that new and ever more complex threats are appearing, making information and resources of it increasingly more vulnerable.

Timely disposition, accuracy and confidentiality of information are elements of crucial importance. The security of information systems encompasses all processes and mechanisms used to protect

computers and similar equipment from unintentional or unauthorized access, change or destruction, but also unplanned events and natural disasters. Pursuant to standard ISO 27001, security is a set of efforts directed at the protection of data and computer resources with respect to confidentiality, integrity and availability.

Attacks on information systems can, according to their type, be divided into active (they change the system) and passive (they do not change the system). The properties of active attacks are such that they change the data flow or create a false data flow and mask the input by supervising or repeating the login, which makes it hard to prevent them. It is of crucial importance to spot them on time and control the scope of damage they can cause. The properties of passive attacks are such that they appear in the forms of wiretapping, reading the content of the data traffic and analyzing the structure of data traffic, which makes it hard to discover them and protection methods are mostly based on prevention.

Protection methods are divided into proactive (the ones that create or control a situation rather than respond to it after it has happened) and reactive (the ones that act in response to a situation rather than create or control it).


The anatomy of information system attacks can be divided into research and assessment, abuse and penetration, privilege increase, keeping of access and denial of service. There are four main categories of information system attacks: interruption, interception, alteration and fabrication. The targets of information system attacks can be data, software and hardware.

The basic concepts of security are: identification (it presents the mechanism of recognizing users) and authorization (it presents the verification of the right of the user's access).

In case of cyber security risks it is important to recognize the difference between risk and uncertainty. When the chances are known but not the outcome we talk of risk, whereas in case of uncertainty not even the chances are known. Cyber security must not be brought into the domain of uncertainty, because that would mean that not all necessary or possible measures have been undertaken. Risk of course presents a threat, but indisputably also an opportunity. What the opportunity will be like depends primarily on the previously devoted efforts and undertaken measures. Risk should be looked at in the context of the probability of its appearance and not through the consequences its realization might have.

The legal aspects of cyber security transgress legal regulations. Cyber-crime can be divided into five offence categories: intrusive offences, content-related offences, copyright and trademark related offences, computer-related offences and combination offences. Intrusive offences are illegal access, data espionage and data interference; content-related offences include pornography, child pornography, racism, hate speech, glorification of violence, religious offences and spam; copyright and trademark related offences are common copyright offences and trademark violations; computer related offences are fraud, forgery and identity theft; while combination offences include cyber terrorism, cyber warfare and cyber laundering.

Operational aspects of cyber security have three levels: employees (human aspect), products (physical aspect) and procedures (organizational aspect). Practical steps towards security for companies include: data encryption, application of digital certificates, adoption and audit of data loss prevention policy, implementation of transmission media policy, protecting the server from malicious software, application of undesired e-mail filters, installation of comprehensive end-security solutions,



introduction of security network hardware and software, regular update of operating systems and software and continuous user education. Practical steps towards security for users include: the use of antivirus software, use of the firewall, regular update of operating systems and software, complete avoidance of pirate software, blocking and ignoring popup windows, caution when downloading e-mail attachments, avoidance of public access points without a secure VPN connection, use of strong passwords in all possible places, caution when sharing information on social networks and regular control of account and credit card balance.

Technical aspects of cyber security are influenced by numerous trends. Trends like Bring Your Own Device (BYOD) cause increased use of personal devices in businesses and create entirely new cyber security issues. Near Field Communication (NFC) technology for mobile payment systems converts mobile platforms into readily available targets for financially motivated cyber-crimes. Social Media (SM) continue to be universally adopted, so the amount of malware and phishing attacks increases dramatically and exponentially. Ransomware (RW) attacks are a result of increase in sophistication of cyber-attacks, they lock down a computer, device or service and hold the data hostage if the user does not pay ransom to the attacker. As services and infrastructure continue to move to the cloud, Distributed Denial of Service (DDoS) attacks are becoming an ever-bigger threat on a daily basis, as they can cripple entire infrastructures. The Internet of Things (IoT) (physical objects embedded with electronics, software, sensors and connectivity) are enjoying huge popularity and are opening a whole new range of problems.

These critical security controls can help with cyber security related issues during all stages (from preparation to response):

- inventory of authorized and unauthorized devices and software
- secure configurations for hardware, software and network devices
- secure network engineering and wireless access control
- limitation and control of ports, protocols and services
- application software security and malware defenses
- controlled use of administrative privileges
- account monitoring and control with controlled access based on the need to know
- maintenance, monitoring and analysis of audit logs
- data protection and recovery capability
- security skills assessment and training to fill gaps
- continuous vulnerability assessment and remediation
- penetration tests and red team exercises
- boundary defense and security incident response and management

# COMPENDIUM 2015

Currently, there are many projects dealing with cyber security. Such projects are needed in order to enable us to respond to expanding issues of cyber security. Three such projects are highlighted here:

- EU CBRN CoE Project 19 - Development of procedures and guidelines to create and improve secure information management systems and data exchange mechanisms for CBRN materials under regulatory control: targets people involved in the manufacture, processing, transport, use and disposal of CBRN materials, competent authorities that have regulatory authority over CBRN materials and agencies that have responsibilities involving the security of CBRN materials
- European Advanced Cyber Defense Centre - National Anti-Botnet Support Centers: provides end-to-end approach from detection to protection and tools and sensors to detect botnet related cyber threats and mitigate cyber-attacks and builds on data acquired through its European center to create prevention strategies and improve the awareness and adoption across users
- IBM X-Force Exchange: cloud based threat intelligence platform which enables rapid research of the latest global security threats while actionable intelligence can be aggregated and collaborated with peers

Cyber security solutions need not necessarily be very expensive or technically complicated, because already the respect for some simple rules of information and web ethics frequently has a positive preponderance. Concerning the fact that there is no ultimate security in any area, including this one, all cyber security aspects must be permanently supervised, analyzed, interpreted, evaluated and tested.

## Biography

**Antun Matija Filipović, M.Sc., lect.**

College of Occupational Safety and Health, Ivana Lučića 5, 10000 Zagreb, Croatia

antun.matija.filipovic@vss.hr

Works at the College of Occupational Safety and Health in Zagreb, lecturing (three courses): Management of Safety, Computer Science and Safety of Computer Systems. Certified as an e-learning tutor, project manager and auditor of many international standards. Formal education broadened by educational courses in the areas of project management, advanced information systems and technologies, social accountability, graphic design and Internet marketing. Member of the management board of Alumni Association of the College of Occupational Safety and Health and member of the international organizing committee of the World Congress on CBRNe. Served as a member of the National Council for Safety at Work of the Republic of Croatia - an advisory body to the Croatian Government from 2011 to 2014. He has a total of sixteen years of work experience in on research and development and engineering jobs in the fields of advanced information systems and technologies and education. Researches the possibilities and advantages of the application of contemporary information-communication technologies in the fields of education and integral safety.

