

UDK 355/359

CODEN SMOOAM

ISSN

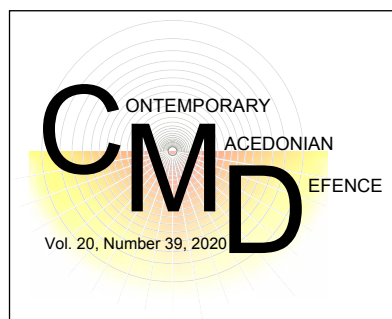
1409-8199

МЕЃУНАРОДНО НАУЧНО СПИСАНИЕ

# СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА



MINISTRY OF DEFENCE  
REPUBLIC OF NORTH MACEDONIA



VOL. XX  
SKOPJE  
DECEMBER 2020

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА	Год. 20	Број 39	Стр. 1-182	Скопје 2020
CONTEMPORARY MACEDONIAN DEFENCE	Vol.	No	pp	Skopje



MINISTRY OF DEFENCE  
REPUBLIC OF NORTH MACEDONIA

**СОВРЕМЕНА** **CONTEMPORARY**  
**МАКЕДОНСКА** **MACEDONIAN**  
**ОДБРАНА** **DEFENCE**

---

ISSN 1409-8199  
e-ISSN 1857-887X

Година 20, бр. 39, декември 2020 / Vol. 20, No. 39, December 2020

Skopje  
December 2020



# **СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА**

Издавач:

**МИНИСТЕРСТВО ЗА ОДБРАНА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА**

Министерство за одбрана

„СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА“

„Орце Николов“ 116 1000 Скопје

Телефони: 02 3128 276, 02 3113 527

Интернет адреса:

WEB на Министерството за одбрана:

<http://www.morm.gov.mk/sovremena-makedonska-odbrana/>

Списанието излегува два пати годишно.

ISSN 1409-8199

Скопје, декември 2020 година

Сите права се резервирани

Се забранува репродуцирање на публикацијата и нејзините делови, како и нивно трансформирање во разни медиуми: електронски, магнетни ленти, механичко фотокопирање, снимање и друго, без писмено одобрение на издавачот и авторите.

# **CONTEMPORARY MACEDONIAN DEFENCE**

Publisher:

**MINISTRY OF DEFENCE OF THE REPUBLIC OF NORTH MACEDONIA**

Ministry of Defence

„CONTEMPORARY MACEDONIAN DEFENCE“

„Orce Nikolov“ 116 1000 Skopje

Tel.: 02 3128 276, 02 3113 527

Internet address:

WEB of the Ministry of Defence:

[www.morm.gov.mk/contemporary-macedonian-defence/](http://www.morm.gov.mk/contemporary-macedonian-defence/)

The magazine is published twice a year

ISSN 1409-8199

Skopje, December 2020

All rights reserved

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic tape, mechanical photocopying, recording or otherwise, without permission in writing from the publisher and authors.

# СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА

---

МЕЃУНАРОДНО НАУЧНО СПИСАНИЕ НА  
МИНИСТЕРСТВОТО ЗА ОДБРАНА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

*Радмила ШЕКЕРИНСКА, претседател на Издавачкиот совет*

*Марина МИТРЕВСКА, главен и одговорен уредник*

*Беким МАКСУТИ, заменик главен и одговорен уредник*

## **МЕЃУНАРОДЕН УРЕДУВАЧКИ ОДБОР**

*Мухамед РАЦАЈ*

*Нано РУЖИН*

*Тони МИЛЕСКИ*

*Николина КЕНИГ*

*Никола ДУЈОВСКИ*

*Наташа ПЕЛИВАНОВА*

*Ана ЧУПЕСКА*

*Александра ДЕАНОСКА ТРЕНДАФИЛОВА*

*Елениор НИКОЛОВ*

*Менде СОЛУНЧЕВСКИ*

*Џелал НЕЗИРИ*

*Жанет РИСТОСКА*

*Паскал МИЛО*

*Антон ГРИЗОЛД*

*Зоран КЕКОВИЌ*

*Синиша ТАТАЛОВИЌ*

*Јанцислав ЈАНАКИЕВ*

*Дезире ПАНГЕРЦ*

*Оливера ИЊАЦ*

*Мајкл ШУЛЦ*

*Патриција ФАРАЛДО КАБАНА*

*Емануела Ц. ДЕЛ РЕ*

*Еике АЛБРЕХТ*

**Секретар:** *Жанет РИСТОСКА*

**Техничка подготовка:** Умит Реџеџи

# CONTEMPORARY MACEDONIAN DEFENCE

---

INTERNATIONAL SCIENTIFIC JOURNAL OF  
THE MINISTRY OF DEFENCE OF THE REPUBLIC OF NORTH MACEDONIA

*Radmila SHEKERINSKA, Chairperson of the Editorial Board*

*Marina MITREVSKA, Editor-in-Chief*

*Bekim MAKSUTI, Co-Editor-in-Chief*

## **INTERNATIONAL EDITORIAL BOARD**

*Muhamed RACAJ*

*Nano RUZHIN*

*Toni MILESKI*

*Nikolina KENIG*

*Nikola DUJOVSKI*

*Natasha PELIVANOVA*

*Ana CHUPESKA*

*Aleksandra DEANOSKA TRENDAFILOVA*

*Elenior NIKOLOV*

*Mende SOLUNCHEVSKI*

*Djeral NEZIRI*

*Zhanet RISTOSKA*

*Paskal MILO*

*Anton GRIZOLD*

*Zoran KEKOVIĆ*

*Siniša TATALOVIĆ*

*Yantislav YANAKIEV*

*Desirée PANGERC*

*Olivera INJAC*

*Michael SCHULZ*

*Patricia FARALDO KABANA*

*Emanuela C. DEL RE*

*Eike ALBRECHT*

**Secretary:** *Zhanet RISTOSKA*

**Processing:** *Umit Redzpi*

**Proofreading and Editing:** *Rozi GROZDANOVSKA, Martina KIMOVSKA*



## **CONTENTS:**

Christophe CHICLET	
<b>BALKANS: THE SOUTH-EAST GATEWAY TO EUROPE</b> .....	9
Toni MILESKI	
Eike ALBRECHT	
<b>INTRODUCTION OF THE EU-CHINA RELATIONS: HISTORICAL OVERVIEW OF STRATEGIC PARTNERSHIP</b> .....	19
Armin KRŽALIĆ	
<b>MIGRANTS IN THE PUBLIC DISCOURSE OF THE CITIZENS OF BOSNIA AND HERZEGOVINA</b> .....	39
Ivan JOVETIC	
<b>TECHNOECONOMIC CHANGES AND SECURITY: NEW PARADIGM?</b> .....	53
Igor GJORESKI	
<b>NATO BURDEN SHARING POLICY AND COVID 19 IMPLICATIONS ON DEFENCE EXPENDITURES</b> .....	69
Karlo PALJUG	
Robert MIKAC	
<b>CONTEMPORARY CRISES: CASE STUDY OF UBER</b> .....	93
Gjorgji VELJOVSKI	
<b>TERRORISM OR INSURGENCY? THE MOST COMMON STRATEGIC FALLACY</b> .....	107
Bojan MIKLOSH	
Lazar DJUROV	
<b>THE INF TREATY - CROSSROADS OF INTERNATIONAL NUCLEAR STABILITY</b> .....	121



Lidija KOS-STANIŠIĆ

Ante ŠUNJIĆ

**DEMOCRATIC CONTROL OF ARGENTINA'S INTELLIGENCE SERVICE DURING  
THE KIRCHNERS' RULE (2003–2015).....135**

Nataša MILETIĆ

**CONTINUITY OF WORK IN THE ENERGY SECTOR IN THE REPUBLIC OF  
SERBIA DURING THE COVID-19 PANDEMIC.....153**

Igor GELEV

Biljana POPOVSKA

**HUMANITARIAN DIPLOMACY AND ITS IMPACT IN TIMES OF PANDEMICS AND  
HEALTH CRISES .....163**

Original scientific article

327(510:497)

327(470+571:497)

327(73:497)

## BALKANS: THE SOUTH-EAST GATEWAY TO EUROPE

Christophe CHICLET<sup>1</sup>

**Abstract:** *Since ancient times, the interest in the control of the Balkans by the Eurasian forces of world Hermland has been great. This geopolitical interest was not accidental, because the Balkans through the corridors of the Aegean Sea, through the Vardar-Moravian valley to the Danube and farther to the Rhine in Germany, served as a real gateway to Southeast Europe. Russia was constantly trying to break through the important Rimland belt and reach the warm seas. In the twentieth century, the USSR in the Stalin era hoped for a possible breakthrough through Tito's Yugoslavia and Albania and eventually Greece to the Adriatic and the Aegean seas. After the historic split with Marshal Tito and the death of Stalin, the Soviet Union temporarily withdrew from such dreams. However, China made a spectacular breakthrough through Albania that lasted until the late 1970s. When the great Asian giant China at the beginning of the 21st century grew into an economic and financial superpower, China's interest in a breakthrough in Europe re-emerged through its south-eastern door to the Balkans. The pharaonic project for the construction of the water road along Corridor 10, codenamed «The Silk Road», was renewed. China seeks to exploit the financial weakness of the impoverished Balkans and made a spectacular entry into Serbia, Greece, Bulgaria, Macedonia, Republika Srpska. This time, China is backed by Russia, which has long dreamed of its own geo-economic interest in the Balkans. But such attempts have not met with much sympathy from the United States and the European Union. The United States is responding through its NATO allies to neutralize the Silk Road project across the Balkan corridor.*

**Keywords:** *China, Russia, USA, South East Europe, Balkans, Geopolitics, Silk Road, Corridor 10*

### Introduction

By disembarking in the Balkans ten years ago, China did not arrive in *terra incognita*. The relations between these two important geo-historical spaces have existed since Antiquity. Although they experienced a long hiatus of nearly twenty centuries, they were resumed in the second half of the twentieth century due to the changes ensuing from the international communist movement. Alexander the Great arrived at the borders of ancient China, Xi Jiping did the opposite. The Chinese Bucephalus was welcome when he arrived at the right moment, taking the place of the European Union and Putin's Russia which disappointed the Balkans that was

---

<sup>1</sup> The Author is doctor of history, specialist for Balkans and member of the Editorial Board of Confluences Méditerranée

deeply upset by the fall of the wall, the implosion-explosion of Yugoslavia, the international financial crisis of 2008 and the decrees of the Troika by the IMF-ECB- EU Commission (1).

In his latest book, *Eurasia. Continent, Empire, Ideology or Project*, (2) the geographer and geo-historian Michel Bruneau considers the Sino-European relations in general and the Sino-Balkan relations in particular throughout the long history. In the first chapter, he announces: “An immense continental space long divided in two, but connected since ancient times”.

The affair began with the Alexandrian epic which took the opposite direction from the great and ancient migratory movements starting from the East to arrive in the West. Alexander of Macedonia is an atypical Greek. Out of the Greek tribes which arrived in the southern triangle of the Balkans, the Macedonians were the last ones and they therefore settled in the north of the Greek area with their city-states and their democratic system. Alexander’s ancestors lived, mixed and blended with the local non-Greek populations (Thracians, Peonians, Illyrians). Alexander, an heir to a kingdom, subdued the Greek cities, but took to fight against the Persian enemy. Moreover, the young king did not stop there. He went as far as India in the north and to the foothills of the Himalayas. When he died, his successors shared the Empire. At the very edge of China, in the 3rd and 2nd centuries BC, two Greek kingdoms developed there, that of Gandhara (northern India) and that of Bactria (northeast of Afghanistan). The latter was destroyed by the Yuezhi nomads between 150 and 130 BC. The successors of King Evkradites could not prevent them from destroying the pearl of the Greco-Bactrian civilization, the city of Evkratideia (now Ai Khanum), as evidenced by the Chinese traveller Zhang Qian sent by the emperor Wudi of the Han dynasty, in the region in 129-128 BC. The Chinese messenger was to obtain a military alliance between Yuezhi and Han in the wars between the Chinese kingdoms of the time (Han against Xiong Nu). After his return to China in 126, Zhang Qian continued to organize missions to the small kingdoms in western China: Saka, Daxia, Yuezhi and Greco-Indians. From this remote period date the first Sino-Greco-Balkan contacts. Less than two centuries later another romanized Greco-Macedonian, Maes Titianos, came into contact with China. Leaving from Antioch in Roman Syria, with his caravan he crossed the Euphrates continuing to Bactria. From there, he crossed the Tien Chan at the Stone Tower and reached Chinese Turkestan and then arrived in Chiang An, the capital of the Han. His journey lasted a year, twelve centuries before Marco Polo! The Romans and the Byzantines did not cross militarily the border which separated them from the Persians and did not seek to push their conquests to the borders of China as had done Alexander and the Hellenistic Greeks, hence this very long break in relations.

### **Quarrels over trivial issues in the communist world**

When the Maoist criticism of “Khrushchev revisionism” met the mosaic of Balkan-communism, Beijing was able to set foot at the junction of the Adriatic and Ionian seas.

By a twist of history, in 1961 Communist China opened its first branch in Europe, in the Albania of dictator Enver Hoxha, by attracting the interest of the small Marxist-Leninist groups of Western Europe in a Sino-Balkan folklore blinded by a repression worthy of Stalin in the 1930s which had hit the land of the Eagles since 1945.

But the affair is deeper and older than the Moscow-Beijing split of 1961. It dates back to the end of World War II. Stalin, the champion of communism in one country, in the face of the Trotskyist utopia, understood that his victory over Nazi Germany

opened up a vaster prospect for him: communism in a single bloc led by Moscow. This Stalinist imperialism came up against national communisms which had been the spearhead of resistance (China-Yugoslavia-Greece), followers of national and social liberation. Stalin's dictatorship was initially rejected by Tito. All the communist parties and especially those that were members of the brand new "Eastern bloc" were asked to denounce the heretic from the summer of 1948. The Albanian CP (Communist Party) was the best student in the class for certain regional reasons that we will discuss below. Mao was the second because, as a fine tactician, he still needed Soviet military aid to win his civil war. But the Chinese thought no less. The Greek Communists were reluctant because their civil war only held thanks to Tito's help. In October 1949, the Chinese Red Army entered Beijing, while two months earlier the last defeated Greek partisans crossed the Yugoslav and Albanian borders. The "Greek lesson" confirmed that the Chinese leaders were right with respect to their mistrust of Moscow's hegemonism.

In order to retain his power, Mao used the ideological map to break up with Moscow. The Soviets would have become "revisionists" by breaking the Leninist-Stalinist regime. Albania immediately followed in the footsteps of the Chinese. In March 1961, Enver Hoxha did not take part in the Warsaw Pact meeting and during the 22nd Congress of the CPSU in October, Khrushchev condemned Albania. A month later, the diplomatic and economic relations between Tirana, the USSR and the People's Democracies were broken. Why did Enver Hoxha take a stand for China against the USSR? The case dates back to 1943-44. He founded the Albanian Communist Party in 1941 and became part of the resistance. But his supporters could only survive with the help of Tito's men. After the liberation of Albania, Hoxha was the minority within a largely pro-Yugoslav Communist Party of Albania. The autocratic apprentice, fearing to lose power, used the Tito-Stalin break to destroy his opponents (3). He then developed a new unwritten theory: "the farther my allies are in geographical terms, the closer they are to me". This is how he got rid of the Yugoslav tutelage and went under the wing of Stalin, forgetting that the latter had suggested to Tito that he could "swallow" Albania in his idea of creating a narrow Balkan federation, without Bulgaria. As Enver was a pragmatic nationalist rather than an ideologist, he cast an evil eye on the Yugo-Soviet rapprochement of 1955. He then thought that Khrushchev could replay "the swallow" in favour of Tito. He therefore transferred to the Chinese camp in 1961, especially since at the Non-Aligned conference which took place in Belgrade on 1 December 1961, the differences between Beijing and Belgrade became evident. The Soviet submarines then left the naval base of Sazan off the port of Vlora and several Chinese soldiers settled there, monitoring the passage of merchant ships leaving the Adriatic! But above all, Beijing sent economic aid (trucks, tractors, etc.) and built a gigantic steel complex in a deep valley behind Elbasan. In the height of the Enverist delirium, the Albanian workers, like "their Chinese comrades", were obliged to do half an hour of Chinese gymnastics every morning before entering the workshops!

After the death of the "Grand Helmsman", Mao Zedong, Hoxha relived the

horrors of the death of the “Little father of peoples”. On 6 October, 1976, the “gang of Four” was arrested. On 21 July, 1977, the “reformer” Deng Xiaoping returned to power and thus Tito was invited to China with pomp from 31 August to 8 September. On 9 March 1978, a strong delegation from the Chinese Communist Party was received in Belgrade. Tirana broke its ties with Beijing accusing the new Chinese leadership of “revisionism”. History stuttered. Having no more Yugoslav, Soviet or Chinese aid, Albania sank into suicidal isolation leading the post-Enverist authorities to make deals with the Italian mafias. In short, the return of China to the Balkans is therefore Tito’s unintentional work.

### **The Greek Trojan Horse**

Beijing left Albania in 1977, but returned discreetly to Athens in 2004. The choice of Greece in general and the port of Piraeus in particular is purely geo-strategic. In the future establishment of the land Silk Road and the maritime “Pearl Necklace”, Piraeus is the centerpiece. Beijing decided to rely on relay ports starting from Dalian on the Korean border, to the Mediterranean. The Greek port enjoys space, deep water and is protected by the Saronikos Gulf. It is in the middle of the Mediterranean almost equidistant from the markets of Western Europe, Central and Eastern Europe, the Turkish Straits and the Middle East.

The Chinese established contact with the Greeks at the end of 2004. Indeed, after the attacks of 11 September, the Olympic Games had to be absolutely secured. The 2004 Athens Olympic Games made the country suffer the negative consequences and Greek taxpayers paid the price which went from 4.5 billion dollars to 9, following the demands of the Americans channelled through the IOC. The Chinese wanted to make their Olympic Games a shining showcase of their new power, and they therefore turned to the Greek specialists who offered them their know-how in the computerization of control and security systems. The bilateral relations were on the move. From 2005-2006, Greece offered mooring facilities to all ships transporting Chinese goods in Souda Bay in the north-west of Crete. Beijing wanted to appropriate the port of Souda as it did in 2008 with Piraeus. But Washington reminded them that Souda Port is home to a major US-NATO naval military base! At the same time, the powerful Greek ship-owners built 415 tankers and cargo ships for the Chinese arsenals. They had the world’s largest fleet with more than 3,000 Greek-flagged or convenience-flag vessels, and China needed its endless stream of goods transported. In exchange, Beijing tripled its imports of Greek olive oil. It was in 2006 that the annual Greek-Chinese inter-ministerial meetings were formalized.

The agreement took place on 24-26 November, 2008 with the state visit of President Hu Jintao. The Greek Conservative Prime Minister Kostaki Karamanlis, the nephew of the great Karamanlis announced that he had just bought the management of part of the port of Piraeus: the container terminal 1 where 1.6 million tonnes transit

per year. It was the Chinese public company Cosco Pacific Ltd that won the deal for 4.3 billion Euros. It will manage this terminal for thirty-five years and is committed to modernizing and expanding the port within six years to handle 3.7 million tonnes, increasing the port's capacities by 250% (4). This is the effect to be achieved. Cosco acquired 51% of the shares of the PPA (Piraeus Port Authority) with an approval by voting of the Vouli (the Hellenic Parliament) in early 2009. On 16 May, 2013, the last Greek Conservative Prime Minister, Andonis Samaras, was received with pomp in Beijing. He obtained the promise for a Chinese investment of 8 billion Euros as his country was sinking into its biggest economic crisis since World War II. Cosco undertook to build a fourth trans-shipment dock for the sum of 230 million Euros. The Chinese giant could afford it as its profits in Piraeus had already tripled. On 14 December, 2015 and then on 20 January, 2016, Piraeus 1 and 2 became Chinese property, holding 67% of the capital of the PPA. This time with government support of the radical left of Syriza! In 2017, Cosco achieved its objectives of 3.7 million tonnes and in 2019 the port was planned to become the second in the Mediterranean.

The takeover of Piraeus was not without social damage. As early as 2012, Cosco, with the approval of the Greek authorities in the PPA Board of Directors, closed their archives. Today, the Association of Greek Historians, with Ménélaos Charalambidis, is increasing its protests requesting that they be reopened, currently without success.

The docks of Piraeus were for a long time a trade union stronghold, held by archaeo-Marxists and a handful of anarcho-syndicalists (5) until the beginning of the 1930s. Then it was the communist militants of the Communist Part of Greece who controlled the dockers' union and that of "Seafarers" (sailors, officers, merchant navy and ferry crew). In 1946, the civil war resumed in Greece and the country became one of the theaters of confrontations leading up to the Cold War. The first mission of the very young CIA was to take over the ports of Piraeus, Genoa and Marseille from the hands of the local Communists. Especially since in the summer of 1947 it was through Piraeus that massive American military aid landed for the royal Greek army that was in a difficult situation facing the supporters of the Democratic Army of Greece. In 1949-1950, the communists were driven from the docks and from the management of the single central trade union, the GCGW (General Confederation of Greek Workers). However, the dockworkers' union, founded in 1925, today affiliated with the IDC (International Dockworkers Council), remained the bastion of the workers' demands, although today it no longer has an organic link with the Communist Party of Greece via the current PAME (All- Workers Militant Front) within the GCGW. From 2013, Cosco took action again in the same way as the CIA, but with gentleness and cunning. Giorgos Gogos, the current Secretary General of the Piraeus Dockers Union, explained: "Our union is the one that has suffered the most. Cosco cannot attack head-on our wages, our pensions and our bargaining rights because they are protected by the Greek constitution. But our problem is the Greek service providers / subcontractors and the in-house union created by the Chinese"(6). If Cosco could not ban free unions like in

China, they tried to bypass them. The dockers - all union members - leaving to retire were no longer replaced by the PPA employment office, but by subcontractors. With the expansion of the port, they hired 1,600 workers, but with new contracts at lower wages. Moreover, the new arrivals had little experience and were poorly trained, resulting in degraded security conditions in a dangerous profession. But the Chinese authorities did not know the “Safety and Health Committees” which govern part of the labor laws in the EU countries! Cosco also took care to create its own yellow union, the Sinedep, to supervise and control the new hires who were not choosy given the state of disrepair of the Greek labor market. The house “unionists” had just signed the new Collective Agreement for Dockers (February 2019), which was much less advantageous than the previous one. Gogos and his activists refused to sign. Finally, the Chinese downsized more than half of the PPA administration personnel. It should be noted that if the dockers’ wages had decreased, it was also due to the fact that the Syriza government applied measures imposed by the Troika Memorandum (IMF-ECB-EU Commission) aimed at general decline in the salaries of civil servants and state employees. The GCGW as a whole could not oppose this ultra-liberal austerity policy, despite the promises of Prime Minister Tsipras and the three elections won by Syriza. Cosco thus appropriately slipped into this breach always thinking bigger. To make room for Cosco in Piraeus, the Greek authorities were considering to move the docks reserved for passenger ferries (Crete and Cyclades) and on 27 March, the Minister of the Merchant Marine Fotis Kouvélis rather enigmatically stated: “There are no ideological barriers to Cosco’s investment in Piraeus, as long as it respects the environmental standards . As for social standards, Kouvélis does not hamper ideology himself! But the man is a former communist of variable geometry (7).

If Piraeus is China’s trump card in Greece, it is no longer the only one. Tourism, energy, metallurgy and telecommunications are in sight as well.

On 15 May, 2017, young Prime Minister Alexis Tsipras was received as the new emperor of Byzantium with a pomp that the Chinese know so well how to orchestrate! The man who never wears a tie, who flaunts his atheism in a country where the separation of the church and the state is still not fully effective, was more than touched. Especially since it differed so much from his visits to the Headquarters of the Commission in Brussels to negotiate the debt of his country. The German delegation did not deign to shake his hand and even the bourgeoisie of Calais were better treated by the English. The Troika thus showed the Greek people that they had to debase themselves (8). A humiliation hard felt by Tsipras and the Greek people.

On 30 September, 2017, the first direct Athens-Beijing flight was inaugurated. Two months later, China signed four cooperation agreements: two in the areas of green energy (with the Chinese coal giant Shenhuan) and metallurgy with the private groups Kopelouzou and Mytilinaios and two others with the state-owned electricity production and distribution enterprises (DEI and ADMHE). Finally, the phone giant, Huawei, will install 5G in Greece in 2020. It already has a subsidiary in Athens employing 120

people and made 200 million profit in 2018. The 5G pilot site is already in operation in Kalamata (9). In short, a solid starting point for conquering the whole of the Balkans.

### **The rest of the Balkans**

For the other Balkan countries, the Chinese strategy is almost the same. The maritime Pearl Necklace is less important and concerns only the port of Durrës in Albania and Rijeka in Croatia. It is the Silk Road which takes precedence, therefore the land routes: highways and fast railways. There is also electricity, mining, tourism, agriculture, nuclear power, household appliances ...

If the annual meetings with Greece began in 2006, those with the CEEC (16 + 1) began in Budapest in December 2012, in Belgrade in December 2014... And all Balkan leaders have always been welcomed in Beijing with pomp, except the Macedonians. The latter, seeing their independence not fully recognized because of a veto from Greece on a name dispute, had made the mistake of recognizing Taiwan in 1998. Three years later they backed down.

The oldest relations were sealed with Milosévić's Serbia, relations which were only the heirs of the good relations forged between Deng and Tito. Moreover, Belgrade and Beijing collaborated militarily. When the NATO bombings started on Kosovo and Serbia, on the night of May 7 to 8, 1999, one or two American stealth planes dropped three bombs on the Chinese Embassy. The entry impact was less than one meter in diameter. However, at the exit point the whole wall collapsed and everything in the middle was vitrified under intense heat. President Clinton apologized, saying his pilots only had old maps of Belgrade and they were targeting a building of the Serbian Ministry of Defense! The Chinese Embassy is the only pagoda-shaped building in the Serbian capital. In addition, it was built on a vacant lot where at the time there were no other houses more than 200 meters around. For some time, however, senior Chinese People's Army officers had resided in the Embassy, in particular artillerymen specializing in the latest generation of land-to-air missiles (10).

This 1999 war was aimed at the withdrawal of Milosévić's troops from Kosovo and hence ultimately enable the independence of this small territory. Beijing never wanted to recognize this independence which could set a precedent in the case of Taiwan and Tibet and the right of minorities to self-determination. This is how Beijing opened its Confucius Institute in Belgrade in 2006 and a branch in Novi Sad in 2013. In 2014, the Chinese built a new bridge over the Danube in Belgrade. The NATO bombings had seriously damaged the bridges over the Danube! Xi Jiping was also received in Belgrade on 14 June, 2016 with all the honors appropriate to his rank.

The two major rail projects of the Balkan Silk Road are the Bulgarian Black Sea-Budapest and Budapest-Adriatic Rijeka fast connections. In 2017, Beijing granted Belgrade a billion dollar loan to build the fast line to Budapest and took the opportunity to buy the management and expansion of Tirana airport (October 2016).



In their conquest of European household appliances, the Chinese have taken over the Slovenian company Gorenje. The latter, the flagship of the Tito economy, was founded in 1950 and was the only Yugoslav company to export in 1961. In 1997, it was transformed into a joint-stock company majority owned by the new Slovenian state. With its subsidiaries in 33 countries, it achieved 2017 sales of 1.3 billion Euros. China's number one television set and world number three, Hisense, took an interest in this flagship business and acquired 33% of the shares. Then in June 2018, for 293 million Euros, it bought 95% of the capital.

From being non-existent ten years ago in the region, China is now the third largest trading partner in Bosnia and Herzegovina and Montenegro and the fourth in Serbia. Each year it gains market shares. It benefits from the reluctance of EU investors, the poor image that the European institutions hold in terms of these countries and what is perceived by many of these countries as an abandonment, even betrayal of the Slavic-Orthodox Russian big brother. When Cypriot and Greek banks called on Moscow to help in 2013-2014, Putin did not move a finger. Sofia, Belgrade, Podgorica, even Skopje are therefore ready to open their arms wide to Beijing and regardless of the social breakdown, especially as the independent unions (Podkrepa, Nezavisnost...) born in the euphoria of the fall of the dictatorships could not capitalize the discontent of the now disillusioned, resigned and fatalistic workers, preferring for the youngest and the most dynamic "to vote with their feet" and to leave the Balkans as was already the case in the period between the two wars and the 1950s.

### REFERENCES:

The Troika imposed three memorandums on Greece that were in force until August 2018 with the following obligations: decrease in the number of civil servants, cuts in salaries and pensions in the civil service, increase in VAT, privatizations at all costs, end of collective agreements ... , in return the country could receive loans to repay its debt. Loans at almost usurious rates that have allowed private and public banks (ECB) to pocket billions.

Michel Bruneau: *L'Eurasie. Continent, empire, idéologie ou projet*, Paris, CNRS éditions, 2018, 352 p.

In order to found the PCA in the fall of 1941, Enver Hoxha brought together the various Marxist groups in the country. Not all of these groups were Stalinists. The Trotskyists and archaeo-Marxists, often belonging to the Greek minority, were killed the same evening. In June 1949, he had Koçi Xoxhe, number 2 of the regime and a man of Tito, shot. In December 1981, he did the same with Mehmet Shehu, his historic right-hand man.

*Images économique du monde*, 2017, 2018, 2019; ed. Colin.

The Archaeo-Marxists, or "Archives of Marxism" of the KOMLEA party were part of the International Left Opposition; they joined Trotsky and then separated from him in the early 1930s, denouncing his sectarianism. They were more powerful than the Greek CP (KKE) until 1934. They were well established in many unions (dockers, sailors, bakers and shoemakers). The anarcho-syndicalists were always weak, established only in Piraeus and in the region of Patras among the wine growers.

Interview with the author, 3 April 2019.

Fotis Kouvélis was born on 3 September, 1948 in Volos, a law and political science student in Athens, he was a member of the Lambrakis Youths led by Mikis Théodorakis on the eve of the colonels' coup of 21 April, 1967. Founding member of the CP of the interior in 1968 (split from the KKE), member of its Central Committee from 1975 to 1987. When the party was transformed into Synaspismos, he took over its General Secretariat from 1989 to 1992. He was the ephemeral justice minister in the Conservative-Communist coalition government in 1989. When Synaspismos turned into Syriza, he left with the right wing and founded the DIMAR (Democratic Left) which participated in the last coalition government (the conservatives of New Democracy, the socialists of PASOK and the right-wing communists of DIMAR). Being deprecated, DIMAR joined the debris of PASOK to create the KINAL (Movement for Change). Being an opportunist, Kouvélis returned and joined Syriza. He was rewarded in February 2018 by becoming Secretary of State for Defense, then Minister of the Merchant Navy.

In the demonstrations against the Troika and the austerity measures, there were banners with crossed portraits of Merkel and Hitler and the most used slogan was “no to the second occupation”, an allusion to the terrible German occupation from April 1941 to October 1944 which caused nearly 300,000 deaths. In% of the population, Greece, together with Yugoslavia was the most affected country, even ahead of the USSR and Poland. It should be noted that Germany still owes 80 billion Euros in war reparations to Greece, a sum which would have partly paid off the Greek debts.

See the daily bulletins of Athinaïko Praktorio, the paragraphs “Ikonomia”.

Christophe Chiclet, Bernard Ravenel, Kosovo: *Le piège*, Paris, L'Harmattan, 2000, 288 p.



## INTRODUCTION OF THE EU-CHINA RELATIONS: HISTORICAL OVERVIEW OF STRATEGIC PARTNERSHIP

**Toni MILESKI<sup>1</sup>**

**Eike ALBRECHT<sup>2</sup>**

**Abstract:** *The history of relations between the European Union and China represents an endless source of diverse analytic approaches and possibilities of creating appropriate evaluations and projections based on historical and actual happenings that concerns both analyzed subjects. Various literature depending on the sources and affiliation of the authors points out to the different approach in the analysis of the historical retrospective of the relations between the European Union and China which covers different scientific fields from politics, geopolitics, geostrategic to possibly the most important economic premises on their continuous process of cooperation. The main thesis in the whole research efforts divided in two papers is related with the question could EU and China be strategic partners and contribute in the creation of a constructive world order?*

*The research in this paper is done based on the overall available literature which the authors could gather. Initially, accessing to the open Internet resources and as well as the official websites of the European Union and China. Consequently, sources of official media portals and analytical centers were used in the research. The entire material is analyzed with an appropriate methodological framework whereupon the obtained results represent an original scientific effort.*

**Keywords:** *International relations, European Union, China, geopolitics, geo-economics, partnership.*

### Introduction

The historical context of the relations between the European Union and China dates way back than the framed analytical period set as the title of this research. That means that a period before 1976, when the diplomatic relations between the European countries and China were officially established, will be also covered. Respectively, the history of relations between the Europeans and Chinese can be traced way back at least to the beginning of the Christian era. The value of goods transferred through the famous “Silk Road” which included sea routes through the Middle East and India, have brought the silk and luxury into Rome. In that period

---

<sup>1</sup> Full Professor at the University of Ss. Cyril and Methodius – Skopje. Faculty of Philosophy – Department of Security, Defence and Peace.

<sup>2</sup> Full Professor at Brandenburg University of Technology Cottbus-Senftenberg, Germany. Faculty 5 - Business, Law and Social Sciences, Department for Public Law, in particular Environmental and Planning Law.

there were little comparative values and goods that Rome could offer to China. These conditions were maintained throughout the major part of the eighteenth century, respectively until the emergence of opium as goods which was offered in China. Nevertheless, the main characteristic of the early trade between European countries and China is that it took place with the help of mediators from Central and South Asia, respectively there was no direct relation between the Europeans and the Chinese in that period.

Two main factors that have continued to model the relations between Europeans and the Chinese to the present day can be perceived to have existed from the beginning. The first factor was the so-called “Tyranny of distance”, which is partially overcome by the modern technology and transport. Until the beginning of the First Opium War or the First Anglo-Chinese war from 1839, neither China nor Europe inflicted geopolitical concerns to one another. The second factor is the primacy of trade as the main content of formation of their relations. (Perdue, P, 2020).

Direct relations between the European countries and China have not started until 1514, when the Portuguese arrived in China through Malacca. But, it is good to know that a certain period before the event the European civilization and the development have been significantly influenced by the transferred findings and discoveries that were firstly made in China. It is interesting that the origin of these findings was unknown until 1620, when the English philosopher Francis Bacon identified three findings: printing, gunpowder and magnet. These three findings have changed the face and the situations within the framework of the whole world. The printing made the change in the field of literature, the gunpowder in the field of war and the magnet in the domain of navigation. Naturally, these findings have enabled the feisty, commercially strong and industrialized European countries to reach China in the nineteenth century and to bring it to the modern age through the armed forces.

As the Europeans in one moment were pulling out of China, weakened by the two World Wars, they paid less and less attention to China. The foundation of the People’s Republic of China in 1949 introduces a new era of politics and economy of the Chinese-European relations on which the consequences of the Cold War influentially acted. Ironically, however the ideological and organizational principles that retained the rise of Communism in China and the image of the new Chinese national identity have European origin, however such conditions did not occupy a significant part in their newly established relations. Despite the indications of certain differences in the policy toward China compared with those of the USA, the policies of the Western European countries were a product and created on the basis of their dependence from the United States in that period of the bipolar world order. Likewise, the Eastern European countries founded and created their relations with China based on their relation with the former Soviet Union. With the end of the Cold War and the changes that featured in China and Europe, both sides had the opportunity to establish more interdependent relations.

This article is a product of a broader and more complex research which is separated in two interdependent parts. The first part, published in this volume of Contemporary Macedonian Defence, is the historical overview of the strategic partnership and refers to the history of relations between the EU and China, their beginnings of establishing relations. All that period was rich with lots of misunderstandings rarely enveloped with political issues and embargoes. While the second part is focused on strategic cooperation, through various forms of partnerships and established cooperation mechanisms up to date. That means a complex analysis of the contemporary Chinese mechanisms of cooperation with the EU like the ‘Belt and Road’ Initiatives and ‘17+1’ mechanisms of cooperation with Central and Eastern European countries.

Whole research, particularly is focused on understandings of the state of relations in the modern era of a globalized world and tries to answer if it is possible for the two main subjects, the EU and China, to create cooperative relations for constructive world order or become, as recently noted by the European Commission, dominantly 'systemic rivals'.

### **Cold War Context of EU-China Relations: 1949-1989**

Relations between Europe and China during the Cold War were created from the current actual problems and the attitude of each party with the United States of America and the Soviet Union. That does not mean that the Europeans and Chinese were not trying to build specific relations in certain periods, but in the end it meant that those moves were coordinated or were derived from their relations with both superpowers. The most obvious way of that is how the 'Iron Curtain' divided the relations between Eastern European countries and China from those relations of the Western Europeans. Respectively, the relations of Eastern European countries with China were completely determined by their relations with the Soviet Union. Although in those frames there was also a difference among those who distanced themselves from the Soviet Union – Yugoslavia, Albania and Romania and those who were subordinated to the Soviet Union. Western European countries have enjoyed bigger freedom within their alliance, although relations of NATO's countries with China generally followed the model of relations established by the United States. These relations were relatively on a low level until the approximation of China and United States in 1971. Then, following the United States, Europe endeavored to build relations with which it will impose anti-Soviet positions to China even at a price of appeasement. However, with these broadly based foundations for relations building with China, at various times China tried to commit to the Europeans, firstly in order to bypass the American embargo as a reaction to the Chinese support of North Korea in the Korean War (Andrew J. Nathan and Robert S. Ross, 1997) and then to gain access to the European technologies (both military and civilian) during the seventies and eighties of the twentieth century.

After the Second World War and the creation of the People's Republic of China several European countries among which Denmark, Sweden, Switzerland, Norway, Great Britain and Netherlands recognized the new government, while the United States continued to recognize the Republic of China-Taiwan. Britain primarily had economic interests in China, hoping to protect and maintain its colony Hong Kong. British diplomats claimed that the recognition of the People's Republic of China will put the West in a better position so it could be able to use all the differences that could occur between the Soviet Union and China because their national interests were not identical. British diplomats have also pointed out that the American policy on recognition of China was too ideological. The outbreak of the Korean War consolidated the cold war division in East Asia and stopped all the attempts of Europeans to develop new approaches toward China at that time. However, the Korean War did not make a great

damage in the relations between Europe and China, not that much as it was the case for the relations between China and the United States. The Geneva Conference from 1954 was convened to resolve the situations in Korea, but it is more remembered by the agreements concerning Indo-China. These agreements were reached through diplomatic efforts of China, Britain and France and they have not had a really major support from the American side. This conference will represent an event on which for the last time the Europeans had the decisive role in the formation of the strategic issues related to China. Western Europe had different positions on the trade issue from 1952 onwards. Then they started trading with China in contradiction of the American trade embargo. However, the Western Europeans were with the USA regarding the most key issues in their relations with China. On the other hand, Eastern Europeans developed different relations with China, primarily because of their affiliation in the socialistic block, but practically because of their relations with the Soviet Union. China was building close relations with them for the benefit of industrial technology which they transferred to China. Yugoslavia was an exception from which China had distanced itself at first because of the Stalin's stigmatization due to their disobedience and then in 1960s with their efforts for revisionism. As the relations with the Eastern Europeans have completely worsened in line with the deterioration of relations with the Soviet Union, Albania and Romania were accepted by China because of the resistance to the Soviet domination.

The Chinese-American cohesion in 1971 brought the two countries on the same line against the Soviet Union. Those events also led to a change in the relations between the Western Europeans and China. China was very interested in military exchange with Western Europe, but despite the great interest in buying advanced weapons very little of it was realized, perhaps mostly because of the inadequacy of technology. For example, a factory for the production of plane engines was paid around 200 million pounds, after which the Chinese had a plane engine, but did not have a proper construction of the plane. The first step in the early 70s of the last century was the establishment of full diplomatic relations with the Western European countries with which until then this had not been done. Then, a period of rapid increase in trade exchange comes between 1971 and 1975.

The People's Republic of China and the European Community establish official diplomatic relations in 1975 in one extremely meaningful historical moment for both parties. Namely, Beijing enters in the anti-Soviet partnership with Washington in 1971-1972. The six members of the European Communities at that time Germany, France, Italy, Netherlands, Belgium and Luxembourg activated the process of European political cooperation as a harbinger for the future Common Foreign and Security Policy in 1970. In 1973 the European Community expanded with Denmark, Ireland and United Kingdom. In 1974 the heads of state and governments of the member states of the European Community agreed to meet in the future as the European Council which represented the executive body for dealing with very important issues and for

establishment of an agenda of the whole European integration process. Moreover, the European Commission was authorized to improve the new areas of cooperation such as the common trade policies. In this context were the established diplomatic relations between the European Community and China in September 1975 in recognition of the future joint international potential.

With the activation of the “Four modernizations” in 1975 by, at that time, Prime Minister of China Zhou Enlai, the European policy makers had hoped that, slowly but surely, the world’s largest market was potentially opening. Despite the expectations that derived from the new trade potential of China, the Western European interest in the development of the relations with China were based on a legitimate ground that the Chinese economic reforms could also cause changes in the political domain.

By July 1977, Deng Xiaoping regained his position as the Vice President of the Chinese Communist Party. The following year, the Third Plenary Session of the Eleventh Central Committee confirmed the victory of the pragmatic line of Deng. As a result of these events, Beijing engaged into an active policy of improvement of the relations with all countries outside the Soviet sphere of influence, established full relations with the USA and tried to win Japan on the greater anti-Soviet line. In that context, the Chinese leaders will start to look at the Western Europe through the prism of national security on Beijing. Following that, China will become supporter of NATO with a purpose to reduce the Soviet pressure from the tense Chinese-Soviet border. From the middle of the 70s of the last century, the Chinese authorities will encourage the European policy creators to spend more on defence in one open anti-Soviet movement. That allowed them to gain access to the European defence subscribers and the bases on the Northern Atlantic Alliance. At that time Beijing purchases anti-aircraft and anti-tank missiles from Italy and Western Germany, radars from France and fighter jets from Great Britain. This was allowed as a result of the re-established diplomatic relations between the USA and China. Washington accepted for their Western European partners to sell certain weapons to China, which the USA because of their domestic constraints were not able to sell. These moves drove the Assembly of Western European Union to review the occurred security problems in the European-Chinese relations. In May 1978, the Assembly of the WEU proposed a resolution draft in which they recommend a careful research of the role that China could play, which is connected with the European security including the observations of increased Chinese claims for industrial technology. These moves indicate that from the very beginning, the security and strategic considerations had their role in Chinese-European relations.

The further development of relations between Western Europe and China crosses into a further advanced stage. In 1979, influenced by France and Germany, the European Monetary Fund as a first step towards Monetary Union, was designed. In 1981 Greece joined the European Communities followed by Spain and Portugal in 1986. Thus, the total number of members in the European Communities peaked at twelve. In the early 80s, the future initiatives for increased political cooperation reached a culmination in



1986, when members of the European Community signed the Single European Act. (Casarini, N. 2009: 25-30).

It is obvious that the context of the development of relations between the European Community and China was changing, especially in the 80s from the twentieth century. This attitude primarily arises due to transformation of China through series of political and economic reforms and their openness which was associated with the establishment of diplomatic relations between China and the USA, and secondly due to the softening of the hostility between China and the Soviet Union. Europeans began to observe China not only as a potentially big market, but also as a place where with the help of their experience they could be useful for China in their endeavour for major reforms and renewal. On the other hand, the Chinese began to observe the Western Europeans as partners for trade and relations development which would be suitable for both parties and which would be freed from strategic complications because of their relations with Japan and the USA. In 1985 the relations were improved to the extent that the European Economic Community and China were ready to sign their first agreement. That agreement was primarily focused on trade facilitation, but it also had a great significance in strengthening their future relations.

Relations with the countries of Eastern Europe have also changed significantly in parallel with the interest of China for the experiences of their reform steps of communism. After all, the organization of the Chinese economy and its national enterprises were much more similar to those of Eastern Europe than the ones of Western Europe. Perhaps for the same reason China's leaders were less enamoured with some of the political changes taking place. Firstly, in Poland in the early 1980s with the emergence of an independent trade union determined to introduce more democracy, and secondly, with the emergence of Gorbachev in the Soviet Union in 1985 which caused a certain dose of concern in China. The Chinese were happy that the participation of the Soviet Union in Vietnam and Afghanistan was brought to an end, which meant a reduction of troops in the North of China, but the Soviet political reforms were observed as a potential challenge for their style of governance.

Close relations with the Europeans were suddenly interrupted by the Tiananmen massacre from 4th of June 1989. The shock and disbelief for that event caused Europe to impose sanctions towards China through the European Council. Concretely, on the European Community Summit held in Madrid on 26th and 27th of June in 1989, the European leaders agreed to impose punitive economic sanctions individually and within the frames of European Community, to suspend all military contacts and arms sales, to cancel all ministerial and official visits to China, to freeze all state-guaranteed loans and to issue a strict condemnation because of the conducted massacre. The events of Tiananmen Square caused particular problems for the French and British authorities. France gave refuge and political asylum to many Chinese students and intellectuals involved in the pro-democracy movement which caused pressure on French-Chinese relations. The British government was in a very complicated position since London

and Beijing were involved in sensitive negotiations over the legal norms for returning of the colonial Hong Kong possession to the Chinese sovereignty. Regardless of these events, on 4th of July 1989, the European Community clarified its intentions for renewal of political contacts with China. On 28th September 1989, Italian Minister of Foreign Affairs Gianni De Michelis met with his Chinese colleague Qian Qichen on the margins of the General Assembly of the United Nations and discussed about the possibilities for the resumption of political contacts and the strengthening of connections between the European Community and China. Furthermore, the Italian government began lobbying among other member states of the European Union for relaxation of sanctions on China. These conciliatory tones and attitudes were in the direction of the continuation of cooperation with China in the hope that the political changes in Beijing will speed up. On 22th October 1989, the Ministers of Foreign Affairs of the European Community decided to gradually renew the economic cooperation and contacts on high level with China. Arms sales and military contacts still remained frozen. By the summer of 1990, most of the European sanctions were abolished, except the military embargo. As a result, China become less vocal in the condemnation of Europe than of America, although China accused Europe for the economic sanctions that caused a major reduction of the two-way trade. (Casarini, N. 2009: 30-31).

At a global level, later on, the communist governments collapsed as the Cold War came to an end. The European expectations were that the Chinese Communist government would soon follow that example. These expectations were strengthened when it came to the disintegration of the Soviet Union in 1991. The Chinese leaders were also shocked by all previous events and took a stand that a part of the reasons for such development of events was the thing that they called Western politics of a “peaceful revolution”. (Ong, R. 2007). That represented a long-term attempt of the West to undermine the communist system with peaceful means.

### **Post-cold War Aspects of the EU-China Relations: 1990-Today**

The end of the Cold War brought the completion of the bipolar structure of international politics that shaped and restricted the relations character among the Chinese and the Europeans in the previous four decades. In the last period of the eighties of the last century, with the Chinese policy of economic reforms and opening towards the external world began the change on the basis of Chinese relations with the capitalist world. However, the real end of the Cold War brought fundamental changes in the world of politics and the economy, whereby new opportunities for China and Europe have opened to deepen and expand their relations in conditions where both sides will slightly depend on third parties. The immediate interest of both sides came under conditions that we can call “domestic effect” from the period of the Cold War with the endeavour of each side to be better positioned so as to be able to successfully deal with the other side. As the Chinese leaders renewed the firm control over its territory and started to

improve their relations with their immediate neighbours, the tour of Deng Xiaoping called "Southern tour" in 1992 contributed even more to the accelerated economic growth based on economic reforms and the Chinese opening. Europeans from their side began strengthening some of the political dimensions of their Union which until then were in the shadow of the economic and trade dimensions. The European Community made progress in the development of its own positions in the field of foreign policy especially in the end of the eighties of the last century, but the end of the cold war division in Europe, the reunion of the two Germanys and the announcement of the post-communist governments in the former Eastern Europe enabled a new momentum that came to a Treaty an expression in the Maastricht Treaty in 1992 which gave an institutional form to the Common Foreign and Security Policy (CFSP) of what is now call the European Union.

China adapted quickly to the situations caused by the end of the Cold War in Europe and began to renew its relations with post-communistic countries of Eastern Europe. Although the main purpose of Beijing was to prevent Taipei from creating diplomatic connections with New Europe, the Chinese rapid acceptance of the new reality enabled eased and improved relations with the European Union after which the events from Tiananmen began to fade. Anyway, trade relations have not been interrupted and the European leaders began to appear on the Tiananmen Square, especially the British Prime Minister, whose visit was of vital importance for ensuring the questions connected with Hong Kong which should have been returned to China as it was arranged in 1984.

In March 1992, the Prime Minister of China Li Peng and the Minister of Foreign Affairs Qian Qichen visited Western Europe, whereby they visited Germany, and the European Commission in Brussels. In the speech of Qian Qichen held in the German Council for Foreign Relations, his views on relations between China and the European Union were presented. Firstly, he pointed out that both sides support the transition process of transfer from a bipolar towards multipolar system of international relations. Secondly, he stressed out that both sides promote peaceful and stable international surroundings and the trend for resolution of global problems dominantly through consultations rather than by use of force. Thirdly, China and Europe have acknowledged the leading role of the United Nations in conflict resolution. Lastly, as fourth, it was stressed out that both sides are highly complementary in the economic sense. (Mackerras, C. 1998: 184).

As a response to the international influence of the rapidly growing Chinese economy and the emergence of East Asia as a new canter of international economy, the European Commission, as an executive body of the European Union, has published its first policy paper in 1993 on the Asian strategy which was basically directed towards China. Although this policy had been created on the initiative of Germany and France it expressed a common view of the entire European Union. China was determined as a distant country that offered new opportunities primarily for trade, but also as a place where the European Union can practice mostly the policies that incurred as a part of

the Common Foreign and Security Policy. In particular, the encouragement of good behaviour development, poverty reduction, training and assistance in management and technology transfer as well as promotion of democracy and development of civil society and other.

On 12th September 1994, Chinese president Jiang Zemin outlined four principles for relations development between China and Western Europe. They included: firstly, development of relations with a view towards the 21st century; secondly, common respect, a claim for common basis, reduction of differences; as third, common benefits and the fourth included resolution of all international problems through consultations and cooperation. It is interesting that these four principles were declared in Paris instead of Brussels. The purpose of this act was two-sided. As first, that event officially signalled warming of the Chinese-French relations after the arms sale to Taiwan in the beginning of the 90s, by France. As second, the act transferred the message that the individual relations with the member states of the European Union, especially with the bigger ones, were still important for Beijing. The relations with the bigger EU members, who are called "The Big Four", included Germany, France, United Kingdom and Italy. The development of these individual relations with major EU members played a significant role in the future development of relations between China and Europe. (Edmonds, R. 2002: 21).

In 1993, Germany became the first member state of the European Union which developed a strategy for Asia. In the "Asian concept of the federal government", the German government highlighted the importance of the Asian markets for Europe. This observation occurred after 1992, when for the first part, trade exchange between EU and Asia exceeded the one between the EU and the USA. The German concept implied that Germany and Europe in general will have to face the challenge of the economically advanced Asia and to strengthen the economic relations with the largest growing region in the whole world. As a result of the newly established circumstances, Germany and the whole EU, vouched for inclusion of the Asian countries in a way more constructive manner and established visits on the region on a high level. As the interest of Britain and France for Asia was known from before, because of their previous engagement, for Germany this was something new.

Parallel with the initiatives of individual EU member states, the European Commission published its communication towards the new Asian strategy in 1994 with main objectives of strengthening the economic presence of EU in Asia, contribution to regional stability, promotion of economic development, and consolidation of democracy and respect of human rights in Asia. In the frames of the new strategy for Asia, on 5th of July 1995, European Commission published its communication on a long-term policy for Chinese-European relations which brought the Chinese-European relations to a new era. In order to put the relations of the European Union member states with China in a so called "Single Integrated framework", the Commission announced that the relations with China should represent a foundation stone in the European foreign

relations both in Asia and in global frames. The starting point of the document of the European Commission was the rise of China, seen as unprecedented event since the end of the Second World War. While the analysis was concentrated on the Chinese economic rise and the potentials of its market for European businesses, the document established a strategy for a constructive engagement to integrate China in the international community. This new policy for China by the EU represented a part of a wider debate which had been already conducted in USA and Eastern Europe on how to deal with the growth of China in the post-cold war era. In 1994, the Trilateral Commission published the report for the growth of China in the world of interdependence which stipulated a policy of engagement of the advanced capitalistic countries towards integration of China into a world economy and benefit achievement from its enormous market. (Funabashi, Y. 1994). In the document, high-level representatives from the core capitalist countries of Western Europe, the United States, and Japan took stock of China's ascendancy in the world economy as well as the profound changes that had occurred in the international system after the fall of the Berlin Wall (1989) and the demise of the Soviet Union (1991). These new developments meant that relations among liberal-democratic states and the Chinese communist regime would now be much less constrained by Cold War dynamics than they had been in the previous era. The gathering process of globalization and the emergence of China and the European Union as new actors of regional and (increasingly) global significance would provide further motives for developing the relationship on a new basis and independent of previous superpowers' dynamics. The publication of EU's new China policy in 1995 marked, thus, the end of the period of Cold-War constraints and ushered in a policy of widespread engagement. (Casarini, N. 2009: 39).

As part of an entire past period of establishment of diplomatic relations, as we already mentioned, relations between the Europeans and the Chinese are taking place on the level of the European Union and on the level of individual countries. As in the previous periods, four main countries, France, Germany, Britain and Italy, represented key players in those relations. The successful return of Hong Kong from Britain to China in 1997, helped reduce the Chinese suspicion towards Britain and their sincere support for the Chinese growth as a main player in the world relations. The return of Macao from Portugal in 1999 represented the end of the remaining European imperialistic point in China. Since then, the European Union and China were able to institutionalize the easier and less problematic dimensions of their relations, which began in 2003 and which are commonly called "strategic partnership". (Garlick, J. 2013:54). But this was happening after China suddenly faced difficult negotiations with the European Union on the conditions for their entry into the World Trade Organization in 2001.

Still, several motivating factors were crucial for the European Union to establish a strategic partnership with China. Official representatives of the European Union hoped that the close engagement will catalyze the social and political changes in China and will provide greater democracy and opening and transparency of the country. In addi-

tion to the normative wishes for consolidation of democratic institutions and practices in China, the more opened, democratic and politically liberal China is also observed as a reliable partner for the European Union in resolving common problems. Democratic and politically liberal China also has smaller chances of becoming a destabilized and revisionist force. Geopolitical aspirations have also been a motivating factor for the representatives of the EU and China to demand an upgrade of their own relations. When the comprehensive strategic partnership was launched in 2003, the authorities in Brussels and Beijing were disturbed about how the USA used its own force in the world, especially in terms of their unilateral use of military power. Leaders in Europe and China believed that such bad practice of the American imperial arrogance should be retained. Romano Prodi, the President of the European Commission, at the time when a comprehensive strategic partnership among the EU and China was launched, called for a “new world order” for managing world’s relations (Beatty, A. 2003). The government officials and political analysts in China were looking at the EU as a possible counterbalance to the USA and as a significant element in the global system in which power and influence will be divided equally. At the end, Europe wanted to show its relevance on the world stage. The building of a strategic partnership with China will show that Europe could have an independent role in world politics. In that context, the former head of EU foreign policy, Javier Solana, called for a stronger Europe with a common strategic vision for capacity building for consolidation of the relations with the emerging powers, as China was. The former President of the European Commission, Jose Manuel Barroso, stated that the development of the strategic, mutually beneficial and lasting relations with China, are one of the top priorities of European foreign policy for the 21st century. Catherine Ashton, Solana’s successor on the position Head of European foreign policy, points out that it is necessary to improve the relations with China in order to stay a relevant factor in the promotion of its own interests on the global scene. (Maher, R. 2016: 960-962).

Parallel to these events, the Chinese government announced the so-called “White Book” for their relations with Europe, which is the first case of such matter related to a country or a region. In 2004, the value of the EU-China trade exceeded the Chinese trade with the USA and Japan, while China became the second most important trade partner for the EU, after the USA. As it was expected, certain outcries over trade appeared, which was actually a common feature between the main trade partners, but that still did not stop the progress in building their relations. Inevitably a question was imposed for abolition of the embargo on weapons, which brought certain limitations in the character of the new European-Chinese relations. Thereby, the two factors were extremely important. The first factor relates to the weakness of the EU as a coherent (interconnected) actor and the second relates to the differences between the Chinese and European approaches to the global role of the USA as the only superpower. The EU can have institutional mechanisms to function as a unitary actor in the negotiation of conditions for the international trade, but that does not apply when it comes to the

wider foreign and security policy. The growing economic relations with the EU were observed as part of the globalization process, but what China attempted for the EU to accept is its multipolar vision in which the EU will become a separate gender, independent from the USA. (Shambaugh, D. 2008: 127-147).

Before the EU-Chinese trade overcame the Chinese trade with the USA and Japan in 2004, on the 30<sup>th</sup> of October 2003, both parties concluded an all-inclusive strategic partnership. This upgrade of the already established strategic partnership was based on the idea that the relations between both parties should be intensified in the spirit of the new strategic meaning. The declaration of the new strategic partnership was accompanied by two sub-stanchioned moves. The signing of the political agreement, opened the doors for China, on the very same day, for participation in the common development of the Galileo system for satellite navigation, led by the European Union, which represents an alternative to the dominant American GPS. The second move was the promise of certain EU policy creators to their Chinese colleagues for initiating formal talks for lifting the arms embargo imposed on China after the events on the Tiananmen Square in 1989. Behind the rhetoric of the official statements, the strategic partnership in 2003 was directed towards a technical and political connection based on the cooperation in science and technology matters and on an attempt to exploit the business opportunities for both sides in the air and defence sector. The announcement of intensified cooperation with respect to the security and strategy policies attracted attention and concern from the USA and their Asian partners. The strategic partnership from 2003 gave an opportunity for some key members of the European Union, together with China, to challenge the American primacy in the key sectors, such as high-tech and security industry. The selected time also indicated the deeper dissatisfaction of European allies because of the unilateral actions of the USA in the framework of global relations. (Casarini, N. 2009: 80-99).

When it comes to the issue of abolition of the arms embargo for China, it is important to note that in September 2003, the European Commission produced the fourth political document for China, calling for complete cooperation in the sphere of political and security matters. The Chinese Ministry of Foreign Affairs, several weeks later, responded with a first political document for the European Union. In the document, there was a clearly set request for improvement of the relations in the military sphere and overcoming the arms embargo on China as soon as possible. France shared these views with Germany, under the leadership of Chancellor Schröder, and together these two countries were the greatest supporters of the abolition of the arms embargo on China. Former French President Jacques Chirac particularly stood out, emphasizing that the arms embargo was outdated. In January 2004, Chirac emphasized that the embargo no longer corresponded to the political reality of modern world and it therefore did not make sense in today's conditions. The German Chancellor at that time, Gerhard Schröder, also emphasized that the embargo should be lifted. By the end of 2003, Silvio Berlusconi, the Italian Prime-Minister, Jose Maria Aznar, the Spanish Prime-Minister,

also joined the previous two. The proposal to lift the embargo was officially set by France and Germany on the European Council in Brussels in December 2003. Sweden and Denmark had opposite standpoints and considered that the situation in terms of respect of human rights in China is not at the satisfactory level.

The USA intervened with strong criticism and opposition to the proposal for removal of the arms embargo to China. The American Government even threatened with the cooperation between the USA and EU in the industrial and defence sector, if the embargo was lifted. Bush administration opposed the removal of the embargo for several reasons. Firstly, the embargo was originally imposed because of concerns regarding human rights and the human rights situation was not improved to a level which would enable the embargo removal. Secondly, the USA was concerned about export control in the EU and the possibility for protection of sensitive technologies to be transferred to China, and especially because the Code of Conduct in the EU was not legally binding and also because the embargo from different EU state members was interpreted differently. Thirdly, the USA had an obligation and interest in maintaining the balance between Taiwan and China, which would allow Taiwan to be able to defend itself.

As a response to American criticism, the official EU representatives stressed that the removal of the embargo represented mostly a “symbolic gesture”. In other words, the removal of the arms embargo would represent a political act which would not suggest that the EU members would endeavor to sell arms and defence technology which was also included in the embargo on China. Also, the EU officials stated that they would approach the revision of the Code of Conduct (COC) which was adopted in 1998, and that it would establish criteria for EU arms sale worldwide. (Casarini, N. 2009: 127).

In the years that followed, especially after the announcement of the EU directives at the end of 2006, there is evidence for deterioration in the tone of the official rhetoric coming from the EU and PRC, because the EU pressed for derogations from China on issues such as trade restrictions, human rights and intellectual property, while China refused these attempts and continued to press for the removal of the arms embargo from the EU and granting People’s Republic of China a market economy status. These events, which effectively created a halt that lasts even today, led to a greater precaution (and even greater pessimism) in the academic expertise on relations, because it became evident that the honeymoon between the two partners had ended and that the relation is in danger to be compromised.

In fact, as stated earlier, the volume of trade between the EU and China bloomed in recent years: for example, between 2004 and 2008 the export from Europe to China grew by 65%, while in the same period the import to Europe from China grew by approximately 18% per year. Unfortunately for Europe, the trade deficit with China also grew quickly. As an illustration, the trade gap between the EU and China expanded from 49 to 130 billion Euros between 2000 and 2006. This deficit meant that a major part of the interest of Europe and that of the USA lay in the persuasion of China to



open its domestic markets to the European imports and investments and also to allow their currency to rise in relation with the Euro. The pressure from the USA managed to force China to gradually allow the Chinese yuan to rise opposed to the Dollar (and thus opposite to the Euro). The opening of Chinese markets proved problematic for the USA and Europe. Despite the EU support for China's entry into World Trade Organization in 2001, difficulties in the accession to the Chinese market still remain. Conditions that became even more obvious over time. In essence, it remains difficult for European companies to successfully penetrate the Chinese market, although some, for example the Czech-German vehicle manufacturer, Skoda has been successful with a growing Chinese demand for its products.

From Chinese perspective, in recent years Chinese leaders and experts began to see Europe as an inefficient mix of 28 member states (today 27, after the UK left the EU on the 31<sup>st</sup> of January 2020), rather than as an effective and resolute actor on the world scene. There are signs of China's disappointment with the negotiations between China and the European Union. For example, in 2009 the Chatham House paper indicated one unnamed Chinese official who stated that "the continuous failure of the 28 member states to come to a common position is rather frustrating and it has provoked many leaders in China to consider the EU as marginal." (Kerry B., Crossick S., 2009: 6). This led the Chinese to negotiate even more for bilateral trade agreements with individual member states, thereby avoiding the bureaucracy of the EU institutions, a policy-based trade which China has already tested in other places in the world, such as Africa and Latin America. (Garlick, J. 2013).

In the middle of an economic chaos of the global financial crisis and the European debt crisis, the trade issues are clearly a dominant aspect of the EU-China relations. These are prevail in the approaches of individual EU nations towards China, while they are trying to obtain agreements and deals with the Chinese, even in spite of the formal EU policy (ex. selling hardware for weapons to China despite the arms embargo, which is perceived as "outdated"). This led, for example, to the obvious twists on the issue of Tibet (ex. from the side of Nicolas Sarkozy who provoked the fury of the Chinese in 2008 when he met with Dalai Lama. Yet, he had already forgotten Tibet by 2011 and actively looked upon Chinese investments in France), while European leaders realized that maintaining a firm attitude for human rights in Tibet will provoke a problem in trade relations. This kind of policy change can be regarded as hypocrisy or pragmatism, depending on the perspective, but there is no doubt that the bilateral trade relations between EU members and Chinese companies (which inevitably must be authorized by the Chinese state) became the main point of the day, although they are contrary to the overall EU policy.

As the European debt crisis becomes acute and is spreading from Greece to other major debtors such as Portugal, Italy, Ireland and Belgium, there are likely to emerge more and more calls from the Europeans for the Chinese to invest in Europe on numerous levels, also including the purchase of bonds and involvement in infrastructure projects, such as reconstruction of roads and ports.

In the middle of the profound changes in the global economic order, which are already taking place, the need for Europeans to re-assess their overall approach and relations toward China will become even greater, especially because the Chinese already progressed in the game within the framework of the reassessment of their approach toward Europe as part of the change of the negotiations with the difficult bureaucratic structures of the EU towards bilateral agreements with individual countries.

At the same time, the viewpoint of the realpolitik implies that the Europeans should consider their tendency for clumsy and ineffective confrontation with issues like human rights, and also develop a more sophisticated relation to China's sensitivity for its sovereignty and the right for self-determination.

As a parallel for the European reassessment of their position, the Chinese side should have a better understanding of what is called a counter-hegemonic challenge of China when in a given situation it will not be accepted with open arms. The Chinese policies "divide and rule" that is conducted without fanfare, but it is still noticeable to the Europeans, will not help achieve China's objectives to increase its soft power with an unofficial framework for "peaceful development". Therefore, for practical purposes, but also for the benefit of all, China needs to show greater sensibility and understanding for the European sensibility, if it wants to establish relations with the EU based on cooperation instead of conflict. It should be pointed out that it is necessary to increase the number and quality of meetings and interaction between government officials, academics and businessmen, while encouraging the participants in the dialogue to learn to be tolerant about the conceptual gaps and cultural differences.

The relations between the European Union and China should have a vision of pluralism of cultures and civilizations, each with their own truths wherein there needs to be found compatibility and reconciliation between them. The development of better cultural programs and trainings in the EU and China should be recommended, as well as financing and educational resources which need to be allocated for this purpose. Such measures should lead in the long-term to strengthening of relations, as well as improved dialog and healthier diplomatic processes. Finally, we should remember that unlike Europe, China has an obvious advantage of having a single united policy, instead of 28 divided entities which are struggling to cooperate. This fact, however unpleasant for Europe to accept, gives China a big advantage to formulate and implement effective policies within its ability. Finally, from European perspective, if Europe does not take measures to find a new, united and pragmatic approach toward China, in order to cooperate with PRC, with one instead of 28 votes, it risks to be left out in the global race towards the uncertain new world order.

From today's perspective, the intensity of the cooperation is reflected through the engagement between the European Union and China which has become more com-

prehensive and more intense since the signing of the agreement in 1985<sup>3</sup> by the two sides. The annual summits between the EU and China were initiated in 1998 and to date there have been 22 such meetings, the last one taking place on 22 June and chaired by President Michel on the EU side and President Xi on the Chinese side.

Both sides have created more than 50 sectoral dialogues covering problems which affect their relations, from trade and financial relations to the environment, energy, education, protection of workers and customers, space cooperation and civil society. Yeh Honglin and Yu Chin made an interesting geopolitical and security analysis, which emphasize that the EU and China discussed the Taiwan issue from the 4-12 EU-China summit. At the 13<sup>th</sup> EU-China Summit, the Taiwan issue was no longer on the agenda. (Honglin, Y. Cheng, Y. 2014).

At the EU and China summit held in 2013, their strategic partnership deepened, which was made official by signing of the agreement of 2003. In 2013, both sides adopted the EU-China strategic cooperation agenda 2020.<sup>4</sup> After the presentation of this strategic document, the joint cooperation between the two sides became more institutionalized and more developed by the fact that more areas of interest have been added. The EU-China strategic agenda offers a list of key initiatives that should be achieved. The consultations for Africa, Central Asia and the neighbours of the European Union and China needed to be strengthened. Both sides decided to intensify the dialog about nuclear security, as well as about the struggle with the problems of nuclear material smuggling. In the sphere of security, both sides concluded that they should work on a common platform for a peaceful, secure and open cyber space. The document stresses out the need for joint combat against pirates, which makes China take an active participation in the so called “Atlanta Operation” (anti-piracy initiative of the European Union). The parties also agreed that they should deepen the Chinese and EU language learning in the educational systems in EU and China. The strategic agenda covers any kind of powerful aspect of cooperation: human rights, trade and security of the oceans, agriculture, space, and air space, as well as many other fields.

At the invitation of the President of the European Council, Herman Van Rompuy, and the President of the European Commission, José Manuel Barroso, President of the People’s Republic of China Xi Jinping visited the European Union in Brussels on 31<sup>st</sup> of March – 1<sup>st</sup> of April 2014. The Presidents had an in-depth exchange of views on bilateral, regional and international issues.

At the Summit in 2014, both sides agreed that this first visit by the Chinese President to the European Union was a historic landmark in the EU-China relations.

---

<sup>3</sup> Agreement on Trade and Economic Cooperation between the European Economic Community and the People’s Republic of China, OJ EU L 250 of 19.9.1985, pp. 2-7), available on the internet under: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ar14206> (accessed on 20.10.2020)

<sup>4</sup> Available on the internet under: [https://eeas.europa.eu/archives/docs/china/docs/eu-china\\_2020\\_strategic\\_agenda\\_en.pdf](https://eeas.europa.eu/archives/docs/china/docs/eu-china_2020_strategic_agenda_en.pdf) (accessed 30.10.2020).

They welcomed the significant strengthening of bilateral ties over the last 40 years, which has benefitted both sides and the world as a whole and underlined their determination to strengthen the global dimension of their cooperation. Both sides were willing to deepen their understanding of each other's development choices. The EU supports China's commitment to deepen reform comprehensively, and acknowledges China's goal of building a moderately prosperous society in all respects, while China supports the European integration process and acknowledges the EU reinforcement of its Economic and Monetary Union.

Donald Tusk, President of the European Council, Jean-Claude Juncker, President of the European Commission, and Premier Li Keqiang of the State Council of the People's Republic of China met in Brussels for the 17<sup>th</sup> EU-China Summit. At the summit in 2015 both sides confirmed their strong interest in each other's flagship initiatives, namely the Investment Plan for Europe, and the "Silk Road Economic Belt" and "21st Century Maritime Silk Road" (The Belt and Road Initiative). Leaders decided to support synergies between these initiatives, and directed the EU-China High-Level Economic and Trade Dialogue in September to develop practical avenues for mutually beneficial co-operation, including through a possible China-EU co-investment vehicle.

At the next summit in 2016, leaders moved forward the strategic partnership between the EU and China. They provided political guidance for the completion of the comprehensive agreement on investment and signed an energy roadmap. The 19<sup>th</sup> Summit between the European Union and the People's Republic of China held in 2017 in Brussels brought a number of important developments to the bilateral relationship, providing also fresh impetus to a partnership that has a global impact. Main accent was placed on climate action. At the Summit, EU and Chinese leaders reaffirmed their commitment to implementing the 2015 Paris Agreement on climate change and, as major energy consumers and importers, highlighted the importance of fostering cooperation in their energy policies.

On the occasion of this 20<sup>th</sup> EU-China Summit, the two sides celebrated the 15<sup>th</sup> anniversary of the EU-China Comprehensive Strategic Partnership. This has greatly enhanced the level of EU-China relations, with fruitful outcomes achieved in politics, economy, trade, culture, people-to-people exchanges and other fields. The Leaders reaffirmed their commitment to deepening their partnership for peace, growth, reform and civilization, based on the principles of mutual respect, trust, equality and mutual benefit, by comprehensively implementing the EU-China 2020 Strategic Agenda for Cooperation. At the 21<sup>st</sup> summit in 2019, the EU and China reaffirmed the strength of their Comprehensive Strategic Partnership, their resolve to work together for peace, prosperity and sustainable development and their commitment to multilateralism, and respect for international law and fundamental norms governing international relations, with the United Nations (UN) at its core. The two sides commit to uphold the UN Charter and international law, and all three pillars of the UN system, namely peace and security, development and human rights.

During the Covid-19 pandemic era the last 22<sup>nd</sup> Summit in 2020 was a video conference meeting. One of the Summit conclusions was the EU readiness to continue to discuss the Strategic Agenda for Cooperation 2025, which can only be concluded once significant progress has been made in the negotiations on the Comprehensive Investment Agreement.

### Conclusions

The historical and chronological overview of the development of relations between the European Union and China clearly recognizes that the long and varied history of building relations between Europe and China casts a shadow on the present even in the moments when the two sides seek to establish closer and more equitable relationships. The analysis of their relations, followed by the development and construction of the theory and practice of international relations, geopolitical and geostrategic determinants of their relations, economic and trade cooperation, the exchange of scientific and human potential, transfer of technology and many other areas, points out to civilizational achievements for which both sides have a proper contribution.

From a strategic, geopolitical and economical point of view, it is very important to note that China, especially after 2012, intensified its relations with 16 countries from Central and Eastern Europe. The format of this cooperation is known as '16+1' summits that are held every year. This cooperation includes the Prime Ministers from Poland, Bosnia and Herzegovina, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Macedonia, Montenegro, Romania, Serbia, Slovakia, Slovenia, Albania and Bulgaria. The formation of the frame '16+1' is one of the most significant achievements of Chinese diplomacy. The '16+1' frame, which offers a variety of mechanisms and treaties between China and 16 Central and Eastern European countries, was established after the historic visit of Chinese Prime Minister Wen Jiabao of Poland in 2012. Today these initiatives are named as '17+1' after Greece joined the initiatives in 2019. The actual events show that the EU and China are still affected by geopolitical distance between them and by their different sets of values and misunderstandings. However, from the analysis of the events in the last decade, we can conclude and ascertain that currently they have the best stage of mutual relations. This paper will present a good basis for further scientific elaboration, assessment and forecast of the future directions of the development of EU-China relations.

### REFERENCES:

- Andrew Beatty. Prodi issues call to arms. <https://euobserver.com/news/10709> (accessed on 30.10.2020);
- Andrew J. Nathan and Robert S. Ross (1997) *The Great Wall and the Empty Fortress: China's Search for Security*. New York: Norton;
- Brown, Kerry and Stanley Crossick (2009) *The EU and China: Time for a change?*, Asia Programme Paper: ASP PP 2009/03 London: Chatham House;
- Colin Mackerras, (ed.) (2000) *Dictionary of the Politics of the People's Republic of China*. (New York: Routledge;
- Edmonds L. Richard, (ed.) (2002) *China and Europe Since 1978: A European Perspectives*. Cambridge: Cambridge University Press;

- Funabashi Yoichi, Michel Oksenberg, Heinrich Weiss (eds.) (1994) *An Emerging China in a World of Interdependence*. New York: The Trilateral Commission, 1994;
- Garlick Jeremy. (2013) *A critical analysis of EU-China relations: towards improved mutual understanding*. *Contemporary European Studies* 1/2013;
- Nicola Casarini. (2009) *Remaking Global Order. The Evolution of Europe–China Relations and its Implications for East Asia and the United States*. Oxford: Oxford University Press;
- Ong Russell (2007) *China’s Security Interests in the 21st Century*. New York: Routledge;
- Peter C. Perdue. *The First Opium War. The Anglo Chinese War of 1839-1842*. [http://ocw.mit.edu/ans7870/21f/21f.027/opium\\_wars\\_01/ow1\\_essay.pdf](http://ocw.mit.edu/ans7870/21f/21f.027/opium_wars_01/ow1_essay.pdf) (accessed on 24.10. 2020);
- Richard Maher, (2016) *The elusive EU–China strategic partnership*. In: *International Affairs* 92: 4 (2016) 959–976. Oxford: John Wiley & Sons Ltd.;
- Shambaugh, D. (2008) *China eyes Europe in the world: real convergence or cognitive dissonance?* In David Shambaugh, Eberhard Sandschneider and Zhou Hong (eds.) *China–Europe Relations Perceptions, policies and prospects*. New York: Routledge;
- Yeh Honglin, YuChin Cheng. (2014) *Republic of China’s Diplomatic Strategy in the EU-China Relations*. In: *Security Dialogues*. Vol.5, No.1. Skopje: Faculty of Philosophy;
- EU-China Summit joint statement <https://www.consilium.europa.eu/media/23732/150629-eu-china-summit-joint-statement-final.pdf> (accessed on 31.10.2020);
- EU-China Summit: moving forward with our global partnership. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_17\\_1524](https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1524) (accessed on 31.10.2020);
- Joint statement of the 20th EU–China Summit <https://www.consilium.europa.eu/en/press/press-releases/2018/07/16/joint-statement-of-the-20th-eu-china-summit/> (accessed on 31.10.2020)
- Single European Act. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A11986U%2FTXT&qid=1604847580322> (accessed on 31.10.2020);
- Treaty on European Union, OJ EU C 191 of 29.07.1992, pp. 1-110. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1992:191:FULL&from=NL> (accessed on 30.10.2020).



## MIGRANTS IN THE PUBLIC DISCOURSE OF THE CITIZENS OF BOSNIA AND HERZEGOVINA

Armin KRŽALIĆ<sup>1</sup>

**Abstract:** *Citizens' public discourse research can be used not only to understand citizens' differences in attitudes towards migrants, but also to consider how dominant discourses help shape migration policy, including the role of policy instruments on the subject. The objective of the paper is to research and give the description of attitudes and perception of BiH citizens about migrants and government activities in dealing with migrant issues. The methodological design is based on the use of qualitative and quantitative data collection methods. The structured interview technique and the group discussion (focus group) method were used as qualitative methods. The majority of respondents (62.8%) believe that migrants are neither a threat to the security of their community nor a threat to the security of Bosnia and Herzegovina. The largest number of respondents, 43.3%, perceives migrants as a threat to the economic development of the community. The public discourse of BiH citizens bears the essential features of liberal-critical schools of security studies (emphasis on human rights and freedoms, humanitarian dimension) as opposed to competitive approaches that believe that one's security can only be increased to the detriment of other people's security.*

**Keywords:** *migrants, the migrant crisis, citizens, migration policies, Bosnia and Herzegovina*

### Introduction

With the closure of the Croatian border with Serbia and by erecting a wire fence in Hungary, in early 2018 Bosnia and Herzegovina became one of the countries which refugees used to pass through in order to reach their destination.

At the macro level, the refugee issue has sparked numerous debates in all European Union countries. The problem related to immigration laws has enabled a sudden rise in the popularity of right-wing extremist<sup>2</sup> parties and called into question the stability and validity of the Schengen area.

---

<sup>1</sup> The author is Ass.Professor at Faculty for Criminalistics, Criminology and Security Studies, University of Sarajevo

<sup>2</sup> Parties such as: National Democratic Party of Germany (NPD), Patriotic Europeans Against the Islamization of the West (PEGIDA), Alternative for Germany (AfD), National Conservative Party Prawo i Sprawiedliwość (PiS - "Law and Justice") - Poland, Front National (FN) - France, Partij voor de Vrijheid (PVV) - Netherlands, Freiheitliche Partei Österreichs (FPÖ) - Austria, Dansk Folkeparti (DF) - Denmark, Fremskrittspartiet (FrP) (Advanced Party) - Norway, Perussuomalaiset PS) - Finland, National



At the micro level, the polarization of society and institutions, which was caused by the population movement, is especially noticeable. Such polarization can be especially contributed to the media, which coined the term “migrant crisis”, and as stated by Kržalić, Korajlić and Mesihović-Dinarević, (2019) “*a special place in this process is played by various political figures, who, through their statements, sought (or succeeded) in securitizing and criminalizing refugees and influencing public opinion and the perception of refugees*”. Securitization has a special meaning in security studies, and the most famous is Waever’s definition, which considers securitization a process by which “something or someone” presents a security threat and justifies the use of emergency measures to eliminate this threat. Several entities are involved in the securitization process, including government employees, politicians, the media, migrants and other allies.

In this paper, we present an original analysis of the attitudes and perceptions of the citizens of Bosnia and Herzegovina towards migrants and the activities of the authorities in addressing migrant issues. The motive for this analysis stemmed from the destructive policies that sought and continue to use the issue of migrants as a destabilizing factor for the national security of BiH. More precisely, these forces want to present migrants as hostility and a threat to security. Hostility is defined as an attitude composed of two different dimensions. The first dimension is reflected in the degree of acceptance of the other, referring to the political issues of demarcation of identity. This requires an examination of whether individuals accept all migrants or only people of the same race/nationality, and the degree of rejection and aversion to people coming from poor countries (Zick et al., 2009). The second dimension is related to the way people predict the impact of migrants. Hostility is not just an attitude of immediate rejection and animosity towards unwanted groups or individuals. It is also an attitude related to an individual’s projection of their future and the way they assess and appreciate the consequences of newcomers on the economy, culture, and their quality of life. Using this conceptual definition of hostility, we examined the perception of BiH citizens towards migrants.

### Methodology

This is a non-experimental study, based on primary data. The sample of the survey questionnaire consisted of 586 respondents older than 18, with a confidence level of 95% and an interval of 5%. For data collection and selection of respondents, the technique “face to face” of random passers-by from the area of Una-Sana Canton, Sarajevo Canton, the City of Banja Luka, Herzegovina-Neretva Canton and Brčko District of BiH were used. The software “KoBo Toolbox” with the addition of a mobile application was used in the survey, and the software SPSS was used for processing and analysis of quantitative data. Of the qualitative methods, the method of examination by the technique of structured interview and the method of group discussion (focus group) were used. Interviews were conducted with migrants from the area of Bihać, Velika Kladuša and Cazin in the period from October 2018 to February 2019. Also, a survey was conducted during this period.

---

Alliance - Latvia, United Kingdom Independence Party (UKIP) - United Kingdom, Lega Nord (LN) - Italy, Chrysi Avgi, Golden Dawn - Greece and Serbian Radical Party (SRS) – Serbia.

Focus groups were held in Bihać, Sarajevo and Banja Luka on March 2019. Focus groups had an average of 10 participants, and the duration of focus groups was up to 60 minutes. The selection of participants was made on the basis of eligibility, i.e. a certain level of prior knowledge in accordance with the researched issues. For the sampling of the focus group participants, we used a non-probabilistic approach using the snowglobe technique. The socio-demographic factor of focus groups is provided, i.e. the heterogeneous composition according to: gender, age, education, ethnic or religious specificity and employment.

### **Perception of social phenomena that contribute to the feeling of insecurity among citizens**

*Migration* is a complex and multifaceted *category related to many different issues*, dealt by a variety of *institutions*, and *involving a variety of administrative levels* (Penninx, 2013 and 2014). Migrant issues in Bosnia and Herzegovina often interact with topics related to security, health, politics, social policy, interreligious dialogue, and education. Furthermore, when discussing migrants in political discourse, the topic is set in terms of danger and risk in such a way that migrants are often criminalized, i.e. presented as a threat to the safety of BiH citizens. (Kržalić et al., 2019 and Maneri, 2009). For these reasons, our commitment is to find out where migrants are in this context through the research questions on perceptions of social phenomena that contribute to the feeling of insecurity among citizens. The countries of Central Europe, which after the fall of communism accepted European values and became full members of the Union, have a clear position that they do not want to accept migrants. This approach differed from the adopted common position of the Union that countries will jointly share the challenges of the Union on issues of migrants. Hungary has gone the furthest in its anti-immigrant policy, which, according to the writing (Mikac and Dragović, 2017), “*argued that migrants pose a threat to its national security and European values*” (p. 136). Koser (2011) states that declaring migrants a security threat has significant consequences for laws, norms, policies and procedures that justify increased surveillance, arrests, deportations and restrictive policies. Kos-Stanišić (2018) states that “*asylum seekers are denied access to safe countries and migrants are thrown into the arms of smugglers or human traffickers, while the anti-immigrant mood grows*” (p. 255). Based on such theoretical discussions, a valid question arises as to whether the passing of migrants through Bosnia and Herzegovina to Western countries is a threat to national security, i.e. whether they contribute and to what extent affect their sense of insecurity. The results of the surveyed citizens show that they believe that the main phenomena that contribute to their sense of insecurity are related to organized crime (drugs, prostitution, smuggling of goods, vehicle theft) and the issue of corruption.

### Social phenomena that contribute to feelings of insecurity

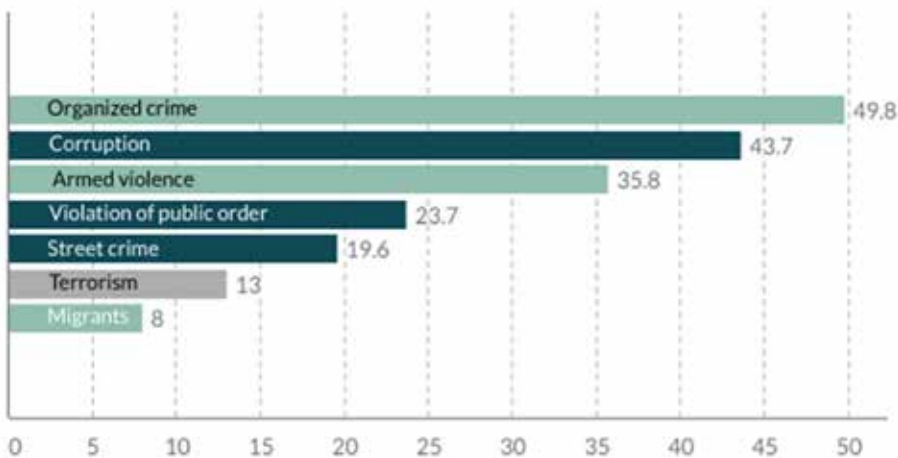


Figure 1. Frequency of social phenomena that strongly contribute to the feeling of insecurity of citizens

Respondents see the issue of migrants and refugees as relevant but not as one of the fundamental issues that contributes to increasing feelings of insecurity. When asked to what extent social phenomena contribute to the respondents’ sense of insecurity, out of the seven social phenomena offered, the largest percentage of respondents chose that organized crime - 49.8% and corruption - 43.7% are social phenomena that contribute strongly/very/greatly to the their feeling of insecurity. Migrants were chosen as the seventh phenomenon that contributes to the feeling of insecurity of citizens. Only 8% of the sampled respondents perceive migrants as a threat that greatly contributes to their sense of insecurity.

### The presence of migrants strongly contributes to insecurity

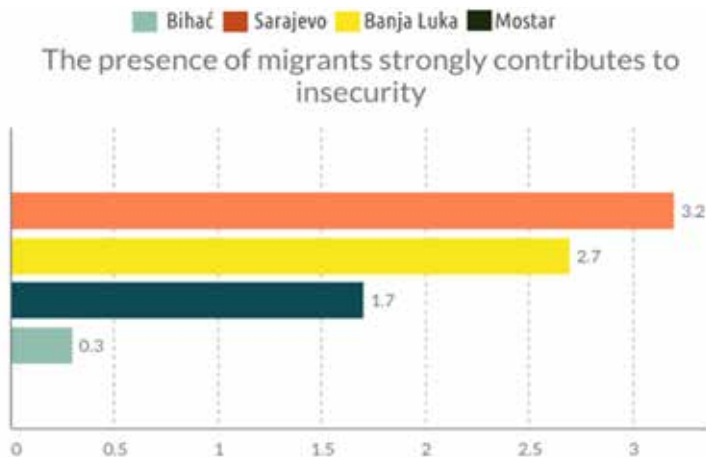


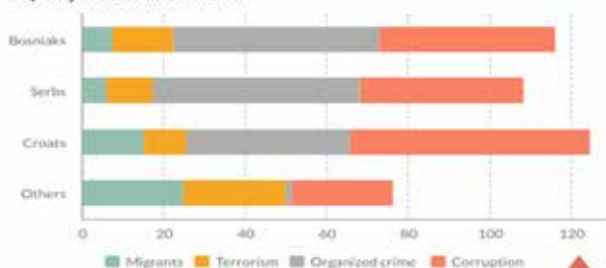
Figure 2. Frequency of citizens' responses that migrants strongly contribute to the feeling of insecurity

The largest number of respondents who stated that the presence of migrants greatly affects their security is in the USC (Bihać 22.3%), followed by Sarajevo Canton 17.8% and Mostar 17%. The Brčko District of BiH and Banja Luka are the cities with the highest frequency of responses that the presence of migrants has little or no effect on their security. The attitude that *organized crime and corruption* contribute the most to their insecurity is most distinct in Sarajevo Canton, 68.2%, followed by respondents from Banja Luka with 54.5%, Bihać with 51.5% and Brčko District of BiH with 36.4%. Corruption as the second social phenomenon that strongly contributes to the insecurity of citizens was most often chosen by respondents from Mostar, 61.5%, followed by respondents from the Brčko District of BiH, 51.5%, Sarajevo Canton 47.1%, Bihać 39.8% and Banja Luka 33.7% .

Regardless of which area our respondents are from or what ethnic group they belong to, respondents think that their feel of insecurity is mostly contributed to *organized crime and corruption*. Interestingly, in relation to the age and gender of the respondents, there is no strong correlation when it comes to the choice of the first two social phenomena that contribute to the feeling of insecurity. This means that men and women choose corruption and organized crime as the social phenomena that contribute the most to the feeling of their insecurity, as well as the respondents, regardless of whether they are young or old. Taking into account that the largest number of migrants in Bosnia and Herzegovina is located in the Una-Sana Canton (USC) and the Sarajevo Canton, we were interested in whether the presence of migrants contributes to the feeling of insecurity among citizens. Attitudes that the presence of migrants is a leading social phenomenon that strongly contributes to the feeling of insecurity of BiH citizens are most evident among respondents from Sarajevo Canton and Una-Sana Canton (12.1%: 11%). A deeper analysis of the answers shows that the issue of danger is perceived in two segments, through the commission of criminal offenses and the danger of terrorism.

### Ethnicity - relationship

Social phenomena that strongly contribute to the feeling of insecurity / two with the highest frequency of the chosen rank - strongly contribute, and with the lowest frequency of the same chosen rank



The largest number from the ranks of the Others (25%) stated that migrants have a strong influence on their security, followed by Croats, 15.2%, Bosniaks 7.6% and Serbs 6.2%.

When it comes to nationality, the largest number from the ranks of the Others (25%) stated that migrants have a strong influence on their security, followed by Croats, 15.2%, Bosniaks 7.6% and Serbs 6.2%.

Respondents believe that out of the seven mentioned social phenomenon, terrorism, the presence of migrants and street criminal, at least contribute to their sense of insecurity. The majority of respondents, as many as 75.5% of them, believe that migrants are ready to leave our country as soon as the opportunity arises. Also, all the migrants we spoke to in the municipalities of Bihać and Velika Kladuša (12 of them) confirmed to us that they want to leave our country as soon as possible, because their goal is going the developed countries of the European Union. Based on the information obtained through interviews with migrants, we learned that “they mostly try to cross the border between Bosnia and Herzegovina and the Republic of Croatia during the night on a 70-kilometer border strip” (# 4, Migrant, Personal interview, December 2018).

This is not always successful in most cases and they usually have 6 to 9 illegal attempts to cross the border. Migrants have a positive attitude towards the USC police and other police agencies in BiH, as well as towards the citizens, but most complain about the work of the Croatian Border Police, which confiscates their travel documents, money and mobile phones. According to the information that we received during the interviews with them, there are frequent cases when the Border Police of the Republic of Croatia uses force against migrants and inflicts bodily injuries on their hands, head and stomach. As proof of this claim, a migrant from the migrant center Đački Dom Borići in Bihać showed us medical documentation proving that his ribs were crushed. When it comes to the border police of the Republic of Slovenia, migrants do not have a bad opinion about their behaviour, but they complain that they have to pay a fine in the amount of 200 Euros for illegal border crossing.

Hostility toward immigrants, racism and xenophobia are on the rise in Europe, according to some case studies - including reports from the European Commission Against Racism and Intolerance and reports from the European Network Against Racism. In addition to researching cultural issues that may contribute to anti-migrant attitudes, through an original survey of citizens, we also examined the perception of threats based on the immediate experience of the respondents. This perception referred to perceiving migrants as a threat to the security of the community and society of the respondents. By threat we mean a threat to the economic development of the community and a threat to cultural identity (a sense of belonging to a group). Baričević and Koska (2017) in a study on the perceptions of migrant workers and asylum seekers in the Republic of Croatia, specifically Osijek-Baranja and Vukovar-Srijem counties, state “that, in terms of the socio-cultural aspect, foreign workers are perceived as a threat, and asylum seekers as a security and economic threat” (page 17). Kumpes and Gregurović (2009) and Čačić and Kumpes (2012) present findings that socioeconomic and socio-cultural factors are critical in explaining the attitudes of the population towards immigrants and immigration.

According to the results of our research, the largest number of respondents, 43.3% of them, perceive migrants as a threat to the economic development of the community. Also, more than one third of respondents (37.2%) perceive migrants as a threat to the security of their community and society, while slightly fewer respondents, 35.8%, perceive migrants as a threat to cultural identity (sense of belonging to a group). These respondents, as well as

focus group respondents, as a key problem in society, cite the poor economy and political opportunities that favour elected representatives who avoid dealing with social issues, the fight against corruption, nepotism and labour market problems and production.

However, the majority of respondents (68.9%) believe that migrants are not a threat to the security of their community, nor a threat to the security of Bosnia and Herzegovina. These respondents, as well as focus group respondents, see the key problem in society primarily in the bad economy and political opportunities that favour elected representatives avoiding dealing with social issues, fighting corruption, nepotism and labour market and production issues.

In the focus groups, the issue of security and threats was specifically addressed. The biggest concern for security among focus group participants is the issue of property and personal security. A small number of focus group participants in Bihać, Banja Luka and Sarajevo said they felt some concern about possible terrorist attacks. If we compare the results of the security issue with the similar results of the study by Baričević and Koska (2017) from Croatia, significant differences are noticeable. In this study, a larger number of respondents “were more inclined to feel a certain concern about possible terrorist attacks and security concerns related to terrorism coincided with the perception of a cultural threat from the “Muslim east”” (p. 23).

When we talk about political opportunities, the largest number of respondents state that political parties define migrant issues as a threat to security (57.8%). Just over one-fifth of respondents point out that political parties define migrant issues as an economic expense. A significant number of respondents emphasize that political parties define migrant issues as a question of threat through a change in the demographic structure of the population and a threat to cultural identity (16.7%: 4.1%).

These findings suggest that there is an intense politicization of the relationship between crises and migration in BiH’s public political discourse, and that politicians and political parties often interpret “migrant issues” depending on the context that suits them - to divert attention from other issues or to support some political issues.

Citizens’ attitudes about government activities on resolving migrant issues

The issue of migration in European countries is regulated by a complex interaction of legal and political provisions at the supranational and national level. The European Union established the free movement of workers and citizens on European soil, but also had to establish a common policy towards third-country nationals as a result of the abolition of internal borders (King et al., 2017). Such community-based policy-making on migration and asylum was formalized by the 1997 Amsterdam Treaty. These policies focus in particular on regulating migration from third countries, combating so-called “illegal immigration” and, to some extent, improving the legal status of migrants. Managing, regulation and settlement of migrants is done primarily at the national level, in combination with the local, regional and municipal levels. In the remaining part of the work we investigated and discussed the ways of managing migrants’ issues in BiH, and the activities and actions taken by the all levels of government in BiH in addressing migrant issues.

The Constitution of Bosnia and Herzegovina, in Article III, paragraph 1, item f), stipulates that institutions at the state level are exclusively competent to create immigration, refugee and asylum policies. Thus, the Strategy in the Field of Migration and Asylum (2016) states that “The said provision is one of the legal bases for the adoption of legal and political documents regulating, in a planned, organized and harmonized manner, the activities of competent institutions in this domain, with view to creating the most efficient control mechanism for the said phenomena in Bosnia and Herzegovina”(p. 23). This norm indicates that the BiH Council of Ministers is the only body that can make decisions and measures regarding issues of refugees, migrants and asylum seekers in BiH, all in accordance with existing international conventions and standards. However, it is important to point out that the BiH Constitution stipulates that the BiH entity and lower levels of government will provide all necessary support to the BiH Council of Ministers to comply with its international obligations. We asked the citizens what level of government and to what extent they complied with their obligations in resolving the issue of migrants and refugees, and based on their answers, we came to an interesting analysis. In general, respondents’ assessments of the authorities offered are the most positive in relation to the activities carried out by local authorities. The share of respondents who believe that local authorities are doing everything in their power to resolve migrant issues ranges between 27.1% and 31.5%, i.e. almost one third of respondents share this view. In contrast to this attitude towards local authorities, 46.3% of respondents believe that state authorities are not doing everything in their power to address migrant issues.

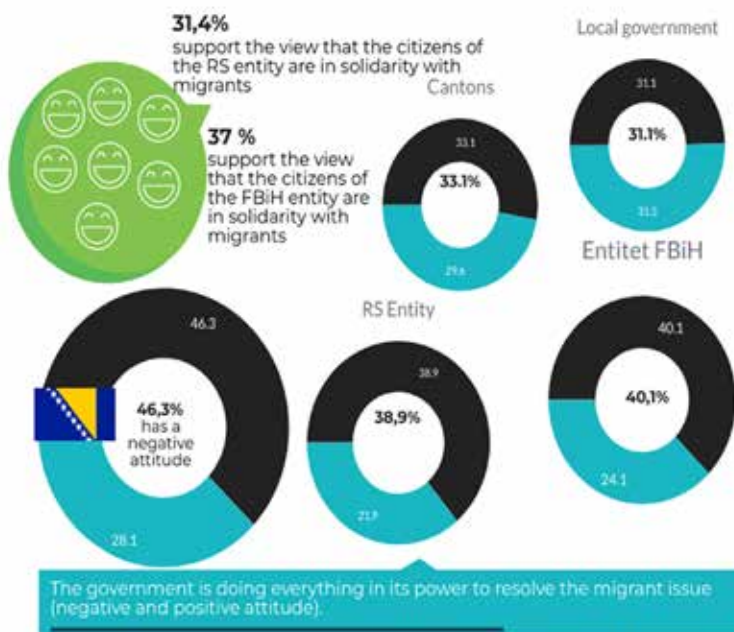


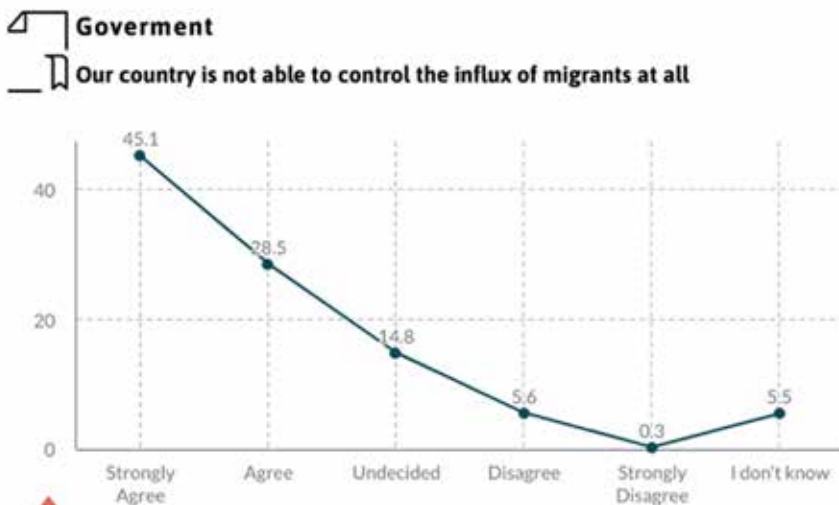
Figure 4. How the levels of government in BiH work on resolving migrant issues

This negative attitude of the respondents towards the work of the state government in resolving migrant issues coincides with the conclusions of the Ombudsman of Bosnia and Herzegovina based on visits to local communities, both in Bihać and in Velika Kladuša during the last four months of 2018. During these visits, the Ombudsmen of Bosnia and Herzegovina concluded that the support of the authorities of Bosnia and Herzegovina to the local communities in Bihać and Velika Kladuša was lacking (Institution of the Ombudsman/Human Rights Ombudsman of Bosnia and Herzegovina, 2018).

In the research, the respondents had a similar, that is, rather negative attitude towards the work of the entity and cantonal authorities in resolving migrant issues. Thus, 40.1% of them believe that the authorities of the Federation of BiH are not doing everything in their power to resolve migrant issues, and there are slightly fewer respondents of this kind in the entity of Republika Srpska (38.9%).

Hence the idea that all authorities in BiH establish a joint solidarity fund to address the issue of migrants in order to at least financially relieve the communities and levels of government that are most affected by the influx of migrants.

The majority of respondents (73.5 of them) were of the opinion that our country is not able to control the influx of migrants at all. Persons with whom we conducted interviews also agree with such attitudes, emphasizing that the police, despite facing a number of problems such as lack of equipment and professional staff, mostly work professionally.



The largest number of respondents, 45.1% of them, support the view that our country is not able to control the influx of migrants and refugees

Graph 5. Response frequency according to the claim that our country is not able to control the influx of migrants



A large number of participants in focus groups in Bihac, as well as in Banja Luka and Sarajevo believe that migrants should be helped in accordance with our capabilities (number of migrants, accommodation capacities, economic resources ...).

*"We have to help these people, because we were in the same situation a few years ago ..."*. (Amer, Focus group. Sarajevo, March 2019).

Most focus group respondents in Sarajevo, Mostar and Bihac believe that migrants should be helped, and compare the current humanitarian crisis (influx of migrants from Iraq, Syria, Afghanistan, Libya) with our own experience that we went through from 1992 to 1995.

In addition to examining the humanitarian approach to addressing migrant issues, we investigated the extent to which citizens associate migrants with the security problem, i.e., perceived threats. Based on the results of the research, it is evident that the opinion of the respondents is divided with respect to the attitude that a significant part of migrants is violent and represent danger, i.e. that they represent hostility for the local community. Thus, 25.8% of respondents support this view, while 24.4% do not support this hostile attitude view. Hostility can actually be related to the context in which people live (Biorcio and Vitale, 2011). Although there is no significant difference between the city and the countryside, living in a large city or suburb reduces the percentage of hostility, while living in the countryside increases it. This is consistent with a similar finding in the US (Wuthnow, 2013).

When it comes to hostility towards the local community, the highest frequency of answers is found among respondents who are undecided, as many as 42.2% of them. However, there are significant statistical differences among the respondents in the view that the appearance of migrants in their city has led to an increase in crime levels. More than one third (37.5%) share this attitude and a little more than one fifth (26.3%) do not agree with this attitude. Almost a similar number of respondents have a neutral opinion towards this attitude, 27.1% of them.

Although a certain number of respondents, 12.6% of them, agree with the view that a significant part of migrants belong to terrorist groups, the fear of terrorism is more evident among those respondents who come from areas where the concentration of migrants is lower or non-existent, namely Banja Luka and Brčko District of BiH.

Almost one third of respondents (32.5%) disagree with the attitude, that a significant part of migrants belong to terrorist groups, and the highest frequency of responses is recorded among respondents who neither agree nor disagree with this attitude, (39.6%). In interviews with focus group respondents, we concluded that the fear of terrorism is more pronounced among participants who have negative attitudes towards migrants.

The living conditions of migrants, which were inadequate at the beginning of the influx of migrants, probably created an attitude shared by almost half of the respondents. Thus, 49.4% of them were worried about the possibility of spreading unknown diseases brought by migrants. In November 2018, when we visited the Borići Dom in Bihac, we could see that it was an *inappropriate place* for the migrants to live in. It is a facility

that is 2 km from the city center. The building had an external wall construction with a roof that leaked on all sides. At the time of our visit, the International Organization for Migration [IOM] was working on improving living conditions of the facility.

### **Respondents' perception of immigration and its consequences for cultural and economic issues**

First of all, respondents were asked about their views on the benefits of living in a society with all kinds of differences (in terms of religion, nation and origin). The majority of respondents, 71.3% of them, consider it positive that they live in different environments, i.e. they agree that it is an advantage to live in a society where people of different religions, nations and origins live, and only 7.4% of respondents have a negative attitude towards such societies.

It is obvious that local politicians do not have such attitudes in mind when adopting certain policies. Through their activities, they adhere more to the attitude of minorities who have a negative attitude towards different societies, thus opting for the propaganda of policies shaped by the conflicts themselves, rather than the need to work more on reconciliation and togetherness.

In addition to this question, we asked the respondents more general questions regarding the immigration of foreigners to BiH, i.e. the desirability of immigration and migrants. More than one half of the respondents, 53.5 of them, support the immigration of foreigners to BiH. It is interesting to note that a small proportion of 7% of respondents are reluctant to support the immigration of foreigners to Bosnia and Herzegovina.

Almost identical views are shared by the participants of the focus groups who had developed discussion on this issue and believe that it would be much better if foreigners from more developed countries come to manage our public companies.

Insecurity towards migrants is often caused by the feeling of the citizens of the state (transit or final destination) that migrants endanger them culturally (especially in terms of language and religion), socio-economically and politically (in the sense that they are potentially disloyal and subversive) (Castles et al., 2014: 199–200).

When it comes to cultural issues, almost one half of the respondents, 48.5% of them, think that it is fine that foreigners who come to our country stay attached to their culture and roots. It is interesting that some participants in the focus groups see this issue, as well as the issue of treating migrants, as a test of the maturity of democracy, and most of them believe that migrants should be treated “humanely” during the crisis.

Almost one third of the respondents, 30.4% of them believe that foreign immigrants are not ready for social and cultural change and adaptation, while slightly more than one third, i.e. 36.9%, believe that they are ready to support our country in case of crisis. There are a significant number of respondents who neither agree nor disagree on these issues.

## Attitudes and prejudice towards migrants

The analysis of the academic literature indicates that four main trends stand out in this issue. First, migrants are usually labelled as “Arabs” or “immigrants” - and negatively labelled. Second, migrants are usually shown either as victims, survivors of the terrible events and in need of support, or as a threat to national transitional societies or final destination, as well as stealing jobs and as a change in the cultural and religious characteristics of the society of final destination (Anderson, 2008). The third trend, which has been recognized in several studies, refers to the systematic absence of the direct voice of migrants in the press. “Finally, *national media* usually discusses *migrants* within the *specific local context*, without a *broader European perspective*” (Bennett et al. 2013, pp. 249-250). Fourth, the latest trend, however, has been changing in recent years, due to what the mass media call a “migrant crisis”.

The research of Baričević and Koska (2017), Kuti, Gregurović and Župarić-Iljić (2016) and Čačić and Kumpes (2012) show that little attention has been paid to the research of prejudice toward migrants in our region. Therefore, our commitment is to examine the attitudes of citizens about prejudices towards migrants, in those places where they had the opportunity for contact with migrants. The vast majority of our respondents are of the opinion that attitudes towards migrants are created on the basis of prejudice, as many as 70.8% of them. The respondents who had this opinion confirm that migrants are subject to prejudices based on cultural and religious characteristics (32.8%), followed by their origin 22.2% and skin colour 5.3%.

Respondents stressed that cultural-religious prejudices are regularly associated with Muslims, especially those coming from Afghanistan and Pakistan, although most respondents told us that they did not make any contact with migrants. This may indicate that migrants are subject to strong prejudices based on media reports in BiH and the labelling of their cultural and religious characteristics. Thus, Lučka and Čekrljija (2020) conclude that “*migrants through various media and means of information, as well as the social networks are stigmatized, dehumanized and labelled as guilty for many bad things that happen in society, and are presented in public as criminals who are predestined to commit crimes wherever they go*”.(p. 23). The best example of spreading false news and anti-immigrant campaigns is the web portal antimigrant.ba and the right-wing group in Serbia “Leviathan”. Most of our respondents believe that the anti-migrant attitude is the result of the cultural and religious affiliation of migrants. An almost equal number of respondents in both entities of Bosnia and Herzegovina are in solidarity with migrants and support the solution of migrant issues, and believe that the policies in BiH define migrant issues as a threat to security.

## Conclusion

Based on the original analysis of the primary data collected, we can conclude that, if we wanted to define the key features of the public discourse of citizens, we could point out the following: the issue of migrants and refugees is still seen as a humanitarian tragedy where

solidarity and togetherness are preferred. In public discourse, on the example of Bihać, Sarajevo, Mostar, we have witnessed and still witnessing the win of universal, collective values over cruelty and politicizing.

The migrant issue in the public discourse of citizens is treated as a supra-political question, a question of universal values. Given this, we can say that the public discourse of citizens about refugees has all the predispositions and characteristics to be a unifying factor, and not a source of contradictions and conflicts.

The majority of respondents (62.8%) believe that migrants are neither a threat to the security of their community nor a threat to the security of Bosnia and Herzegovina. The largest number of respondents, 43.3% of them, perceive migrants as a threat to the economic development of the community. Also, more than one third of respondents (37.2%) perceive migrants as a threat to the security of their community and society, while slightly fewer respondents, 35.8% of them perceive migrants as a threat to cultural identity (sense of belonging to a group).

The majority of respondents (73.5 of them) are of the opinion that our country is not able to control the influx of migrants at all. The people we interviewed agree with these views, emphasizing that the police, despite facing a number of problems such as lack of equipment and professional staff, mostly work professionally.

Bosnia and Herzegovina must urgently find a solution to maintain control over its border and shape a coherent national identity. Under international law, states are required to control their borders and decide who can enter, but also who can stay in the state.

The public discourse of BiH citizens bears the essential features of liberal-critical schools of security studies (emphasis on human rights and freedoms, humanitarian dimension) as opposed to competitive approaches that believe that one's security can only be increased to the detriment of other people's security. This concept should be followed until the issue of refugees is resolved, and these goals must be based on the concept of peace and humanity. It is precisely this fact that should represent a huge capital for the future and a pledge to prevent a more significant influence of right-wing discourse. Yet in the end, the question arises as to why, despite such attitudes at the micro level, public discourse at the macro level has begun to change in recent years.

It is important that the voices of those who fight every day for respect for human rights and the dignity of all persons are heard in political discourse. Also, it is necessary to oppose the very loud populist voices, as well as every form of violence, racism and xenophobia that we increasingly encounter in public discourse. This may indicate that public and scientific discourse is increasingly retreating before political discourse. For all these reasons, we have to ask ourselves, where does such a retreat lead us?

## REFERENCES:

- Anderson, B. (2008). "Illegal immigrant": Victim or Villain? *ESRC Centre on Migration, Policy and Society Working Paper No. 64, University of Oxford, 2008, 43*, 1–23. [https://doi.org/Wimmer\\_2007](https://doi.org/Wimmer_2007)
- Baričević V., & Koska V. (2017). Stavovi i percepcije domaće javnosti o nacionalnim manjinama, izbjeglicama i migrantima. Zagreb: Centar za istraživanje etičnosti, državljanstva i migracija (CEDIM) i Fakultet političkih znanosti, Sveučilište u Zagrebu
- Bennett, S., J. ter Wal, A. Lipinski, M. Fabiszak & M. Krzy Żanowski (2013), 'The Representation of Third-Country Nationals in European News Discourse', *Journalism Practice*, 7 (3), 248-265,

- Biorcio, R. & Tommaso V. (2011). 'Culture, Values and Social Basis of Northern Italian Centrifugal Regionalism. A Contextual Political Analysis of the Lega Nord.', in Michel Huysseune (ed.), *Contemporary Centrifugal Regionalism: Comparing Flanders and Northern Italy*, Brussels: Royal Flemish Academy of Belgium for Science and the Arts Press, pp. 171-199.
- Institucija ombudsmena/ombudsmana za ljudska prava Bosne i Hercegovine. (2018). *Specijalni izvještaj o stanju u oblasti migracija u Bosni i Hercegovini*. [https://www.ombudsmen.gov.ba/documents/ombudsmen\\_doc2019010713545979bos.pdf](https://www.ombudsmen.gov.ba/documents/ombudsmen_doc2019010713545979bos.pdf)
- King, D., Le Galès, P. & Tommaso V. (2017). 'Assimilation, Security, and Borders in the Member States', in Desmond King and Patrick Le Galès (eds), *Reconfiguring European States in Crisis*. Oxford: Oxford University Press, pp. 428-450.
- Kos-Stanišić, L. (2018). Ilegalni migranti u tranzitu kao prijetnja sigurnosti građanima Meksika. *Migracijske i Etničke Teme / Migration and Ethnic Themes*, 34(3), 251–273. <https://doi.org/10.11567/met.34.3.2>
- Kržalić, A., Korajlić, N., & Dinarević, S. M. (2019). Securitization and Criminalization of Migrants in Bosnia and Herzegovina. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3386164.3389104>
- Lučka, D., & Čekrljija, S. (2020). *Izbjeglice i migranti u trouglu Bosne i Hercegovine, Hrvatske i Srbije*. <https://www.fed.de/>
- Mikac, R., & Dragović, F. (2017). Masovne migracije : posljedice i put naprijed. *Forum Za Sigurnosne Studije, Vol. 1 No.*, 130–152. <https://hrcak.srce.hr/198071>
- Strategija u oblasti migracija i azila, (2016). [https://bih.iom.int/sites/default/files/Strategy/Strategija\\_BiH\\_2016.pdf](https://bih.iom.int/sites/default/files/Strategy/Strategija_BiH_2016.pdf)
- Smajić, M. (2017). Sigurnosni aspekti migracijske krize: između humanosti i oblikovanja novih "umjetnih" manjina. *Forum za sigurnosne studije*, 1 (1), 153-167. <https://hrcak.srce.hr/198076>
- Penninx, R. (2013). International migration and multilevel governance in Europe. In V. Bilger, S. Klinglmair, & M. Hofmann (Eds.), *10 observations on the future of migration: costs, benefits and policy responses*. International Centre for Migration Policy Development (ICMPD). <https://hdl.handle.net/11245/1.447246>
- Penninx, R. (2014). Chapter 8 Integration of Migrants : Economic , Social ,. *Integration The Vlsi Journal, January 2004*, 137–151. [https://www.researchgate.net/publication/254920820\\_Integration\\_of\\_migrants\\_Economic\\_social\\_cultural\\_and\\_political\\_dimensions](https://www.researchgate.net/publication/254920820_Integration_of_migrants_Economic_social_cultural_and_political_dimensions)
- Wuthnow, R. (2013). *Small-Town America. Finding Community, Shaping the Future*. Princeton: Princeton University Press.
- Zick, A., Kuper, B., & Wilhelm, H. (2009). *Prejudices and Group-Focused Enmity-A Socio-Functional Perspective'* (H. of P. In A. Pelinka, K. Bischof, & K. Stögner (Eds.) (ed.)). Amherst, N.Y: Cambria Press. <https://pub.uni-bielefeld.de/record/1856715>

## TECHNOECONOMIC CHANGES AND SECURITY: NEW PARADIGM?

Ivan JOVETIC<sup>1</sup>

**Abstract:** *Technological changes impacts economy, security and society. Inability to adequately respond to the changes usually leads towards paradigm changes. Security and economic security are not exceptions at all. They evolve and change creating the new security paradigm. This paper focuses on different security impacts including corporate as well as individual(s) security. In addition, it is attempting to provide correlation rationale of corporate security, individual(s) security, economic security, as well as overall security. The novel economic security paradigm is related to the technological advancements and changes such as cyber and artificial intelligence. The potential new arms race is one of the changed paradigm outcomes. And, if it fully happens and further develops, it will have significant security and economic impact. Overall, this means that technological changes also (re)shape individual(s) security within the new paradigm. However, it also means that Goethe was right and that “technology will not save us”. Evolved paradigm might.*

**Key words:** *security, economic security, paradigm, techno-economic paradigm, cyber, change*

### Introduction

Definitions and paradigms are intertwined and interdependent. Paradigms are changing whenever previous set of definitions and theories show inability and incompatibility with the changes and their explanations. Kuhn referred to it as to *scientific revolution* and it has quite wide applications. Changes in the security contexts and rise of new security challenges directly change the respective paradigm. Current and future technoeconomic changes are positively correlated with tremendous changes of economic, security and cyber paradigms.

This paper deals with the definitions of security and the impact of technoeconomic changes. It is about adding the new dimension of impact on security and its different forms. A partially neglected element is the impact of the cyber security domain on the economics and the economic security. The potential explanation of the respective situation and trend can be related to the standard approach to security as a related element of the state and society in general. Previous, as well current technological changes prove this as a partially wrong premise. Individuals have been liberated by the technological advancements and changes. Respective changes also confirm the historically and logically founded Smith's ideas and previous attempts of individual security context framing. Individual security as a form of security is highly emphasized upon technoeconomic changes, as well as some other socio-economic changes. Consequentially

---

<sup>1</sup> PhD, Lecturer the UDG-Faculty for International Economy, Finance and Business

as firms (companies, corporations, etc.) are one of the most vivid and present organizational forms of individual endeavours, they are indeed expected to frame consequences and impacts on corporate security due to changes.

Cyber security challenges are one of the remarkable examples of technoeconomic changes. Respective challenges are leading to higher anonymity and attribution, precisely due to technoeconomic changes. They are also leading to direct expenditures of respective institutions, either due to prevention, or due to recovery. Common denominator, as well as necessity of potential solutions quest, is bringing all stakeholders towards the joint aim and importance of cooperation.

### Security paradigm(s)

The grand industrial-technological as well as social-political changes do change the warfare method. Consequentially, they change the security paradigm in wider, but also in the narrower context. It seems that the era defined as globalization derives the biggest changes and transitions due to: (i) complexity of technology and (ii) technology dependence.<sup>2</sup>

Beck, according to that, defined risk society, where risk increases with the increase of the technology's complexity (Beck, 1992). Historically, security paradigm has been introduced by Cicero and Lucretius who defined it as philosophical and psychological state of mind, i.e. subjective feeling of freedom from sorrow (Brauch, 2005). Subsequently it will be used as political concept within Pax Romana indicating political stability (Brauch, 2005). Since the 16th century, this respective concept began attaining public security context also indicating protection of vassals by the ruler in peace, as well as assistance and support to the ruler by vassals during the war. The idea that only a sovereign state can care for the security of its central referent object, i.e. security of the individual has been formed during the 17th century (Ejdus, 2012). In the historical and philosophical aspect, this respective idea is being formed alongside the definition of sovereign states as the most powerful actors in the international system, which happened in 1648 by the Peace of Westphalia. In addition, Hobs in 1651 defined the individual(s) as the referent object of security while defining the "social contract" idea also defining the state as the subject of security (Ejdus, 2012).<sup>3</sup> During the observed period, the security paradigm can also comprehend the economic security paradigm of the individual(s).<sup>4</sup> However, it will not be defined as such for the next several centuries.

---

<sup>2</sup> It is considered that current the technological development is larger than the human civilization's previously accumulated technological development– Gudic, Milenko (2014), lecture: *The road less traveled*

<sup>3</sup> As Ejdus defines "security grammar" include danger (what endangers), referent security object (what is being endangered), security subject (the one that protects) and means/measures of security (the means of protection).

<sup>4</sup> Indirect existence of the economic security paradigm can be linked to the necessity of protection and assurance of individual security and forms of property and assets (although it still cannot be talked about capitalism as an exchange synonym, certain exchange forms have existed since the Ancient economy).

Development and strengthening of national romanticism, as well as nationalism are part of 18th century. Consequentially, the process of establishing the state as the central referent object of both, identity and security began during the 18th and 19th century. The respective process rounded up with the First World War (Ejdus, 2012). During the following period states will remain as such security objects. The respective object has only anchored such position after the geopolitical block division and the beginning of the Cold War. However, some further geopolitical but also technological and economic changes led to the end of the Cold War, but also to the transformation of the security's central referent object. The new global techno-economically lead reality has led to widening and deepening of the security concept. Accordingly, the new dimensions of security such as: (i) political, (ii) economic, (iii) ecological, (iv) social and others have been included. Moreover, the idea that the state is the only referent object of security has been abandoned. Along the state, new security's referent objects have risen: (i) individuals, (ii) different (interest) groups, (iii) regions as well as (iv) own international system (global security context) (Ejdus, 2012). However, this must be expanded with differently motivated networks, rouge states and supranational institutions. The NATO Strategic concepts from 1999 and 2010 are one form of the respective transformation's confirmation. The impact of real changes becomes clearer due to the role and impact of the Strategic concept as the key NATO document.<sup>5</sup>

The key question is what security means. It seems that the first law of security refers to it as to "essentially disputable concept" due to large number of definitions (Baldwin, 1997). However, it seems that Wolfers had a valid point defining the security concept in an objective and subjective context (Wolfers, 1952). Accordingly, security in an objective context measures absence of threats i.e. endangerment of basic adopted social values, while security in a subjective context measures the absence of fear that basic values of society will be endangered.<sup>6</sup> Security perceived as threats absence tendency might be the most general but not the most adequate definition (Buzan, 1983). It seems that Ejdus' point referring to existence of dangers i.e. threats, challenges and risks positions as the central notion of security without which security debates are meaningless is quite accurate (Ejdus, 2012). Almost every key context has its own cause of existence. Danger is cause of existence of security as consequence. Similar comparison can be identified in many different concepts. What is the religion without the sin or economy without the crises i.e. imbalances as disequilibrium?<sup>7</sup> Buzan's definition is not entirely directed towards the lack of central notion rather to the tendency

---

<sup>5</sup> It is the key document after the Washington Treaty. It defines new challenges, risks, threats as well as the responses.

<sup>6</sup> Definition (in an objective context) does not a priori include threat absence rather it measures their degree. Precisely, it is possible that threats exist and that system is being endangered and therefore *endangered degree* i.e. *security consistency degree* is being measured.

<sup>7</sup> Alan Meltzer considers crises to market economy correlation equals to sin to religion correlation (according to prof. Steve Pejovich).



towards absence of threats. However, Wolfers' definition seems more appropriate because threats absence measurement is more important than tendency towards their absence.<sup>8</sup> Similar comparison in economy would be between exchange tendency and actually executed exchange. Beck can also be supportive in the context of security and (non)anticipated dangers revolving. He makes distinction between anticipated risks and non-anticipated threats.<sup>9</sup> Measuring is possible only after defining them in the real world. Precisely, measuring is possible only after threat detection which has distinct meaning in nonconventional, cyber world. Reason for respective comprehends asymmetry, anonymity and quite often secrecy as the core elements of threats. It seems that Beck is also tracing the idea that globalization itself blurs the line between internal and external – transnational security threats and challenges.

### **Economic security paradigm**

The global stage changed at the end of the 20th and at the beginning of the 21st century (re)established economic security paradigm. It was indeed the first such formulation attempt. However, peace and free market exchange correlation have been previously seen and formulated by Adam Smith as well in 1776. Exactly that will become the basis for definition of one concept within the traditional approach of security studies i.e. liberal peace theory. This respective approach assigns peace preservation antecedence to economic freedom and free exchange

Tracking Wolfers' security concept also enables defining of economic security as measuring of the basic economic value endangerment absences i.e. measuring absence of economic threats and dangers. Economic security in the narrower context can have several meanings: (i) production and trade of products and services with direct impact on the state's defence capability; (ii) economic policy instrument used as an offensive or defensive security policy tool (economic assistance, sanctions, restrictions); (iii) capability of maintaining of a certain economic development level as security function as well state's international position function; (iv) individual(s) economic security especially in the context of basic resources access or in the wider context of employability, poverty and education and (v) the one related to the global economic, societal and ecological stability (Beck, 1999). Economic security represents a paradigm of the individual(s) as well as the society's economic values

---

<sup>8</sup> This is particularly important in unconventional i.e. cyber world. In respective world threats can be *present* even if did not or could not measure them. Most of the threats are being discovered ex post and after such discovery endangerment degree is being measured i.e. assumes the measure of their absence.

<sup>9</sup> Beck also provides distinction to three global threat types: (i) ecological damages and techno-industrial dangers driven by wealth desire (ozone layer, global warming, regional water supply shortages) as well as unpredictable risks of genetic engineering; (ii) poverty related risks (environmental destruction) and (iii) weapons of mass destruction.

*Even though he does not state them, cyber weapons and tools can represent form of mass destruction weapons but also tool for economic and overall security undermining (author's remark)*

protection. Simultaneously, it represents protection of undisturbed exchange as well as establishment and maintenance of adequate economic growth and development which firstly enables both, state/region stability and individual(s) security itself. Observing economic security meanings in the narrow sense leads to the conclusion that production and trade as well as capability of maintaining of certain economic development level are the most important meanings. Moreover, they are directly correlated with the security function. Therefore, it can be concluded that economic security is a (pre) condition of the overall security. Impact of economy on security is undisputable and proven throughout history of techno-economic changes. The respective is especially valid knowing that economic/purchasing power of state itself (re)shapes security power. Significance of economic power is especially highlighted during the public debt crisis and limited resources. Historically, there is a tremendous correlation between economic capabilities on one side and survival capabilities (of great powers) on the other side (Kennedy, 1988). Nevertheless, reverse direction i.e. impact of security on the economy is also particularly important. Firstly, security must be observed as economic resource enabling undisturbed development.<sup>10</sup> The respective is crucial for small and microstates in order to ensure their own internal and partially external security. Secondly, it is also relevant for grand nations as aside the internal security they ensure own international position as well as form of international “order”. Probably the most apparent case is the USA which defined economic power as the source of American power and leadership within their official documents (US National Security Strategy, 2010). The economic security paradigm as well as security in general is dependent on the researcher’s view to the world (Brauch, 2005). Individual, economic freedom and exchange degree as well as the level of personal and system’s economic wealth can be identified as the central referent economic security object within respective context.<sup>11</sup>

According to Ejodus, security does not exist without dangers and threats (Ejodus, 2012). Congruently, economic security paradigm has its own central notion in threats that endanger it. Threats according to Ejodus can be divided into the levels of: (i) individual, (ii) state and (iii) international system. At the individual level, threats comprehend poverty, illness, hunger, crime, violence and terrorism. Poverty comes again as the threat on the state level as in the context of state’s basic services provision as in probability context of war, terrorism and extremism of any kind. GDP per capita

---

<sup>10</sup> Importance of undisputed economic development and growth is being especially recognized in the region faced the clashes and wars. Although this context usually leads to imagining Middle East (certainly justified) it is also necessary to observe “own yard” i.e. Western Balkan which had 11 wars in just 87 years of the 20<sup>th</sup> century. What kind of economic development is possible in such situation?

<sup>11</sup> Systems comprehend the state as still referent political organization unit. However, it should comprehend Ohmae’s region-state as well as regional integrations such are EU and the NATO whose aim is welfare protection within its *territory*. Certainly, welfare levels are not and cannot be the same at every *territory* part. Moreover, they should not be, as success responsibility is driven by individuals and system levels (cities, regions, states). On the other hand, members and supranational institutions as its core task have protection of overall and economic values and security.

level represents the corner stone indicator for such analysis conduction. According to the respected survey, states with GDP per capita lower than \$250 have 15% chances of civic war while respective probability is less than 1% for the countries with GDP per capita of \$5000 (Rice, Graff, Pascual, 2010). Second serious state level threat is energy deficit. US foreign policy pivot after the oil shocks in the 1970s witness the seriousness of this threat. Furthermore, energy security significance is being additionally confirmed by key NATO and member states documents and strategies.<sup>12</sup> Certain authors define four dimensions of energy security: (i) availability of energy products and services; (ii) reliability of energy services provision; (iii) availability at the market, transparent and predictable prices and (iv) ecological sustainability (Pascual, Elkind, 2010). However, 21st century changes required introduction of at least fifth dimension i.e. energy infrastructure's reliability relating to the non-predictability of cyber world "risk society". Ejdus considers globalization itself as the threat to state's economic security mainly because necessity of protection from ruthless global competition and all challenge globalization is brining. However, globalization succeeded in enabling both, individual's and system's liberation as well as providing economic prosperity to the individuals. At the very end, there would be no significant economic security resources without globalization itself. Nevertheless, if Ejdus is tracking Elsasser and partially Perkins and if assumed that partocracy and corporatocracy have negative impacts than context is being changed (Elsasser, 2009; Perkins, 2012). Moreover, such view should have been fully supported. Perhaps that leads to the necessity of changing the name of the process into globalism.<sup>13</sup> At the international system level the threat can be economy system design (parts of it) and protectionism and monopoly existence. Remarkable global economic interdependence can also be considered a threat, especially due to the possible spill over effect which has been confirmed by both, sovereign debt and financial crisis.<sup>14</sup> Again the key challenge is not core nature of globalization rather it is the power of partocracy and corporatocracy. The aforementioned is within the Benjamin's claim context that the advancement of each civilization has its own barbarian side (Benjamin, 1942). Conventional (Somali pirates, fundamentalists) and unconventional (cyber) terrorists processes are also threatening, alongside globalism and corporatocracy. Due to the increased number of all-level-threats, it can be considered that economic freedom and individual(s) and society's development have positive impact on solving economic security threats. Existence of barbarian side of globalization i.e. globalism is a challenge per se and it requires answers beyond the Sisyphus process' restraining.

---

<sup>12</sup> Energy security importance and partial energy dependence existence is also being confirmed by certain parts of Crimean crisis as well as behaviour of some western states.

<sup>13</sup> Globalism as any other -ism (Nazism, socialism, fascism, Europeanism, etc.) has negative context and can be excuse for numerous security (overall and/or economic) endangering policies.

<sup>14</sup> Crimean crisis can also be used as real example of political behaviour as economic interdependence consequence.

## Impact of technoeconomic changes

Dominant security notion in the literature refers to security (and defence) of state and society. Nevertheless, due to the papers' foundation in the realm of philosophy of liberty and free individual it is necessary to define security in the respective context. It is strongly believed that individual has been born free and that his/her security is being guaranteed by the social contract form. Individual(s) security in the objective context refers to absence of life, property and all individual rights endangerment. Subjective security of the individual refers to the absence of fear that respective values will be endangered. It is strongly believed that the key determinant of the security-freedom pair is *limitation of each individual's freedom is freedom of any other individual*. Even if individual security is being observed in the cyber world context it can also be discoursed about measured absence of individual's endangerment (objectively) i.e. measure of fear regarding values endangerment (subjectively).

Companies (firm, SME, corporation regardless the shape and size) represent one of the forms of activities and entrepreneurship organizations of the individual(s). Therefore, corporate security represents quite an important aspect of individual(s) security. It can also be defined in objective and subjective context as well as previous forms of security. Corporate security in an *objective* context refers to the *absence of company's property, assets, employees, IT systems and rights endangerment*. On the other hand, corporate security in the *subjective* context refers to the *absence of fear that the company and its values will be endangered*. Corporate security can (or even must) be observed in the cyber world context. Therefore, it refers to *measured absence of company's endangerment* (objectively) i.e. *measure of fear regarding values endangerment* (subjectively). Notion and concepts tracking are evident for each security case including *measuring* i.e. ex post element of the cyber context.<sup>15</sup> Corporate security can partially be differentiated due to the size to large companies (usually identified as corporations) and small and medium enterprises as the most frequent and common business activity organization forms.<sup>16</sup> Security of companies or corporations regardless of their size is specifically positioned challenge within the cyber challenges' domain. However, the notion of corporate security is wider than cyber corporate security. Corporate security elements comprehend: (i) individual(s) security; (ii) physical security (property, assets, employees); (iii) IT security; (iv) corporate management; (v) crime detection and prevention; (vi) fraud identification; (vii) risk management and (viii) crisis management.

It seems that the most frequent corporate security *attack* form is the so-called DDoS or distributed denial of service. DDoS represents attack aiming to make online services unavailable by significant traffic increase towards the attack target from

---

<sup>15</sup> Measured absence of corporate endangerment is being gauged by endangering identification: physical attacks, IT attacks, DDoS attacks etc.

<sup>16</sup> Papers use the *corporate security* term regardless of the company type observation. Distinction necessary to be maybe in certain cases due to size and complexity of security challenges will emphasize company type.

various different sources.<sup>17</sup> It represents *threat* and *challenge* to important information publishing and access either by individual or by company. Targets are usually banks, news and information portals, while targets can also be any size and profile companies.

Security spectrum transformation has also led to emersion of numerous private *stakeholders* and *service providers*. However, inclusion of private institutions in the security and defence domain is not 21<sup>st</sup> century novelty. One of the examples even prior to the formal occurrence of the nation-state has been the East India Company.

Kaspersky Lab belongs to many of today's stakeholders and participants. They alongside B2B International analysed DDoS corporate attacks cost price on various company's size. According to their "*Global IT Security Risks Survey – Distributed Denial of Service (DDoS) Attacks*" such attacks cost is within USD 52.000 to USD 444.000 interval due to the company size. Aside the financial stability and/or development plans endangerment, authors believe that such attacks can also impact the *good will* i.e. company's reputation if they lead to partners or clients access loss to the company's online services. Furthermore, specific possibility and expenditure is also potential data loss. Respective potential losses gain significance due to size and scope of technology development and its everyday business usage. However, there are potential signs of caution regarding the overall research due to: (i) surveyed level i.e. certain potential defects regarding answers sincerity and preciseness and (ii) surveyors level i.e. such data identification *opens new markets* for Kaspersky like companies. The latter can be confirmed by simultaneous promotion of *Kaspersky DDoS Protection* solutions. Nevertheless, the notion of the potential results exists and even more important respective incidents impact and danger can be even higher due to: (i) hyper-digitalization i.e. increased interconnectedness and possibility that the Internet "*ceases to exist*" and (ii) DDoS package price on the black market. The first peril refers to the Internet usage for increased number of products and services. The respective refers to companies doing business in the traditional sector domain for which the Internet is significant for: (i) business (systems, data bases); (ii) sale (online trading systems) and promotion (social networks). In addition, according to Google's Erich Schmidt there is possibility that the Internet "*ceases to exist*". Schmidt primary believes that the Internet of Things (IoT) growth will impact the feeling of dynamism and melting of virtual and real world. The second peril refers to the current price of USD 150 for *DDoS package* on the black market. The respective price provides a weeklong denial of service. According to the study, overall expenditures point out several different potential problems companies might face. Moreover, the same company can face several different forms of expenditures.

DDoS attacks have several consequences. The most important one is temporary loss of access to critical and essential business information (61%). It is being followed by inability of doing core business (38%) and loss of business opportunities and con-

---

<sup>17</sup> [www.digitalattackmap.com](http://www.digitalattackmap.com)

tracts (33%). At the end, there is a negative corporate credit rating (29%) as well as insurance premium annuity (26%). However, an additional consequence occurs as post-incident reaction is always in the form of unplanned expenditure. According to the *Global IT Security Risks Survey* reactions of the companies were: (i) consultations with the security IT experts (65% of respondents); (ii) investments into corporate IT infrastructure modification (49%); (iii) lawyers expenditure (46%) and (iv) risk manager inclusion expenditures (41%). Nevertheless, those are not the only post-incident expenditures. It is possible to expect occurrence of *reputation loss* expenditure (38%) as well as *corporate image recovery* (30% of respondents). Respective is in particular important due to the high possibility of attack revealing to the partners and clients. According to the *Global IT Security Risks* attacked companies itself announce attack information (72%) whereas a significant percentage (43%) directly inform clients about the incident while relatively significant part informs official institutions (36%) and media (26%).

IoT devices are also one of the security issues. Their exponential increase from 3.8 billion devices in 2016 to 11.2 billion (or 294% increase) in 2018 or even projected 20.4 billion (82% increase) devices. Unimaginable projections of more than 20 billion devices connected to the Internet in the cyber world also mean expansion of the attack surface as well as interconnected transmission dots. Having in mind that IoT devices have not been essentially designed for security and with security features leads us to the conclusion they simply can be *entry points* and *transmission modes of the attack*. This is another angle of the new security but also techno-economic paradigm.

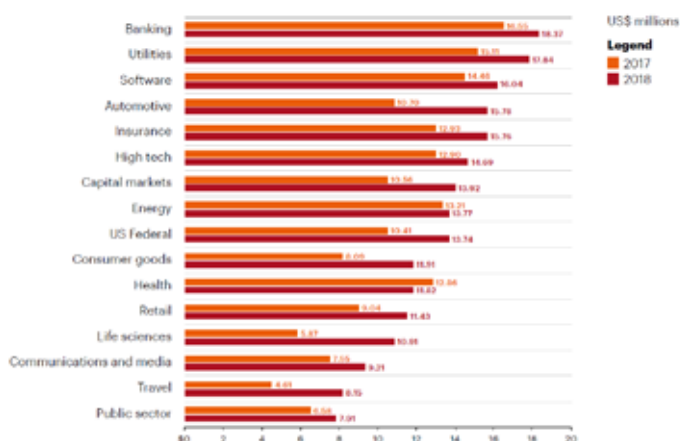
Important society security aspect is critical infrastructure protection. Information technology development impacted critical infrastructure observation as both, physical and tangible, but also cyber and intangible.<sup>18</sup> However, critical infrastructure proprietorship is important regardless of its form. Corporations own more than three quarters of critical infrastructure in developed economies. In US corporations own 80% of critical infrastructure (Cavanagh, 2004). Respectively, corporate security can significantly be observed as society's security. Private companies are service providers to many other companies and individuals. Respective services comprehend electrical energy production and distribution, transport including all forms, water supply, telecommunication services including the Internet, delivery services which mainly form critical infrastructure. Moreover, all respective forms of services and business sectors are *critically* connected to the Internet. The relationship primarily refers to business usage of the Internet, as well as impact to the usage process. Technological implications will have particular impact of certain sectors integration such is *drone* usage in delivery (already the agenda of several companies). Therefore, infrastructure security becomes individual(s) security due to inability of isolation.

---

<sup>18</sup> However, significant part of cyber infrastructure can be observed in physical context.

Observing the cyber-attack impact on corporate security and industries we can conclude that none of them is being fully safe and isolated. According to the recent US research it seems that the largest annual cyber-crime expenditure is in industries such as banking, infrastructure services, software, energy, insurance, high tech, health, automotive and capital market. In 2017, respectively these industries had an average annual expenditure of 16.55, 15.11, 14.46, 13.21, 12.93, 12.9, 12.86, 10.7 and 10.56 USD millions. Moreover, the 2018 data shows increase in each observed industry. The highest expenditures were in banking (18.37 USD millions), infrastructure (17.84), software (16.04), automotive industry (15.78), insurance (15.76), high tech (14.69), capital market (13.92) and energy sector (13.77).

**Figure 1:** Average annual cyber-crime cost price per industry in US

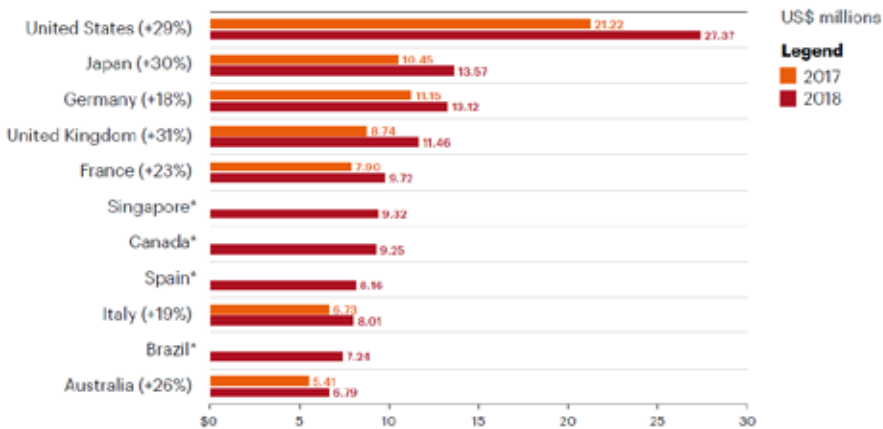


*Source: The Cost of Cybercrime, Accenture Security, 2019.*

Industries are not the only observation field. State level analysis has also been undertaken (figure 2). Analysis was conducted in the USA, Japan, Germany, UK, France, Singapore, Canada, Spain, Italy, Brazil, and Australia. Unfortunately, there are no available data for China and Russia which would provide a more comprehensive global overview. In all observed countries (excluding the four with only 2018 data) there been identified cost price increases. Three groups of countries can be identified based on respective data: (i) USA with expenditure over 20 USD millions per year, (ii) Japan and Germany with over 10 USD millions per year and (iii) remaining eight states within 5 – 9 USD millions range per year. The same approach for 2018 makes triple distinction: (i) USA with expenditure of over 25 USD millions per year, (ii) Japan, UK and Germany with over 11 USD millions per year and (iii) remaining seven states within the 6 – 9 USD millions range per year. It can be also

concluded that the level of economic development is *positively* correlated with the cost price per year.

**Figure 2:** Average annual cyber-crime cost price per states

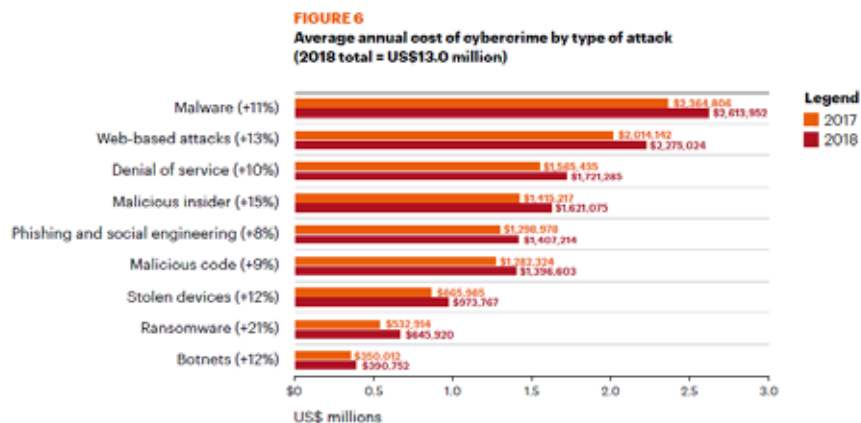


*Source: The Cost of Cybercrime, Accenture Security, 2019.*

Global level observation alongside certain available inputs limitations leads to the conclusion that there are several cost price scenarios. According to the CSIS cost price is USD 575 billion. On the other hand, McAfee and Lloyds estimate a cost price at 375 i.e. 400 USD billions. Certain calculations have been made by Juniper Research as well. Their estimation is at 2.1 thousand billion for 2019. Finally, IMF estimates cyber crime's financial global economy consequences as third in total, only after corruption and drug trafficking (Lewis, 2018).

DDoS has been previously used as an excellent example of attacks, new stakeholders and cost price increase. However, there are some other threat forms. According to the analysis the most expensive forms of threats i.e. attacks are malware, web-based attacks and DDoS, where the first two have cost price of 2.3 i.3 2.6 USD million in 2018, respectively. It is highly indicative that all attack forms and their cost prices are increasing. Moreover, it is indicative as to what are the attacks with the highest increase: ransomware with 21% increase, internal threats with 15% and web-based attack with 13% increase. Overall projected expenditure based on respective attacks in US accounted for 13 USD millions in 2018.



**Figure 3:** Average annual cost of cybercrime by type of attack

Source: *The Cost of Cybercrime, Accenture Security, 2019.*

## Cyber-security trends

The key cyber security challenges both on corporate and on an individual i.e. society level include: (i) products and services cybernetics; (ii) IoT existence and application; (iii) artificial intelligence. Companies already conduct significant part of their business on or by the Internet. Data archiving, financial data and reporting, products and services sale, invoicing, payments, autonomous vehicle driving, video surveillance, intra-corporate communication etc. have been conducted thanks to the Internet, applications and the cloud. An additional challenge is the existence of everyday use appliances which are connected to the Internet. It seems that such platforms provide background for Schmidt's thesis on ceasing the internet as we know i.e. its melting with the real world.

It is possible to expect higher and larger cybernetization and real and virtual world integration. And that is the biggest cyber security challenge. Increased vulnerability of private and business context demands increased defence as well as continuous improvement within cyber-real world. However, the essential question is the possibility of efficient ex ante defence.

Lewis (2018) believes that cyber-attacks will increase due to: (i) faster acceptance and adoption of new technology by criminals, (ii) increase of user numbers especially from less developed states with inadequate cyber security, (iii) increased levity of cybercrime execution, (iv) increased number of cybercrime centres, (v) additional cybercriminals sophistication enabling easier activities monetization, (vi) significant increase of IoT devices, (vii) potential AI usage, (viii) cloud expansion as well as

its usage in malware hiding and attack initiation. Even though cryptocurrencies are sometimes targeted as supportive tool for increased cybercrime this is probably not fully valid. One of the additional supportive mechanisms can be technological development itself, i.e. decreasing price and higher accessibility of cybercrime products (as shown in the DDoS package case).

Lewis also believes that nation-states are still the most dangerous and the most obvious cybercrime source. Financial resources, extensive human capital as well as certain legal protection are the key nation-state's motives.

The important question also is the impact of AI and robotization and their correlation with economy and security. It seems that robotization in the military context has positive first iteration impact on individual(s) security as well as on liberation from certain military field activities and decrease of human casualties. However, within second iteration and economic context it has negative impact due to dilemmas of distinction between military and civilian elements by the robot itself and its artificial intelligence. Robotization in the civilian business (even though the line is blurred) first has negative and afterwards relatively positive correlation. Negative correlation refers to jobs losses and socio-economic individual(s) security impact. Positive impact might be in restructuring of jobs, creation of currently unforeseen jobs and skills, as well as larger benefits to individuals both with respect to a more efficient and meaningful work and in the increase of leisure. However, the respective is also correlated and dependent on individuals, their knowledge and skills.

Machine learning includes deep learning as forms of artificial intelligence application and ability of the system to automatically learn and enhance from experience itself. The respective leads to decision making optimized for defined outcomes. Artificial intelligence in all its forms can be a defensive security challenge, but also it can be an applicable offensive security form. Artificial intelligence requires big data, computing power, as well as capable algorithm engineers. However, it also requires entrepreneurs, scientists, complementary industries, but also supportive public policies. The respective points out that current developed nation-states can be involved. Moreover, this field might be the new arena for superpower status both economically and military. Potentially it is a new Cold War but with some different competitors – US and China. Partially certain data proves respective pattern although not sufficiently. According to MSC, in 2019 US has invested USD 43 billion while China has invested USD 7 billion into AI.<sup>19</sup> Comparing with them the rest of the world has invested combined USD 8 billion into AI.

It seems that AI will reshape political and economic relations which will result in digital globalization consequences on states (Lee, 2018). Lee also believes that one of the AI race outcomes might be notion of further technological colonization. Having this in mind as well as AI's identification as one of the security challenges

---

<sup>19</sup> China's data might be undervalued due to the complexity of data validation. In any case, China will definitely increase its AI investments.

(MSC, 2019) it seems that AI driven challenges are not only military-security, but rather techno-economic.

### **Instead of conclusion**

Technological progress (re)shaped the world since its existence. Hand, stone, rope, wheel, powder, automobile, internal combustion engine, radar, sonar, the Internet, artificial intelligence etc. have been the impulses of change. Human civilization has previously absorbed many technology derived economic changes. Moreover, technological changes were the ones that continuously have created new paradigms, both in security and in economy. In addition, technological progress significantly multiplied development speed, and it is expected to grow even further and higher.

Advancement and technoeconomic changes directly impact and create cyber challenges. The respective changes alter concepts, definitions and paradigms of security, economic security, individual security, corporate security and other relevant sub-security domains as well as their intertwined and overlapping concepts. In addition, they redefine ratio and scope of security as well as define new “enemies” and challenges. It also shows that all additional technological advancement induces the new security threat. Therefore, Beck was apparently right, and increasing technology leads to increased risk. The respective has been proven throughout the concepts’ comparison as well as cause-effect relations and analysis. One of the important questions is if individual’s security has been affected by cyber-security challenges, why corporate security would be an exemption. Moreover, corporate security is probably the most targeted and vulnerable part of society due to importance of corporations and their consequential impact on individuals.

The rise and evolution of new cyber threats is also to be expected. It will probably become *new normal* like any other “revolution” which happened in the past. Furthermore, this means that also quest for solutions will be ever evolving. Current potential solutions might include: (i) basic security solutions implementation as well as defensive technology investments both on the device level and on the level of cloud technology; (ii) international cooperation in the legal application domain as well as the expansion of investigative power of agencies and institutions; (iii) cyber capacities strengthening in developing countries including all infrastructure forms; (iv) advanced data collection standardization of threats; (v) international community pressure towards every cybercrime supportive and financing country; (vi) global partnership of different stakeholders including private actors and interest groups. Majority of the proposals are valid and have contribution potential with respect to the traditional security definitions as to changed security definitions. However, some including international legal application as well as sponsoring-states pressure might be disputable due to: (i) attribution problem and (ii) interlaced interests of foreseen “pressure” states and some sponsoring states. Capabilities strengthening, defensive technology investments, as well as data collection standardization might be quite beneficial tools in each context. In addition, interest networks can be peered form of combat. Many cybercrime activities are network centric as well as network aimed. Therefore, similar counterpart can be defensively beneficial. All aforementioned require understanding about changed technoeconomic as well as the economic security paradigm.

Current technological changes such as cyber, artificial intelligence, machine learning, robotization etc. have a remarkable distinction – they are developing and evolving exceptionally fast with inevitable changes. Technological determinism, not as identical patterns and impacts context, but rather as *determined* change occurrence, has its valid position within

the new techno-economic paradigm. The respective paradigm has an additional correlation with corporations and their security, safety, and networks. Finally, it confirms patterns of both, technological changes, and each scientific revolution. As Kuhn noted every normal science existed as long as it was capable to deal with problems and challenges. Wherever current normal science failed, the scientific revolution continued and answered the challenges. However, ex post it also became the (new) normal science which as science in general has subjective value set of the scientists, researcher and cannot be value neutral. Why would technoeconomic and security paradigm be different?

## REFERENCES:

- Adler, Pol S. (2006): *Technological Determinism*, *The International Encyclopedia of Organization Studies*, ed. Clegg Stewart; Bailey, James R. (Sage)
- Bachmann, Sascha-Dominik (2011): *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21<sup>st</sup> century threats – mapping the new frontier of global risk and security management*, *Amicus Curiae Issue 88*
- Baldwin, David A. (1997): *The concept of security*, *Review of International Studies* 23, 5-26, British International Studies Association
- Beck, Ulrich (1992): *Risk Society*, Sage, London
- Benjamin, Walter (1942): *Theses on the Philosophy of History*, The Institute for Social Research, NY
- Benoit, Emile (1973): *Defense and Economic Growth in Developing Countries*, Lexington Books, Lexington
- Boot, Max (2006): *Technology, Warfare and the Course of History 1500-today*, Gotham Books, NY
- Brauch, Hans Gunter (2005): *Threats, Challenges, Vulnerabilities and Risks in Environmental and Human Security*, United Nations University, Institute for Environment and Human Security
- Buzan, Barry (1983): *People, States and Fear: The National Security Problem in International Relations*, Harvester Wheatsheaf
- Cavanagh, Thomas E. (2004): *Corporate Security Measures and Practices An Overview of Security Management Since 9/11*, The Conference Board, U.S. Department of Homeland Security
- Dreyer, Paul; Jones, Therese; Klima, Kelly; Oberholtzer, Jenny; Strong, Aaron; Welburn, Jonathan William; Winkelman, Zev (2018): *Estimating the Global Cost of Cyber Risk: Methodology and Examples* RAND Corp.
- Ejdus, Filip (2012): *Međunarodna bezbednost: teorije, sektori i nivoi*, JP Službeni glasnik i Beogradski centar za bezbednosnu politiku, Beograd
- Elzesser, Jirgen (2009): *Nacionalna država i fenomen globalizacije*, Jasen, Beograd
- Eriksson, Johan; Giacomello, Gianpiero; ed. (2007): *International Relations and Security in the Digital Age*, Routledge Advances in International Relations and Global Politics
- Goldstein, Joshua S (2003): *War and Economic History*, *The Oxford Encyclopedia of Economic History*, ed. Joel Mokyr, Oxford University Press, New York
- Harari, Yuval Noa (2018): *21 Lessons for the 21st Century*, Penguin Random House, NY
- Jovetić, Ivan (2013): *Implikacije tehnologije na politike i strategiju bezbednosti i odbrane*, International Scientific Conference - The Balkans Between Past and Future: Security, Conflict Resolution and Euro-Atlantic Integration, Ohrid, str. 559-572. Fakultet za bezbednost, Skopje

- Kay, Sean (2004): *Globalization, Power, Security*, Security Dialogue vol. 35, Sage Publications
- Kennedy, Paul (1989): *The Rise and Fall of the Great Powers*, Random House, New York
- Kuehl, Dan (2007): *The Information Revolution and the Transformation of Warfare*, in K. de Leeuw, ed: *The History of Information Security: a Comprehensive Handbook*, Amsterdam, Elsevier Science
- Kun, Tomas S. (1974): *Struktura naučnih revolucija*, Nolit, Beograd.
- Lee, Kai-Fu (2018): *AI Super-powers China, Silicon Valley and the new world order*, Houghton Mifflin Harcourt, Boston, New York.
- Lewis, James (2018): *Economic Impact of Cybercrime—No Slowing Down*, CSIS
- Liang (2011): *Shadow Networks: The Growing Nexus of Terrorism and Organized Crime*, Geneva Centre for Security Policy, GCSP Policy Paper no.20
- McCarthy, Daniel R (2015): *Power, Information Technologies, International Relations Theory*, Palgrave MacMillan, Hampshire
- Munich Security Report, MSC 2019.
- National Security Strategy of the United States 2010, [www.whitehouse.org](http://www.whitehouse.org)
- Nye, Joseph S. Jr (2011): *Budućnost moći*, MATE, Zagreb
- Pascual, Carolo; Elkind, Johnatan (2010): *Energy Security: Economics, Politics, Strategy and Implications*, The Brookings Institution, Washington
- Perkins, Džon (2012): *Ispovesti ubice ekonomije*, Plato, Beograd
- Perez, Carlota (2002): *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, Edward Elgar Publishing, Inc., Northampton
- Ponemon Institute, Accenture Security (2019): *The Cost of Cybercrime*
- Rice, Susan E.; Graff, Corinne; Pascual, Carlos: (2010): *Weak States and US National Security*, The Brookings Institution, Washington
- Tofler, Alvin; Tofler Hajdi (1998): *Rat i antirat*, Paidea, Beograd
- Vukotić, Veselin (2011): *Istorija budućnosti*, CID, Podgorica
- Waltz, Kenneth (1959): *Man, the State and the War*, Columbia University Press, New York
- Wolfers, Arnold (1952): "National Security" as an Ambiguous Symbol, Political Science Quarterly, Vol. 67, No. 4., The Academy of Political Science

Original scientific article

327.51(100-622HATO):336.5

355.45:336.5(497.7)

616.98:578..834]-036.22(100)

## NATO BURDEN SHARING POLICY AND COVID 19 IMPLICATIONS ON DEFENCE EXPENDITURES

Igor GJORESKI<sup>1</sup>

**Abstract:** *The aim of the paper is to evaluate the implementation of NATO policies, recommendations and guidelines in the field of defence expenditures in accordance with the Declarations and the accompanying documents from 2014 Wales Summit. The pledge to share 2% of GDP for defence expenditures and at least 20% of them on major new equipment aims to increase the Alliance's ability to meet the three core tasks arising from the 2010 Strategic Concept. At the same time, research and development (R&D) of new capabilities to respond to the rapidly changing threats and risks in the Euro-Atlantic area is a challenge not only for each Ally, but also for NATO as a whole entity. The paper provides an analysis of the implementation of the "2/20 pledge" policies and recommendations of the Alliance from the 2014 Wales Summit in view of meeting the guidelines to spend a minimum of 2% of GDP on defence by 2024 and 20% of it on major new equipment, including related R&D of new capabilities. A parallel of defence expenditures distribution by main categories has been made for the period 2013-2020. The main categories include operational expenditures (personnel, operations and maintenance) and capital investments in defence (equipment and modernization, and infrastructure). At the same time, the distribution of defence expenditures by main categories for the period 2013-2020 for the Republic of North Macedonia was analyzed in accordance with NATO methodology and data provided by the Ministry of Defence of North Macedonia. In addition, expert analyses related to COVID 19 implications and impact on the economic and GDP growth are presented. This COVID 19 implication is expected to have a certain positive or negative impact on defence expenditures in 2020, as well as in the following years. No matter which scenario prevails, experts agree that defence expenditure needs to maintain an upward trend not only as a percentage of GDP, but also in real terms. This is necessary not only for dealing with modern, rapidly growing and unpredictable threats to citizens' security and safety, but also for the economic recovery of the Allies from the COVID 19 effects.*

**Key words:** *defence expenditures, equipment, personnel, operations, COVID 19.*

### Introduction

The contemporary constellation of relations in defence and security has given a new dimension to the security challenges in 2020. This year, all countries in the world, including the members of the most powerful military-political alliance - NATO - have faced challenges related to dealing with the COVID 19 pandemic. The COVID 19 implications have had a posi-

---

<sup>1</sup> Associate Professor at Military Academy "General Mihailo Apostolski" Skopje, Republic of North Macedonia

tive or a negative impact on the projected economic and GDP growth of almost every member country of the Alliance. The intensified measures for protection against the outbreak of COVID 19, as well as the interruption of land, sea and air communications have influenced and affected the economic and GDP growth of the Allies in different ways. Most countries have adjusted their initial projections for the expected upward growth of their economy in line with the new challenges posed by COVID 19 and the restrictive measures they introduced to deal with it. Such corrections also affected the reduction of the projected GDP growth of the countries. The adjustments in the economic and GDP growth have also led to rebalances of the central budgets of the NATO members in order to provide additional budget funds in dealing with COVID 19.

The aftermath of the Pandemic and its second wave has left much to be desired and uncertainty about the future of economic growth, including defence expenditures. Most of the governments have introduced restrictive measures and at the same time sought ways to increase resources to meet the needs of the health sector and mitigate the fiscal implications for the economy caused by pandemic measures (Csernaton, 2020), as well as to project defence in those circumstances. The objective was to reduce public spending and support economy and citizens with more finance from the central budget.

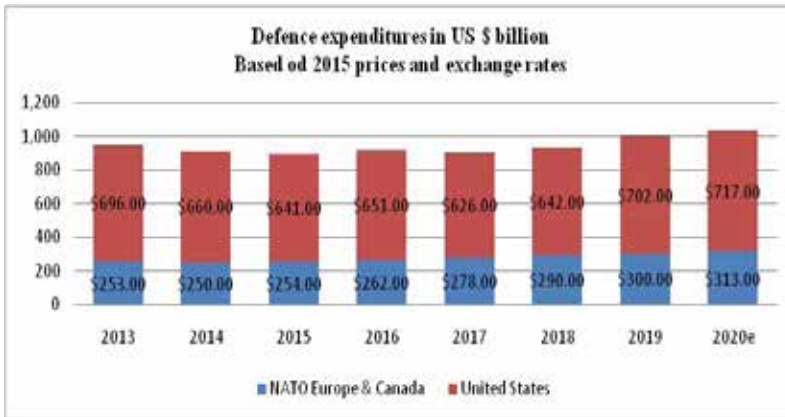
The experts and economists have proposed to find more money through limiting or reducing defence expenditures. This proposal will have a long term impact on the countries' resilience and will make them more vulnerable to other threats and risks, especially hybrid threats. According to the Wales Summit conclusions, all NATO members committed themselves to reach the level of defence expenditures of minimum 2% as a share of GDP in the next decade. The data clearly indicate that there was an upward trend in investing in defence expenditures in the years after the Wales Summit. It signals the commitment of NATO members to strengthen and more equitably distribute their contributions to collective defence (Hazen, 2020). It remains unknown whether this trend of defence expenditures increasing in accordance with the NATO guidelines from Wales will be maintained in 2020 and continue in 2021? However, many experts believe that COVID 19 will slow down this trend.

## **1. Burden Sharing in Alliance's Security**

To protect our freedom, we must continue to invest in our defence. All NATO Allies are increasing defence spending and more Allies are meeting the guideline of spending 2% of GDP on their defence. (...) Economically, politically and militarily, together we are stronger. (NATO Secretary General Jens Stoltenberg. Columbia University, New York, 26 September 2019.)

It is of great importance for the Alliance to ensure a fair burden sharing among Allies on defence expenditures, investment in capabilities, as well as in NATO-led operations, missions and activities. Threatened by Russia's expansionist policies and the annexation of Crimea, as well as China's growing influence in Europe, Allies agreed at the 2014 Wales Summit to adhere to the burden-sharing principle and continuously invest in development, procurement and maintaining of the capabilities necessary for the Alliance to defend its interests and citizens. Immediately following the Wales Summit, many of NATO's European allies and Canada began to gradually increase their defence expenditures. Globally, defence

expenditures in 2019 increased by 4% in real terms compared to 2018. In the same period, there was a 4.6% increase in defence spending in real terms among NATO European allies and Canada.

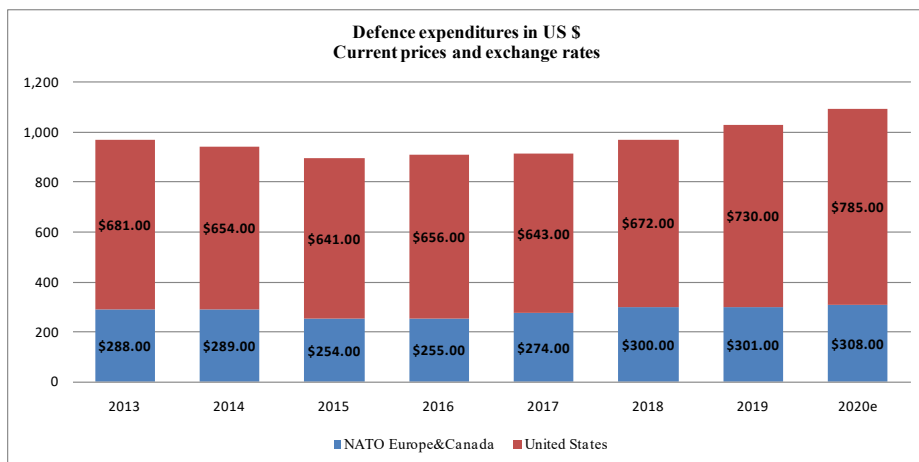


(Source: NATO Communiqué PR/CP (2019)123, 2019, p.4, and NATO Communiqué PR/CP (2020)104, 2020, p.4)

The analyzes of the member states' defence expenditures for the period 2013-2020 show that the US contribution to the Alliance's overall real costs is around 70%, while European allies and Canada account for 30%. Redistribution in terms of GDP is 52% at the expense of the United States and 48% at the expense of the European allies and Canada (The Secretary General's Annual Report 2019, 2020, p.39). In 2019, the Alliance's total real costs (based on 2015 prices and exchange rates) were around the amount of US \$ 1 trillion, while in 2020 they increased by nearly US \$ 30 billion and reached the amount of US \$ 1.029 trillion. The United States in 2020 allocated US \$ 717 billion from the overall Alliance's expenditures or US \$ 15 billion more compared to 2019. The European members and Canada allocated US \$ 300 billion in total for defence expenditures in 2019. The amount of these members increased by 13 billion in 2020 and amounted to US \$ 313 billion. Compared to 2018, the United States increased its contribution by US \$ 65 billion, and other European Allies and Canada increased their contribution by US \$ 10 billion (Marcus, 2020). Total US defence expenditures of US \$ 717 billion in 2019 include US \$ 60 billion for defence of their interests in the Pacific and Asia (Mesterhazy, 2018, p. 4). These expenditures have no real common interest of NATO's European allies.



The situation in real terms and in current price is as follows:



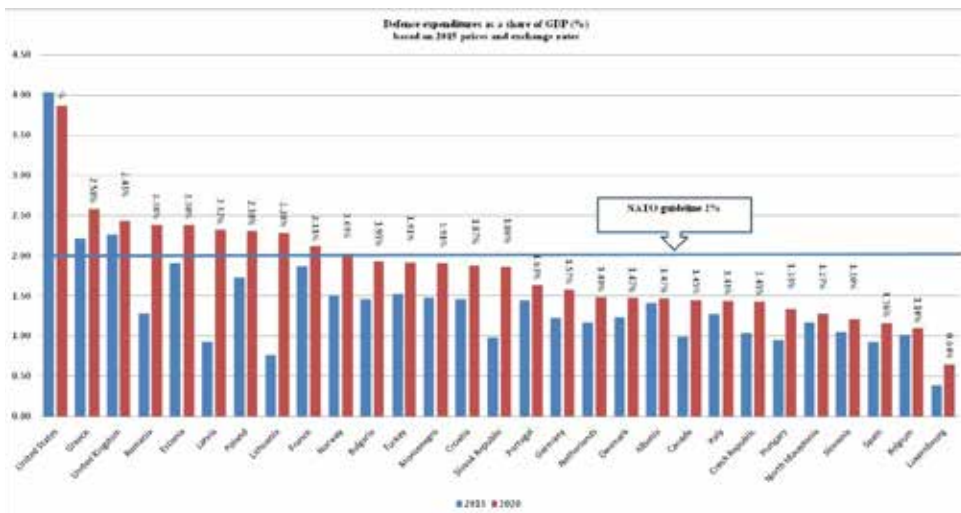
(Source: *NATO Communiqué PR/CP (2019)123, 2019, p.4, and NATO Communiqué PR/CP (2020)104, 2020, p.4*)

The figures in the Table show that European allies and Canada had lowest increase in defence expenditures in % in the period 2015-2016 by an average of 0.39% (Béraud-Sudreau and Giegerich, 2017), or in real terms the costs rose by just over US \$ 1 billion, while in the same period the United States increased its real costs by 2.29% or about US \$ 15 billion. Based on the Wales Summit guidance, the European Allies and Canada, in the period 2016-2020, cumulatively increased the defence expenditures in real terms by US \$ 130 billion. This trend is expected to go upward and Allies plans to increase defence expenditures to US \$ 400 billion by the end of 2024 (The Secretary General's Annual Report 2019, 2020, p.7).

### 1.1 *NATO Guidance of minimum 2% defence expenditures*

At the 2014 Wales Summit, Allies agreed to increase defence expenditures in real terms to 2% of GDP by 2024 (Wales Summit Declaration, 2014). The data show that only three members (USA, UK and Greece) allocated more than 2% of GDP until 2014, in 2018 three more allies reached that level (Estonia, Latvia and Poland), and in 2020 a total of 10 member countries (France, Norway, Lithuania and Romania) reached over 2% of defence spending in line with Wales guidance. Only the economy of Bulgaria did not follow this step and decreased its defence spending from 3.18% in 2019 to 1.93% in 2020. The United States is still leader in this regard with 3.83% of GDP defence spending. Greece is close behind with 2.58% and United Kingdom with 2.43%. Compared to 2013, the United States has reduced defence

spending from 4.03% to 3.87% of GDP and despite this percentage reduction, the increase in spending in real terms is US \$ 21 billion. All Allies have positive trend and constantly increase defence expenditures as a share of GDP. There are increases in defence spending among all the Allies in real terms. The situation with defence expenditures as a share of GDP for the period 2013-2020 is graphically presented in the Secretary General's Annual Report 2019 and in NATO Communiqué PR/CP (2020)104, 2020 as follows:



(Source: *The Secretary General's Annual Report 2019, 2020, p.40 and NATO Communiqué PR/CP (2020)104, 2020, p.3*).

Six years after the Wales Summit, there is still debate whether the expenditures as a share of GDP at minimum level of 2% is the right indicator of real defence spending? If we look at defence expenditures in real terms, we will notice that among the top 10 Allies that spend more in real terms for defence, only four have reached the level of minimum 2% share of GDP while the rest spend less than 2% of GDP. For example, defence expenditures of Greece as a share of GDP are 2.58% and it is second with the highest share of percentage, but according to defence expenditures in real terms Greece is in the thirteenth place. On the other hand, the defence expenditures of Canada as a share of GDP are 1.45%, and according to defence expenditures in real terms Canada is in the sixth place. The situation of defence expenditures in real terms in the period 2014-2020 for NATO member countries based on 2015 prices and exchange rates in millions of US \$ is as follows:

Million US \$ (based on 2015 prices and exchange rates)					
Defence expenditures real change 2014-2020					
	2014	2020	Real change 2014 - 2020	Share of real GDP (%) 2014	Share of real GDP (%) 2020
United States	660,062	716,886	8.61	3.73	3.87
United Kingdom	61,316	67,236	9.65	2.14	2.43
Germany	39,222	52,918	34.92	1.19	1.57
France	43,931	48,817	11.12	1.82	2.11
Italy	20,786	24,299	16.90	1.14	1.43
Canada	15,562	22,377	43.80	1.01	1.45
Turkey	11,784	18,015	52.87	1.45	1.91
Spain	10,607	13,635	28.55	0.92	1.16
Poland	8,521	12,077	41.74	1.85	2.30
Netherlands	8,649	11,460	32.49	1.15	1.48
Norway	5,862	7,798	33.03	1.55	2.03
Belgium	4,400	4,919	11.80	0.97	1.10
Greece	4,355	4,915	12.87	2.20	2.58
Romania	2,309	4,863	110.62	1.35	2.38
Denmark	3,399	4,633	36.31	1.15	1.47
Portugal	2,562	3,263	27.36	1.31	1.63
Czech Republic	1,686	2,723	61.48	0.95	1.43
Hungary	1,032	1,793	73.75	0.86	1.33
Slovak Republic	832	1,668	100.53	0.99	1.86
Bulgaria	640	1,040	62.66	1.31	1.93
Lithuania	357	1,000	179.88	0.88	2.28
Croatia	892	949	6.39	1.85	1.87
Latvia	245	651	165.55	0.93	2.32
Estonia	432	596	37.98	1.92	2.38
Slovenia	411	552	34.40	0.97	1.20
Luxembourg	212	391	84.67	0.38	0.64
Albania	150	181	20.94	1.35	1.47
North Macedonia	105	136	29.10	1.09	1.27
Montenegro	59	86	44.98	1.50	1.91

(Source: *The Secretary General's Annual Report 2019, 2020*, p.120 and *NATO Communiqué PR/CP (2020)104*, 2020, p.9).

In terms of defence spending allocated by countries in real terms, it can be concluded that the United States is the first on both bases, followed by the United Kingdom with 2.43% of GDP or over US \$ 67 billion, while France with 2.11% of GDP provides over US \$ 48.8 billion and is in the fourth place. According to NATO, the defence expenditures of Germany are 1.57% as a share of GDP and it is the third major contributor in real terms with around US \$ 53 billion. In real terms, Germany increased its defence expenditures by 9.7% in 2019 compared to 2018 (Marcus, 2020). In other words, Germany increased its defence expenditures as a share of GDP from 1.19% in 2014 to 1.57% in 2020, or in real terms the increase is more than US \$ 15.5 billion, and it is the second major increase after the United

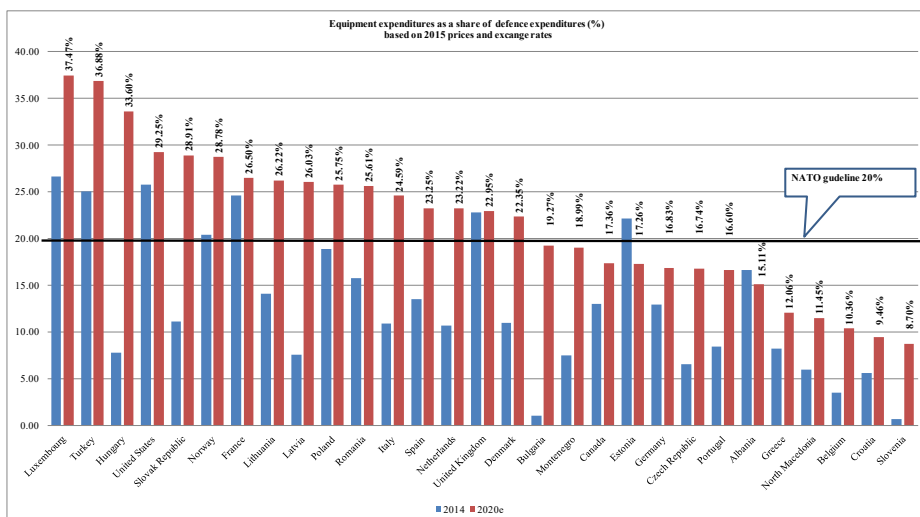
States. Nevertheless, Germany's policy of increasing its defence spending has been sharply criticized by the United States. The US Secretary of Defence Esper, during his visit to Brussels in June 2020, reaffirmed NATO's 2014 Wales policy, and said: "I continue to urge all of our allies to meet their target goal of 2% of GDP. We've moved a good distance here in the last few years but there's much, much more we need to do to ensure our collective security." In support of Germany's policy on defence spending, German Chancellor Merkel said: "We in Germany know that we have to spend more on defence; we have achieved considerable increases in recent years, and we will continue on that path to enhance our military capabilities" (as in Cook, 2020). In line with Chancellor Merkel, the German Defence Minister Annegret Kramp-Karrenbauer warned that "looking at the percentage of a country's GDP spent on defence is an increasingly insufficient measure of commitment to the NATO military alliance" (Kramp-Karrenbauer as in DW, 17.07.2020). Commenting upon Kramp-Karrenbauer's statement, the Ministry's Parliamentary State Secretary Peter Tauber said: "while Germany aims to allocate around 2% of overall GDP to defence, as previously agreed by NATO members, the country currently provides around 10% of the alliance's military capabilities".

The largest percentage increase in defence expenditures in the period 2014-2020 was made by Lithuania with an increase in real terms by almost 180%, followed by Latvia with an increase of over 165%, Romania with over 110% and the Slovak Republic with over 110%. In the same period, three of the top ten largest contributors in real terms increased costs minimally, the United States by 8.61%, the United Kingdom by 9.65% and France by 11.12%. From the top ten NATO contributors in real terms, the largest increase in this period was noted in Turkey by 53%, followed by Canada by 44%, Poland by 42%, and Germany by 35% (NATO Communiqué PR / CP (2020) 104, 2020, p.9).

## 1.2 Equipment, Research and Development

The second segment of the 2014 Wales Summit pledge is for all Allies to provide an allocation of at least 20% of defence spending to new major equipment, and R&D in new capabilities. Significant progress has been made by the Allies in this regard. In 2020, 19 Allies invested more funds in equipment than in 2019 (NATO Communiqué PR / CP (2020) 104, 2020, p.13). A total of 16 member states followed the Alliance's guidelines and reached the level of distribution of defence expenditures with at least 20% for new major equipment. The data show that the Allies are not only investing in capacity development, but also in improving the readiness, deployability, sustainability and interoperability of their forces in line with the Alliance Capabilities Targets (The Secretary General's Annual Report 2019, 2020, p.47 ).

The distribution of the defence expenditures by major equipment and R&D in new capabilities for 2014 -2020 period is as follows:



(Source: NATO Communiqué PR / CP (2020) 104, 2020, p.3 and p.13)

In 2019, the largest percentage for new major equipment and R&D for new capabilities was allocated by Bulgaria, an incredible 59% compared to 9.65% in 2018 and represents an increase in this category by over 600%. In 2020, most funds for equipment and R&D for new capabilities are allocated by Luxembourg with 37.5%, followed by Turkey with 36.9% and Hungary, which increased investments in equipment from 23.81% in 2019 to 33.6% in 2020. In 2020, the United States spent 29.25% of its defence expenditures on new major equipment and R&D. Convincingly at the bottom of the list are Slovenia with 8.7% and Croatia with 9.46% allocation of funds for new equipment. It is evident that almost all countries are gradually increasing investment in new equipment and weapons systems and in modernization of the existing equipment, including R&D for new capabilities (NATO Communiqué PR / CP (2020) 104, 2020, p.13). A decrease in this category of defence expenditures in 2020 was noted in Bulgaria, which reduced the funds for this purpose from 59% to 19%, followed by the Slovak Republic, which allocated 40% in 2019 and in 2020 reduced the spending to 28.9%, then Lithuania which allocated 37.5% in 2019 and a year later reduced it to 26.2% (NATO Communiqué PR / CP (2020) 104, 2020, p.13). In this category, European allies and Canada spent about US \$ 66 billion in 2019 (The Secretary General’s Annual Report 2019, 2020, p.41).

### 1.3 Investment in infrastructure

Regarding investment in Infrastructure, data indicates that in 2020 Luxembourg is the leader in this category with 11%, followed by Montenegro with 8.3%, Estonia and Latvia with 7.93% and the Czech Republic with 7.80%. The other countries have investment below 6%, while the United States allocates 1.33% in this category. Portugal has the lowest investment in this category in 2020 with 0.19%.

Distribution of defence expenditures by main category (%) - Infrastructure

	2013	2014	2015	2016	2017	2018	2019	2020e
Albania	1.17	0.86	1.40	1.37	0.92	1.09	1.64	2.93
Belgium	2.28	1.81	0.93	0.96	1.05	1.43	1.19	1.60
Bulgaria	0.47	0.63	1.27	0.63	0.83	2.62	1.09	6.87
Canada	4.12	3.81	3.63	3.03	2.98	3.58	2.75	3.73
Croatia	1.21	1.24	1.98	1.26	3.59	1.00	1.41	1.65
Czech Republic	2.72	2.34	3.32	3.91	3.99	5.31	7.04	7.80
Denmark	1.16	0.97	1.09	2.16	1.95	1.49	1.74	2.44
Estonia	11.54	8.20	8.45	12.15	11.27	8.63	6.13	7.93
France	2.30	2.33	2.80	2.70	2.88	3.51	3.12	2.87
Germany	3.55	3.75	3.60	3.39	4.06	4.15	3.99	3.66
Greece	0.63	1.10	0.65	0.58	0.79	0.62	0.66	1.26
Hungary	2.32	1.07	1.21	1.13	1.64	4.85	3.50	3.07
Italy	1.57	1.40	1.30	0.70	0.94	1.92	0.67	1.65
Latvia	6.26	8.89	6.64	12.83	15.02	6.97	10.30	7.93
Lithuania	2.04	2.17	2.16	3.59	3.92	2.24	2.40	4.87
Luxembourg	11.81	10.26	7.79	6.64	4.64	5.05	3.16	10.99
Montenegro	0.09	0.96	2.47	2.41	0.88	2.24	1.42	8.30
Netherlands	2.74	4.77	3.19	3.90	3.02	3.46	3.29	3.28
North Macedonia	1.74	1.24	1.67	1.28	1.01	0.95	3.89	2.70
Norway	5.33	5.71	5.30	6.56	6.93	6.67	6.44	6.95
Poland	5.62	5.47	4.74	4.62	4.21	3.45	5.27	5.09
Portugal	0.04	0.11	0.25	0.06	0.03	0.12	0.11	0.19
Romania	1.16	1.09	1.27	2.77	2.09	1.54	3.53	4.91
Slovak Republic	0.29	0.57	1.99	3.75	2.97	2.00	1.17	2.16
Slovenia	1.33	0.65	0.61	1.14	0.45	1.40	0.57	1.84
Spain	0.67	0.66	0.97	0.97	0.68	0.64	0.98	1.21
Turkey	2.72	2.77	2.56	2.42	2.95	2.53	2.04	3.08
United Kingdom	2.04	1.95	1.63	1.87	2.25	2.99	2.11	1.70
United States	2.08	1.71	1.45	1.22	1.23	1.77	1.28	1.33

(Source: NATO Communiqué PR / CP (2020) 104, 2020, p.14)

### 1.4 Contribution to operations

In the category Other, which covers the costs related to operations and maintenance in 2020, the United Kingdom and Estonia allocate the most funds with 41.39% and 40.48% respectively. The United States allocates 32.04% in this category of expenditures. The largest increase in resource allocation in this category, compared to 2019 was noted in Luxembourg and Bulgaria with 8% each, Spain with 7%, and Belgium with 6%. The changes range up to +/- 2% increase / decrease in costs in other countries.

The percentage distribution for the category operations and maintenance in the period 2013-2020 by country is as follows:

Distribution of defence expenditures by main category (%) - Operations and Maintenance								
	2013	2014	2015	2016	2017	2018	2019	2020e
Albania	7.3	14.44	11.53	22.57	23.92	18.79	20.86	22.31
Belgium	17.53	16.83	17.4	17.52	17.23	17.72	19.36	25.44
Bulgaria	29.64	25.51	21.6	24.57	22.74	24.74	9.74	17.89
Canada	32.28	32.26	32.14	33.25	28.95	33.46	34.68	31.51
Croatia	20.01	16.65	17.73	15.83	18.99	18.67	18.33	17.19
Czech Republic	25.75	29.73	29.65	27.43	28.35	28.95	25.39	25.16
Denmark	35.84	36.78	35.4	34.65	40.66	36.97	32.01	29.83
Estonia	34.14	31.03	39.18	31.30	34.62	40.36	44.20	40.48
France	19.91	24.43	24.37	24.92	24.97	25.92	26.61	26.43
Germany	33.84	32.63	34.61	36.05	35.20	35.49	36.06	37.61
Greece	12.75	13.55	16.90	12.84	11.37	9.60	9.96	11.05
Hungary	37.64	41.10	40.83	35.84	40.62	34.82	37.54	26.83
Italy	10.93	11.27	11.42	9.42	10.80	11.30	12.11	11.61
Latvia	28.68	30.59	29.69	24.25	31.38	27.63	34.51	29.08
Lithuania	22.2	26.24	27.79	20.85	23.67	23.30	20.01	24.43
Luxembourg	22.52	17.82	16.11	17.73	18.90	16.35	16.37	24.21
Montenegro	10.91	13.06	14.07	17.80	13.73	13.84	11.60	13.50
Netherlands	26.16	28.05	30.14	30.20	30.04	28.99	27.14	25.05
North Macedonia	23.11	23.18	19.53	22.21	20.53	19.52	20.36	23.20
Norway	33.88	33.24	32.90	31.46	31.36	31.30	30.06	30.12
Poland	22.78	24.24	20.11	26.61	23.71	22.89	22.73	22.20
Portugal	11.46	10.19	9.15	8.61	8.35	15.26	11.60	17.80
Romania	9.13	11.98	15.78	11.79	9.90	10.50	12.99	16.38
Slovak Republic	22.19	19.16	23.49	22.22	21.08	20.99	17.95	19.86
Slovenia	16.88	16.38	15.31	21.80	20.47	20.36	23.23	22.92
Spain	18.71	18.5	19.03	19.78	17.28	17.89	16.14	23.09
Turkey	15.8	15.27	15.49	14.43	15.73	14.65	12.61	12.79
United Kingdom	38.22	38.63	39.82	41.62	40.92	41.00	40.97	41.39
United States	37.72	36.87	36.51	28.73	31.83	32.49	32.28	32.04

(Source: NATO Communiqué PR/CP (2019)123, 2019, p.14, and NATO Communiqué PR / CP (2020) 104, 2020, p.14)

### 1.5 Personnel

Regarding personnel expenditures, there are variations from country to country, but the global tendency is for these costs to continuously decrease and reach the level of up to 50% of defence spending. In more detail, the situation in personnel expenditures in the period 2013-2020 is as follows:

Distribution of defence expenditures by main category (%) - Personnel								
	2013	2014	2015	2016	2017	2018	2019	2020e
Albania	75.25	68.05	78.15	68.05	68.20	70.70	62.89	59.65
Belgium	77.34	77.84	78.23	76.80	75.52	70.69	68.38	62.61
Bulgaria	65.37	72.84	73.66	65.64	68.33	62.99	29.42	55.96
Canada	52.44	50.90	53.76	53.11	57.37	51.02	47.77	47.39
Croatia	68.06	76.55	72.28	75.40	71.72	76.96	73.71	71.71
Czech Republic	62.03	61.40	55.27	61.97	56.11	54.57	53.16	50.30
Denmark	51.74	51.27	52.01	49.51	47.01	49.88	48.19	45.39
Estonia	39.83	38.62	39.56	38.70	34.89	34.27	34.18	34.33
France	49.23	48.59	47.79	47.94	47.98	46.90	45.81	44.20
Germany	49.86	50.67	49.86	48.35	48.96	47.99	45.26	41.89
Greece	74.56	77.18	72.05	73.13	76.56	78.76	76.88	75.63
Hungary	48.96	49.77	48.21	49.66	42.41	39.98	35.14	36.50
Italy	75.00	76.41	77.55	70.79	67.58	65.66	70.21	62.15
Latvia	52.98	52.97	50.06	43.87	38.59	34.21	33.53	36.95
Lithuania	66.53	57.53	48.49	45.50	40.79	37.47	40.02	44.47
Luxembourg	51.10	49.31	42.77	45.56	34.40	33.42	30.76	27.33
Montenegro	87.68	78.53	78.03	75.32	80.44	72.87	72.89	59.21
Netherlands	58.53	56.50	55.51	51.77	52.19	51.16	48.07	48.45
North Macedonia	67.76	69.66	67.66	68.14	72.00	68.45	61.93	62.65
Norway	42.21	40.64	39.96	38.60	37.08	36.43	34.23	34.16
Poland	57.70	51.45	41.96	47.15	50.04	46.14	47.77	46.96
Portugal	79.85	81.27	81.90	81.38	80.19	74.84	71.67	65.41
Romania	78.99	71.15	63.30	65.01	54.67	54.48	57.90	53.09
Slovak Republic	70.14	69.14	56.24	58.72	58.21	54.74	40.81	49.07
Slovenia	80.52	82.31	82.23	76.03	75.04	72.38	69.09	66.53
Spain	68.25	67.34	65.18	72.61	61.64	59.64	61.86	52.45
Turkey	54.58	56.88	56.82	57.60	51.02	45.18	46.75	47.26
United Kingdom	37.85	36.59	36.80	35.27	34.35	33.82	34.07	33.95
United States	34.38	35.45	36.64	45.01	41.22	39.28	38.93	37.38

*Source: (The Secretary General's Annual Report 2019, 2020, p.124, and NATO Communiqué PR / CP (2020) 104, 2020, p.13)*

The data provided by NATO indicates that only Greece maintains a certain continuity in these spendings of over 70% and in 2020 it allocated 75.32%. Croatia with 71.71% is one step behind Greece and is the second in the distribution of expenditures in this category. The largest increase in personnel spendings was noted in Bulgaria, which increased its personnel expenditures from 29.42% in 2019 to 55.96% in 2020. Also, an increase of just over 8% was noted in the Slovak Republic, which increased personnel expenditures from 40.81% in 2019 to 49.07% in 2020. A total of 6 member states (Norway, USA, UK, Latvia, Hungary and Estonia) allocate less than 40% for personnel expenditures and all of them allocate a minimum of 2% as a share of GDP for defence expenditures. Luxembourg with 0.64% as a share of GDP allocates only 27.33% for personnel. The United States allocates 37.38% of its total defence expenditures for this purpose.

## 1. COVID 19 Implications on Allies' Economic Growth and Defence Expenditures in 2020 and Beyond

In the run-up to the Pandemic in March 2020, the NATO Secretary-General Jens Stoltenberg was very careful about the COVID 19 implications on the economies and



projected GDP growth, as well as on the defence expenditures of Alliance member countries. The general conclusion is that the COVID 19 crisis will have severe consequences on government budgets, but it also reinforces the critical need to continue investing in defence and security. Stoltenberg said that: “There will be severe economic consequences of the coronavirus crisis... And in the short term, consequences not only for the total economy, but for government budgets. When we think about long-term consequences, it is too early to say anything with certainty. You have to remember that when NATO allies agreed to invest more in defence, they did so because we live in a more uncertain, unpredictable world. This has not changed; I expect allies to stay committed to investing more in our security. We also need to remember that by investing more in our security and armed forces, we’re providing surge capacity for all our societies to deal with unforeseen events, crisis and natural disasters, as we, for instance, see now” (Aitoro, 2020).

The World Bank forecasts from June this year are that in 2020 global economy is expected to decline by - 5.2%, which is the greatest recession in the last 80 years. The most developed economies are expected to have the largest impact and the decline of their economies would be around -7%. The US estimates that their economy is expected to decline to -6.1% (World Bank, 2020a, p.8). Developing economies and emerging markets are expected to have the least consequences with a -2.5% decline in the economy (Severieva, 2020). On the other hand, the revised forecasts of the International Monetary Fund (IMF) from May to June 2020 indicate that world economy will record a global decline of -3.3% at the end of the current year (IMF, 2020a, p.20). The IMF forecasts in October imply that world economy will decline by as much as -4.4%, and world’s most developed economies will experience a decline of as much as -5.8% (IMF, October 2020b). The consequences of COVID 19 regarding the economies of European NATO allies indicate that GDP in general declined from -7.5% up to -12% in the first two quarters of 2020. Preliminary data for the third quarter show a decline in GDP in some countries by -12.7%, especially those countries that in previous years had high revenues from tourism. Translated into Alliance defence expenditures, this means, depending on the scenario, a reduction in defence budgets from US \$ 21 billion to US \$ 56 billion by 2020 (Fiott, Terlikowski & Schütz, 2020). These estimates for a possible reduction in defence expenditures are several times higher compared to the economic crisis in 2009, when the budgets of NATO member states from Europe were reduced by about US \$ 10 billion. NATO’s European allies lose about \$ 24 billion in defence expenditures over six years of economic recovery (Fiott, 2020).

The baseline projections of economic growth, including those related to defence expenditures, are directly related to estimates as to how long the Pandemic crisis and the recession in the economies will last. Predictions go in two different directions (pessimistic and less pessimistic) as to how long the Pandemic crisis will last. According to the pessimistic forecast, if the crisis lasts for a long period of time and the number of infected people increases in large numbers, then the countries may decide to re-

impose post-lockdown measures (social distancing and more effective testing, tracing, and isolation practices). Such measures will again affect the reduction of economic and GDP growth of countries. In this case, the recovery will be significantly weaker, with a major shock to the financial market and widespread bankruptcy of countries in the group of new markets and emerging economies. The less pessimistic predictions are that the pandemic will spread at a slower pace and the number of infected will be lower, so that economic growth could begin immediately after the easing of COVID 19 measures (IMF, 2020a, pp. 13-15). However, in order to realize this forecast, appropriate fiscal and monetary policies of the countries are needed to help the economy in order to restore the trust of consumers and investors (World Bank, 2020, pp.79-80).

The consolidation of the economies will depend on which scenario will take place in reality and this will be reflected in the growth or in the reduction of defence expenditures. The lessons learned from the past financial crises indicate that the overall fiscal implications and effects of COVID 19 are expected to manifest on government spending policy in the years after 2020. Hence, the commitment to defence expenditures of minimum 2% as a share of GDP is likely to remain. The real resources available to countries will be projected according to the adjusted GDP and the declined economic growth. This means that in the coming years there will be less money in real terms. The defence expenditures of NATO's European allies will require greater efficiency. Despite the pessimistic and less pessimistic forecasts related to defence expenditures reduction, the final data for 2020 will still be most accurately known at the end of the fiscal year. Compared to the major financial crisis of 2008 which resulted in a GDP decline in 2009, the largest reductions in defence expenditures occurred in 2012 and 2013. However, it is logical to expect similar implications related to defence expenditures in the years following the end of the Pandemic (Fiott, Terlikowski & Schütz, 2020). In the case of the 2008 economic crisis, European Allies had to reduce defence expenditures from 1.45% to 1.69% of GDP on average in the period 2009-2013. After 2014, there was a slow gradual increase of their defence expenditures and they reached the level of an average of 1.5% of GDP in 2018 (Mesterhazy, 2018, p.8). This means that three years of stagnation and reduction were followed by three years of recovery and an increase in defence expenditures. It is noteworthy that a year before the reduction in defence expenditures, i.e. in 2011, they reached a record level of US \$1.55 trillion globally. It took five years for defence expenditures to return to US \$ 1.56 trillion in 2016 (Barrie, Childs, McGerty, 2020).

No one can say for sure how long European economies and defence expenditures could take to recover after COVID 19. The previous 2008-2009 economic and financial crisis took almost six years to reverse savage cuts, but the increase in spending only occurred in 2014 because of Russia's invasion of Ukraine. In the case of COVID 19, NATO and its European allies do not have six years to revitalize their economies and defence expenditures. They must act quickly. The experience teaches us that reduction of defence expenditures will not increase resistance to security threats to NATO's

European allies. The reduction of defence expenditures will have a strong impact on the implementation of equipping plans of the armed forces of the Allies. This could call into question the Alliance's forces readiness and its ability to respond quickly to security threats. This is an exceptional challenge faced by almost all Allies, especially in the part of implementation of the Capabilities Targets requirements. Having in mind the current cuts in defence expenditures, this is a challenging issue for each Ally and everyone is looking for a way to solve it most painlessly and respond appropriately to the COVID 19 challenges (Fiott, Terlikowski & Schütz, 2020).

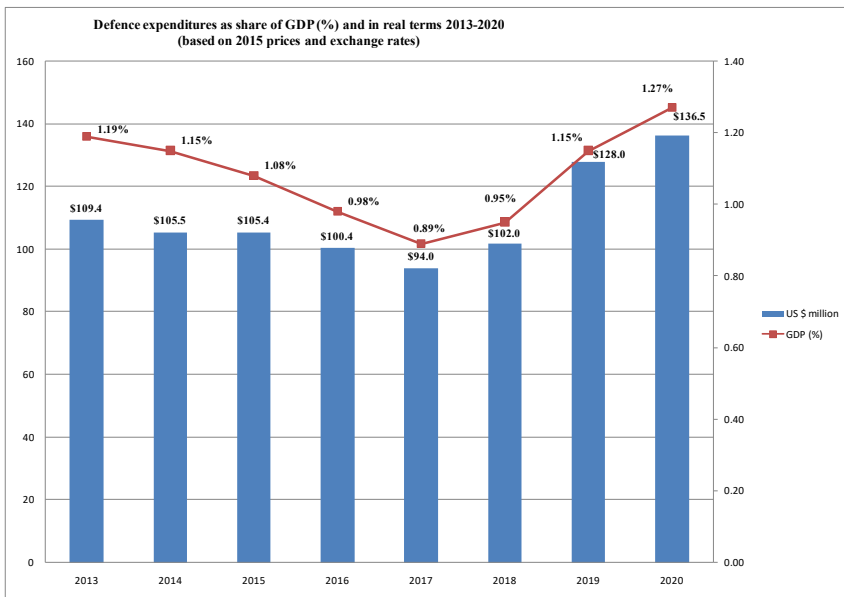
As simple as it may sound, the range of security challenges facing Europe today is broader and more complex by magnitude than in 2008. The events that have taken place on the political scene in the last decade are closely linked to the rapidly growing and unpredictable security threats to Europe, Russia's revisionist policy and the annexation of Crimea, failed and failing states in Europe's neighborhood, the menace of terrorism, the adverse effects of climate change, hostile activity in cyberspace, unregulated migration and a more assertive China (Fiott, Terlikowski & Schütz, 2020). All of them are sufficient indicators for Europe to take more comprehensive measures to strengthen its role on the international stage. Dealing with the current challenges is an argument plus for NATO's European allies in the fight to keep defence expenditures growth in life. This means that no one can afford the luxury of 5 to 6 years to recover as it was the case with the 2008-2009 recessions. If there were a drastic reduction in defence expenditures, then it would have a strong impact on the security on European soil and beyond. The fear of such a scenario is justified because the effects of the Pandemic make the world even more insecure, unstable and interdependent, and they can strongly affect the security, stability, democratic values and interests of NATO's European allies. There are fears that defence expenditures cuts by Allies will not only increase Europe's dependence on transatlantic members, but will also significantly undermine the burden-sharing principle and can make European allies dependent on "third countries" and "will significantly undermine the credibility of European nations as military partners within NATO."

In this case, the positive dimension of the Pandemic has shown us that we should not always look only at the military dimension of defence expenditures, but we should also consider the civilian dimension. It is a strong argument in the fight to justify the growth of defence expenditures. One of the recommendations of the 2016 Alliance Summit in Warsaw is the need to build a "resistance" of the entire society to security threats. It also calls for a "Whole of Government Approach" in dealing with crises and emergencies. In the case of the Pandemic, the facilities and capabilities of the armed forces were used to deliver medical supplies, transport patients and support the civilian authorities in providing hospital facilities by adapting military facilities for the temporary care of the infected, and so on. In this particular situation, armed forces were deployed on the ground to assist where they were most needed, where civilian authorities did not have sufficient capacity to deal with the health crisis. In addition to

using weapons, soldiers now know how to deal with the Pandemic and thus contribute to defence and deterrence. These arguments should be taken into account in discussions on defence expenditures cuts as more appropriate.

## 2. Defence Expenditures of the Republic of North Macedonia 2013- 2020

North Macedonia has a consistent policy regarding stable and long-term investment in defence expenditures. Defence expenditures have been relatively stable for the last 10 years, at about US \$ 105 million a year, which roughly equates to 1% as a share of GDP. This figure has fallen from 2.15% of GDP in 2007, for a number of reasons, including the global financial crisis. Funding over recent years has been barely sufficient to maintain current defence assets, but not to develop them as planned (SDR, 2018, p. 29). Defence expenditures expressed as % of GDP and the actual expenditures for the period 2013-2020 calculated in real terms in US \$ based on 2015 constant prices and exchange rates are graphically presented as follows:



*(Source: Ministry of Defence of the Republic of North Macedonia, 2020)*

Several measures have been taken to meet the Alliance recommendations and guidance in the field of stable and long-term defence expenditures at the level

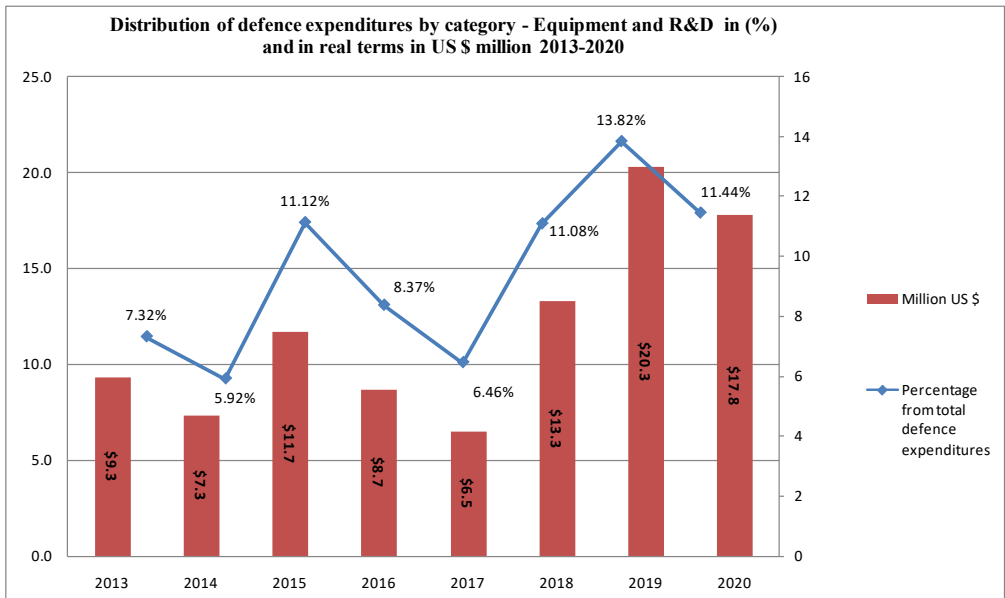
of minimum 2% as a share of GDP and allocation of funds of at least 20% for new major equipment and R&D of new capabilities. In July 2018, the Government adopted the Strategic Defence Review 2018 which provides recommendations for achieving stable and long-term financing of defence expenditures in line with the 2014 Wales Summit guidance. The policy of the Government is to reach this projection by 2024 through a continuous increase in defence expenditures by 0.2 percent each year starting from 2019. Based on a detailed macroeconomic projection from the Ministry of Finance for the national GDP growth rate, the Ministry of Defence made a projection of defence expenditures for the period 2019-2028 as a share of GDP. These projections are elaborated in detail in the Long-Term Defence Capabilities Development Plan 2019-2028 (LTDCDP 2019-2028). This plan was approved by the Government in May and endorsed by a Resolution of the Assembly in June 2019. The defined defence expenditures according to LTDCDP 2019-2028 will be the basis for financing the missions, tasks and activities set out in LTDCDP, the projected organizational-formation structure of the MoD and the Armed Forces, the undertaken international obligations to participate in operations and missions, the undertaken obligations to meet the requirements of the Capability Goals in terms of capability development, and forces, including the need for new major equipment and modernization of the armed forces (LTDCDP 2019-2028, 2019, pp.70-71).

The data indicate that the upward trend of defence expenditures increase began in 2019 in accordance with the planned projections in LTDCDP 2019-2028. Thus, shows that defence expenditures from 0.95% in 2018 increased by 1.15% as a share of GDP in 2019. In 2020, defence expenditures reached 1.37% of GDP. However, as a result of the implications of the COVID 19 in May 2020, defence expenditures were reduced to 1.27% of GDP, or in real terms they were reduced by US \$ 29 million. The reduction in real terms covered the non-essential costs, but it was mostly reflected in the category of equipment and modernization where the envisaged funds were reduced by almost half.

Regarding the distribution of expenditures by categories, the MoD policy is to achieve the ceiling in accordance with NATO recommendations and guidance. This means balanced costs by category, namely 50% for personnel, 20% for new major equipment and R&D and 30% for operations and maintenance.

### **1.1 New Major Equipment and R&D**

The distribution of defence expenditures by category for new major equipment and R&D as a percentage of total defence expenditures for the period 2013-2020 is as the follow:



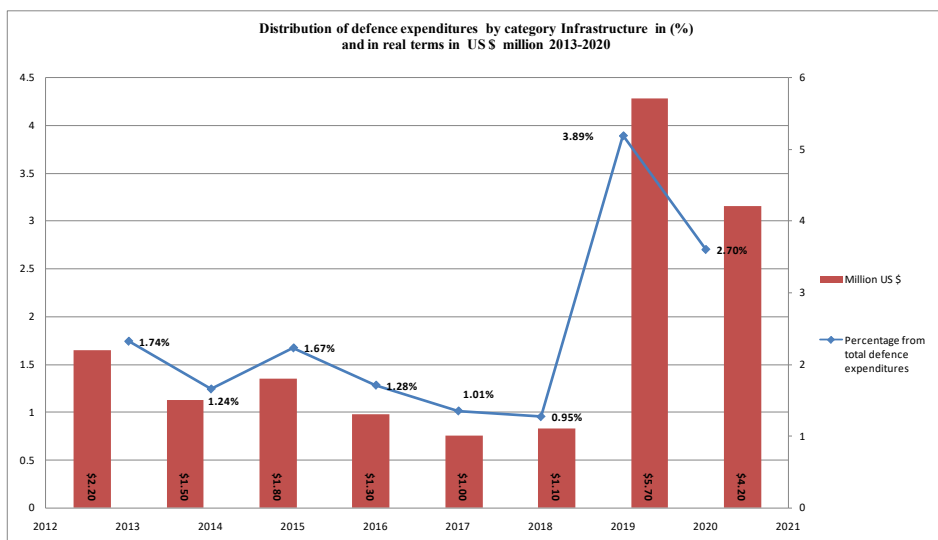
*(Source: Ministry of Defence of the Republic of North Macedonia, 2020)*

In the period 2013-2020, North Macedonia invested in real terms the amount of US \$ 94.9 million in new major equipment and R&D, as well as in the modernization of the Armed Forces, or an average of US \$ 11.8 million per year. The lowest level of percentage allocation of 5.92% was recorded in 2014 or in real terms it was an amount of US \$ 7.3 million. The lowest amount of only US \$ 6.5 million invested in this category was noted in 2017 or 6.46% of the total defence expenditures. Since 2018, there has been an upward trend in the distribution of defence expenditures for new major equipment and R&D. The highest level was reached in 2019, and a total amount of US \$ 20.3 million or 13.82% of the total defence expenditures was invested. For 2020, 18.23% of the total defence expenditures or in real terms an amount of US \$ 33.6 million was initially planned to invest. However, due to the outbreak of COVID 19, the total defence expenditures for 2020 were reduced by US \$ 29 million. Most of the reduction affected the plans for new major equipment and modernization. The initially provided funds for equipment and R&D were reduced from 18.23% to 11.44% or in real terms they decreased by almost half and amounted to US \$ 17.8 million. An encouraging fact is that the proposed projections of defence expenditures for 2021 are projected at 1.60% as a share of GDP or in real terms, US \$ 208.7 million of which 25.69% are planned for new major equipment and R&D in 2021 (Ministry of Defence, 2020). The data for North Macedonia show an increase in the allocation of funds intended for new major equipment and R&D, as well as for modernization,

from 5.92% in 2014 to 13.82% in 2019. If it maintains this policy of investment in defence expenditures, North Macedonia is on its way to reach the level of minimum 20% distribution of total defence expenditures in this category before 2024 and it can even be reached in the fiscal 2021.

## 1.2 Investment in Infrastructure

The trend of distribution of funds for infrastructure is in line with the Alliance policy where most allies invest within the limits of up to 5% of their total defence expenditures. There are some exceptions from the Allies where investments in infrastructure account for over 10% of total defence spending, but these are cases on an annual basis. Most of these funds are intended for renovation and ongoing maintenance of existing infrastructure facilities, as well as for the construction of new infrastructure for the needs of the Armed Forces.



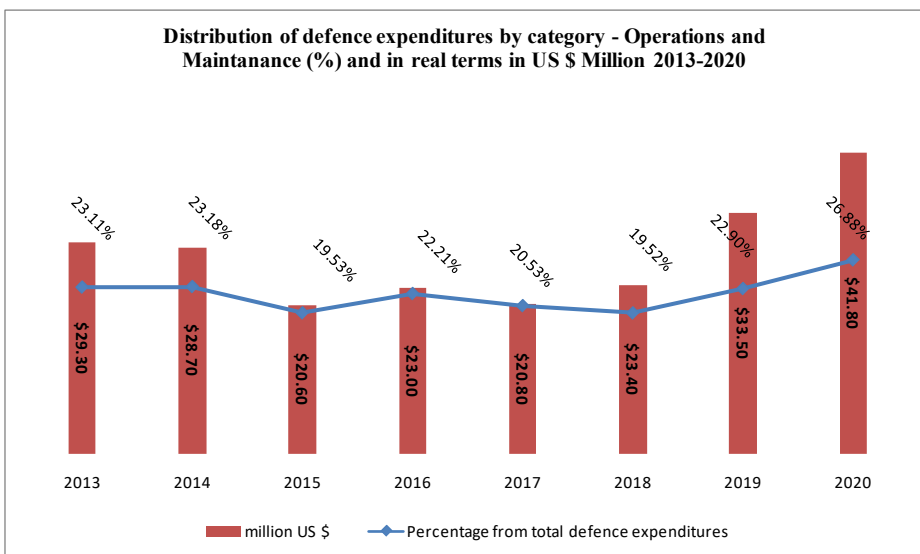
*(Source: Ministry of Defence of the Republic of North Macedonia, 2020)*

The allocation of funds for infrastructure in North Macedonia in the analyzed period ranges from 0.95% of the total defence expenditures in 2018 up to 3.89% in 2019. In 2020, infrastructure investments are projected at 2.7% of the total defence expenditures. In real terms, in the analyzed period 2013–2020, a total amount of about US \$ 19 million in infrastructure projects was invested. The projections and plans in the draft 2021 defence budget are to invest in real terms an amount of US \$ 6.2 million or 2.59% of total defence expenditures in infrastructure. These investments in infra-

structure have contributed to the maintenance of the necessary facilities for smooth functioning and performance of the constitutional and legally assigned obligations of the Ministry of Defence and the Armed Forces of the Republic.

### 1.3 Operations and Maintenance

The distribution of funds in the category of operations and maintenance includes the costs for international operations, for ongoing maintenance of the existing equipment and armament and other overhead and other costs necessary to ensure the normal functioning of the armed forces and the defence system. The allocation of funds in the category of operations and maintenance in the analyzed period 2013-2020 ranges from 19.5% to 23.1% of the total defence expenditures. In 2020, there was an increase in the allocation of funds in this category by 4% compared to 2019, or in other words, they increased from 22.9% in 2019 to 26.88% in 2020. In real terms, this means an increase by an amount of US \$ 8 million. For 2020, an amount of US \$ 42 million was allocated for this category of costs. The draft defence budget projections and proposals for 2021 are to invest an amount of US \$ 51.5 million or 24.66% from the total defence expenditures for 2021 for operations and maintenance.



*(Source: Ministry of Defence of the Republic of North Macedonia, 2020)*

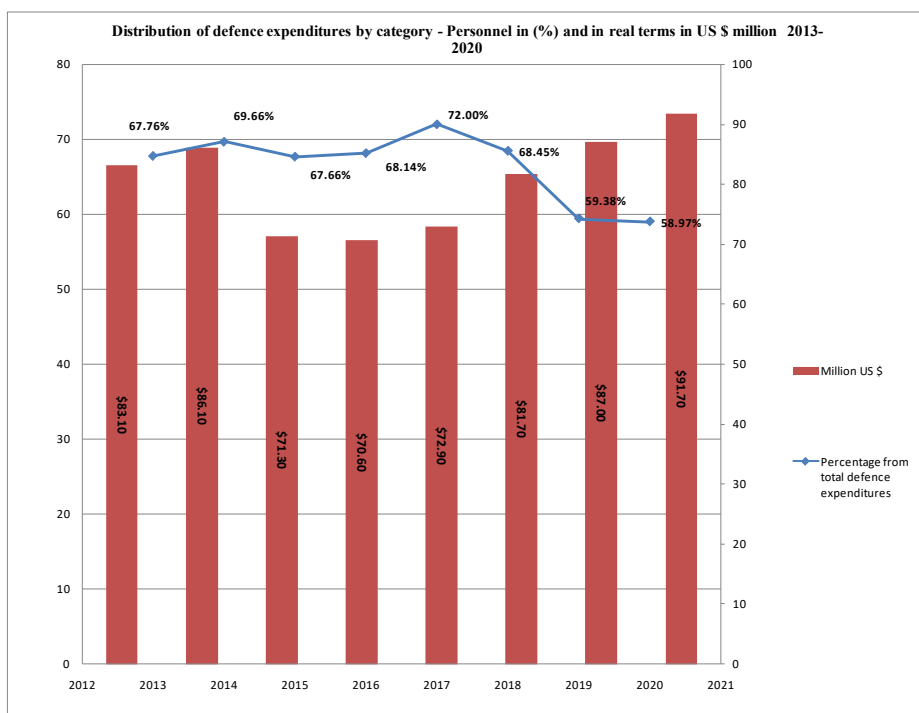
These funds are also used to finance international operations led by NATO, the UN and the EU. The decline of 23.18% from 2014 to 19.53% in 2015 is due to the completion of the ISAF mission (December 2014) and the beginning of the Resolute Support Mission (January 1, 2015), which initially had lower requirements. Depending on the mission needs, the number of members of the armed forces who were deployed to international



operations also varied. The increase from 22.90% in 2019 to 26.88% in 2020 is a result of the deployment of a contingent of the Armed Forces of North Macedonia to the KFOR mission in Kosovo in October 2020. In the period 2013-2020 in the category of operations and maintenance, a cumulative amount of US \$ 221 million was spent, of which about US \$ 42 million was spent only on the contribution to Alliance-led international operations.

### 1.4 Personnel Expenditures

Regarding the distribution of funds for personnel, it can be noted that the highest percentage was allocated in 2017 and 72% of the total defence expenditures were intended for personnel costs or in real terms it amounted to US \$ 72.9 million. That is the year when defence expenditures reached the bottom and were 0.89% as a share of GDP or in real terms US \$ 93.1 million. With the policy of gradual increase of defence expenditures by 0.2 percent per year, it can be noted that for a period of three years, significant progress has been made in reducing personnel costs. Personnel costs decreased from 72% in 2017 to 59.38% in 2019 or the reduction is slightly more than 22%, which provided more funds for other categories. The downward trend in personnel costs continues in 2020 as they fell to 58.97% of the total defence expenditures or in real terms they increased by US \$ 18.8 million compared to 2017 and in 2020 reached the level of US \$ 91.7 million.



(Source: Ministry of Defence of the Republic of North Macedonia, 2020)

The draft defence budget projections and proposals for 2021 are to invest an amount of US \$ 98 million or 46.70% from total defence for personnel. That means additional decrease of personnel cost by more than 12%.

## Conclusion

In the period 2013-2020, significant progress was made in increasing defence expenditures as a share of GDP and in real terms. The upward trend is noted in almost all Alliance member countries. Compared to 2013, when only three NATO member states met the requirements to reach a minimum of 2% as a share of GDP in defence expenditures, that number increased to 10 Allies in 2020. Compared to 2019, Bulgaria's economy did not keep pace and reduced defence expenditures from 3.18% to 1.93% in 2020. Despite the commitment of all Allies to achieve the NATO guidance on defence expenditures at minimum 2% as a share of GDP by 2024, it cannot be concluded with certainty that all countries will achieve this by 2024. There are many debates whether the 2% as a share of GDP for defence expenditures is the right indicator of the burden-sharing policy and measurement of the contribution to the development of Alliance forces and capabilities. The data analysis shows that the allocation of 2% of GDP does not mean automatic and correct distribution of the burden and sharing within the Alliance. Most of the economically weaker members and smaller countries have achieved or are close to achieving the level of 2% of GDP for defence expenditures. However, this does not mean that they will allocate more funds in real terms than the larger and economically more powerful members whose expenditures are below 2% of GDP. For example, in the period 2013-2020 Germany increased its defence expenditures by only 0.34% of GDP, or from 1.23% in 2013 to 1.57% in 2020, or in real terms, defence expenditures increased by over US \$ 13 billion. While Romania increased its defence spending from 1.28% in 2013 to 2.38% in 2020, an increase of 1.10% of GDP, in real terms defence expenditures increased by only US \$ 2.7 billion. Germany's US \$ 13 billion increase in defence expenditures is basically equivalent to the annual defence expenditures of nearly half (15) of the Alliance smaller member states. Any variation and correction of GDP in a downward sense strongly affects the costs in real terms, despite the fact that the percentage of allocation from GDP is maintained.

The Allies' second obligation, which also ensued from the 2014 Wales Summit, is to allocate at least 20% of the total defence expenditures to capital investments that include equipping and modernization, R&D of new capabilities, as well as investments in the infrastructure. Significant progress has been made in this segment and in 2020 sixteen (16) Allies have already reached the level of at least 20% allocation of funds in equipment and R&D. It can be expected with certainty that the other members will reach this level of capital allocation by the end of 2024, and possibly earlier.

The COVID 19 opened many dilemmas and is a strong challenge for the most economically powerful members of the Alliance, who are expected to bear the brunt of the burden-sharing in the Alliance. The lessons learned from the financial crisis in 2008-2009 teach us that no drastic reductions in defence expenditures are expected by the end of 2020. Most members of the Alliance are likely to maintain the current level of defence expenditures or continue to increase spending significantly as a percentage of GDP. However, this does not necessarily mean more funds in real terms. The largest decrease in defence expenditures is expected to occur after 2023, when probably adjustments to the burden-sharing methodology between allies could be announced. This would at least mean a policy of diversity in the percentage allocation of defence expenditures as a share of GDP. It means that the economically stronger Allies

will have a lower percentage, and the economically weaker will have a higher percentage as a share of GDP. No one can say for sure how things will proceed with certainty and discussions will take place between the expert public and within the Alliance itself. The pandemic is sure to leave its mark on Allies defence expenditures policy.

The Republic of North Macedonia, as the 30<sup>th</sup> member of the Alliance shows significant progress in increasing its defence expenditures with the Government's policy of continuous spending increase of 0.2 percent per year. In the last three years, i.e. starting from 2017 to 2020, defence spending has increased from 0.89% to 1.27% accounting thus for a 50% increase in real terms from US \$ 93 million in 2017 to US \$ 138 million in 2020. According to LTDCDP 2019-2028, the 2021 draft defence expenditures projections and proposals are to reach the level of 1.59% as a share of GDP or in real terms an amount of over US \$ 200 million. Will these projections and proposals become reality? To see this, we will have to wait until the end of the calendar year when the Assembly is obliged to adopt the draft budget for fiscal 2021.

### REFERENCES:

- Aitoro, Jill, (2020). NATO points to 'severe consequences' on global budgets from coronavirus crisis. 11 March 2020. (<https://www.defencenews.com/global/europe/2020/03/19/nato-points-to-severe-consequences-on-global-budgets-from-coronavirus-crisis/>).
- Barrie, Douglas. Childs, Nick. McGerty, & Fenella, (2020). Defence spending and plans: will the pandemic take its toll? 1st April 2020. <https://www.iiss.org/blogs/military-balance/2020/04/defence-spending-coronavirus>).
- Béraud-Sudreau, Lucie; Giegerich, Bastian, (2018). "Counting to two: analysing the NATO defence spending target", IISS Defence and Military Analysis Programme, International Institute for Strategic Studies, 14 February 2017, <https://www.iiss.org/en/militarybalanceblog/blogsections/2017-edcc/february-7849/countingto-two-67c0> - "NATO Defence Spending and European Threat Perceptions", *Survival: Global Politics and Strategy*, vol. 60, no.4, pp.53-74 August-September 2018.
- Cook, Lorne, (2020). Pentagon chief seeks to reassure NATO over US troop plans. Associated Press 26 June 2020. (<https://abcnews.go.com/International/wireStory/pentagon-chief-seeks-reassure-nato-us-troop-plans-71471162>).
- Csernaton, Raluca (2020). EU Security and Defence Challenges: Toward a European Defence Winter? June 11, 2020, (<https://carnegieeurope.eu/2020/06/11/eu-security-and-defence-challenges-toward-european-defence-winter-pub-82032>).
- Fiott, Daniel (2020). Will European defence survive Coronavirus? Expert Comment 11/2020 - 27/3/2020. [http://www.realinstitutoelcano.org/wps/portal/rielcano\\_en/contenido?WCM\\_GLOBAL\\_CONTEXT=/elcano/elcano\\_in/zonas\\_in/commentary-fiott-will-european-defence-survive-coronavirus](http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/commentary-fiott-will-european-defence-survive-coronavirus)).
- Fiott, Daniel. Terlikowski, Marcin. and Schütz, Torben, (2020). It's time to vaccinate Europe's defence budgets. Apr 20, 2020, (<https://www.euractiv.com/section/defence-and-security/opinion/its-time-to-vaccinate-europes-defence-budgets/>).
- Hazen, Bradley, (2020). NATO's progress on burden sharing remains strong. 13 August 2020, (<https://www.atlanticcouncil.org/commentary/infographic/natos-progress-on-burden-sharing-remains-strong/>).
- Marcus, Jonathan, (2020). Global defence spending is on the rise in an unstable world. February 14 2020. <https://www.bbc.com/news/world-51475892>).

- Mesterhazy, Attila, (2018). Burden Sharing: New Commitments in a New Era. Defence and Security Committee (DSC) Sub-Committee on Transatlantic Defence and Security Cooperation (DSCTC), 170 DSCTC 18 E rev 1 fin., 17 November 2018.
- Deutsche Welle, (2020). NATO spending rules need revising due to coronavirus, German defence chief says. Citation - Kramp-Karrenbauer, 17.07.2020. (<https://www.dw.com/en/nato-spending-rules-need-revising-due-to-coronavirus-german-defence-chief-says/a-54214272>).
- International Monetary Fund, (2020a), World Economic Outlook Update, A Crises Like No Other, An Uncertain Recovery, June 2020, <https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEUpdateJune2020>
- International Monetary Fund, (2020b), Real GDP Growth, October, 2020, [https://www.imf.org/external/datamapper/NGDP\\_RPCH@WEO/OEMDC/ADVEC/WEO\\_WORLD](https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEO_WORLD)
- NATO Communiqué PR/CP (2019)123, (2019). Press Release, NATO Public Diplomacy, Brussels, 29.November, 2019.
- The Secretary General's Annual Report 2019, (2020) NATO Public Diplomacy Division 1110 Brussels - Belgium [www.nato.int](http://www.nato.int) © NATO 2020.
- Wales Summit Declaration, (2014). Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 September 2014, [https://www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](https://www.nato.int/cps/en/natohq/official_texts_112964.htm)
- World Bank, (2020a). Global Economic Prospects, June 2020. Washington, DC: World Bank. © World Bank. <https://openknowledge.worldbank.org/handle/10986/33748> License: CC BY 3.0 IGO.
- World Bank. (2020b). The Human Capital Index 2020 Update: Human Capital in the Time of COVID-19. World Bank, Washington, DC. <https://openknowledge.worldbank.org/handle/10986/34432> License: CC BY 3.0 IGO.”
- World Population Review, (2020). NATO Spending By Country, 2020. Defence Expenditure of NATO Countries (2012-2019). (<https://worldpopulationreview.com/country-rankings/nato-spending-by-country>).
- ДПРОС 2019-2028, (2019), Долгорочен план за развој на одбранбените способности 2019 – 2028 година, Министерство за одбрана на република Македонија, 2019 година.
- Севриева, Марија. (2020). Светска банка предвидува најголем пад на економијата и раст на сиромаштијата. 14 јуни 2020 година, (<https://www.slobodnaevropa.mk/html>).
- СОП 2018 (2018), Стратегиски одбранбен преглед 2018 година, Министерство за одбрана на Република Македонија, 2018 година.
- Министерство за одбрана (2020), Трошоци во одбраната на според НАТО методологија 2003-2020 година. Податоци добиени преку слободен пристап до информации од јавен карактер заведени под бр. 09-4311/2 од 21.10.2020 година.
- ММФ по втор пат ќе ја ревидира прогнозата за економски раст. 12 мај 2020 година, (<https://www.slobodnaevropa.mk/a/30608357.html>).



## CONTEMPORARY CRISES: CASE STUDY OF UBER

Karlo PALJUG<sup>1</sup>  
Robert MIKAC<sup>2</sup>

**Abstract:** *Doing business in the digital world and providing services via digital technologies have become a part of everyday life and a condition of progress. Many companies operating in this area, such as Uber, have experienced global expansion, great growth and brand recognition due to their excellent idea. In addition to success, they also face crises that jeopardize their business, customers' privacy, as well as the company's value. Uber has faced several very serious crises during its short history, so the purpose of this research is of a twofold nature: first, to analyze how the company acted during crises; second, to show the area of regulations such as the General Data Protection Regulation, in order to minimize potential as well as actual crises in the digital world. The aim of the research is to analyze Uber's behaviour in crisis, to detect a number of publicly available indicators on how to deal with and resolve the crisis, and to provide recommendations for similar crises that will happen to businesses in the digital world.*

**Keywords:** *Uber, GDPR, digital technology, regulation, personal data, crisis, crisis management*

### Introduction

The frequency of crises in the modern world shows how subjects have to pay attention to the management. Crisis management is not only reflected in the sphere of physical threats but also of digital as well as emerging hazards, which manifest themselves in the violation of the 'colossal' regulation. The fast digital world has given many advantages, as well as dangers that do not affect the digital sphere alone, but transcend into the real physical world. In order for digital technologies and e-economy to continue to develop, they need a large amount of data, which brings challenges that need to be successfully overcome, otherwise breaches are possible, and they are often expensive.

The main drivers of digital demands are corporations, and data for them have become more important than ever before. However, as drivers, they are also extremely vulnerable when it comes to the cyber sphere of doing business. One important aspect of this is also the use of large sets of personal data for different purposes, with the aim of maximising profits.

However, the rules adopted in the field of data protection set out to a large extent the conditions under which data can be used correctly for the required purposes. Although the protection of personal data is not a question that arose several years ago, it is an area of privacy that has been developing at least in the last fifty years.<sup>3</sup> Today, we are witnessing a rapidly changing

<sup>1</sup> The author is MSc. & univ. spec. polit., Zagrebačka banka, Croatia

<sup>2</sup> Tue author is PhD, University of Zagreb, Faculty of Political Science, Croatia

<sup>3</sup> For example, in the German state of Hesse in 1970, the Data Protection Act was adopted, followed by the adoption of similar regulations across Europe — Sweden in 1973, France in 1978, etc.

way of doing business, which is the result of the digitalisation of processes within corporations as well as in the society. In addition to the development of numerous data collection models of individuals, it has been shown that manipulation of personal data can have significant consequences (Information Commissioner's Office of the United Kingdom 2018a).

Any data breach constitutes a potential crisis that can bring significant negative effects on business. In order to overcome it, a good understanding of the matter is crucial, along with the clearly established crisis management mechanisms, as well as sufficient resources.

Crisis management represents the capacity of the organisation to act quickly, efficiently and effectively in situations where the objective is to minimise adverse effects on the normal course of the business, and the damage itself. As a set of functions, it aims to identify, learn and anticipate possible crisis situations and to establish specific ways to enable the organisation to prevent an escalation of the crisis or to find ways to minimise the consequences and return to its normal situation (Kešetović et al. 2013: 101).

The case of data breach that has affected the international corporate Uber is one of the flagrant examples what subjects are not allowed to do when confronted with a crisis situation. Uber was a target of a hacker attack in 2016, during which the attackers were able to gain access to the source code on GitHub, find Cloud Credentials and use them to download data. Although the breach has occurred in the United States, it has affected a vast number of individuals across the world, including citizens of EU Member States.

If such a situation occurred at now when the General Data Protection Regulation is applicable, it would, at the very least, withdraw the sanction against a legal person which, through its failure enabled the data breach, but which could be much higher than the one in the United States. This example is a good way of pointing out what matters and what should be avoided.

The aim of this work is to explore how the international company Uber managed a crisis situation, which steps need to be taken to protect its own value, its users and data (data from users and corporations). The purpose of the study is to analyse ways and models of application of different approaches and crisis management measures in this specific case, in order to draw lessons for similar cases in the future. The central research question is explanatory and is stated as follows: How did Uber manage the mentioned crisis? To answer this question, we will try to use desk top qualitative research framework using several different scientific methods to be explained below.

The structure of the research shall be divided as follows: *Introduction* will be followed by the heading of the theoretical and methodological framework where the key concepts and methods of research will be explained. This is followed by a *Data protection* in which a normative framework will be presented. After which comes the section on *Data breach* which explains how the breach occurred. Part of the *Uber case and the crisis management* key parts of the crisis, as well as what Uber did during the crisis will be presented. This is followed by a *Discussion* about Uber's methods of dealing with the crisis which will be analyzed in accordance with the set theoretical and methodological framework and the *Conclusion* will provide a cross-section of all research and recommendations for future action in similar crises.

### **Theoretical and Methodological Framework**

“The crisis has led to a change — either sudden or gradual — bringing about a serious problem that needs to be addressed immediately. In business, the crisis is everything that may cause sudden and serious harm to employees, reputation or financial

performance of the company” (Luecke 2005:15). The commercial crisis represents a situation in which an organization find itself — influenced by internal or external factors — that threatens its survival (Sučević 2010: 12-15). Managing certain situations that do not necessarily require a crisis, or if they are transformed into a crisis by addressing crisis management. Previously, it was stated that the crisis management represented the organisation’s ability to deal rapidly, efficiently and effectively in situations where the objective of minimising adverse effects on the normal course of business, and of the damage itself (Kešetović et al. 2013: 101). In that regard, a crisis management is part of a broader system of organisational risk management. Although we are all aware of numerous crises, “rare managers are actively preparing for potential crises”. They are still less training for crisis management. None of these gaps should be surprising, as crisis management is still a young discipline (Luecke 2005: 15). Therefore, as the main theoretical framework of the analysis we take the theory of crisis management, which is part of security studies, economics and management studies, and as such, represents an extremely suitable basis for this research.

In crisis management analysis, the most commonly and globally used is the framework consisting of four phases: prevention, preparedness, response, and recovery. We need to determine when and at what level the analysis is carried out. According to Ole Holsti, there are four reference levels of crisis analysis: the state, the bureaucratic organization, society and the individual (Kešetović et al. 2013: 29). Our research includes an analysis at the level of the organisation. Moreover, for a more detailed analysis approach, different authors have developed additional stages of analysis compared to four globally used. Arjen Boin and associates have developed a theoretical framework that involves five critical tasks for crisis management: observation, decision-making, interpretation, completion and learning (Boin et al. 2005: 10). Norman Ougustin considers that there are six phases of the crisis management at the disposal of the business companies: crisis avoidance, preparation for crisis management, crisis recognition, crises containment, crisis resolution, drawing conclusions (Ougustin: 2010:11). While Richard Luecke refers to eight stages: preparing for possible dangers, avoiding dangers, contingency planning, crisis recognition, containing crisis, crisis resolution, media cooperation, learning from the crisis (Luecke 2005: 16-20). Given the available space in this survey and for the purposes of this work, we have decided to focus primarily on a part of the solution to the crisis by closing the solutions outlined here by the authors.

According to Boin et al. (2005: 79), successful crisis management requires a framework of what the crisis is, which allows them to define appropriate strategies for resolving it. Ougustin (2010: 46) states that it is necessary to start implementing the crisis plan as soon as possible. When a company is exposed to a crisis, the assumption is that it has several realistic options at its disposal; they need to be considered and the company needs to act in accordance with its crisis plan. Luecke (2005: 122-124) believes that during a crisis, time works against those who need to resolve the crisis, and the more time passes, the problem spreads, takes root and becomes increasingly



difficult to overcome. So it is necessary to act quickly and decisively in any crisis. It is also necessary to tirelessly communicate with all key groups of the public such as clients, shareholders and employees. Communication, among other things, is a tool in suppressing rumours and coordinating all activities needed to resolve the crisis.

Since this analysis has been given to an explanatory research question (How?) specified in the case study method for carrying out the analysis (Yin 2007: 16). “Study (Analysis) on selected cases implies the use of different methods to analyse in details one or several selected cases concerning the same or a similar subject or issue of research.... The method of analysing the case is used to better understand the substance of the problem, to develop more general theoretical claims about the regularity in the analysed structure and process, to create a typology or categories relating to social phenomena or to develop new hypothesis tested at a later research activity” (Tkalac Verčić et al. 2010: 94). So that the research involves one unit of analysis, the conduct of Uber in a crisis, that is to say a single case, is investigated, since Uber manages the crisis in which it found itself. Additional methods used are analysis, synthesis and comparative method. The analysis is used to study individual parts in relation to the whole and other parts. Synthesis explains the state of reality by assembling simpler parts into a particular unit. While using a comparative method, we analyze individual parts of the same case study.

### **Data Protection**

A fast digitalised world has created the need to adopt a comprehensive regulation to protect the personal data of each individual. Why is that so? This is due to the fact that the personal data has become new oil of the economy, as well as the technologies that go with it. Personal data can be used in a variety of ways, some of them are most often used for marketing purposes, but it goes to the realm, sometimes difficult to understand – development of artificial intelligence, calculating risk, improving business, etc.

However, misuse of personal data may entail consequences for people, which may be minor, but can also be horrible.<sup>4</sup> From the illegal use of the electronic addresses to send marketing messages, to identity theft, with the prospect of even worse consequences in the future.

Therefore, in order to ensure that the use of personal data is provided for in the expected frameworks, as well as to guarantee adequate protection from malicious individuals and groups, in 2016, the EU adopted legislation affecting business to a very large extent. The referred legislation is the General Data Protection Regulation,

---

<sup>4</sup> For example, the Cambridge Analytica case has shown how illegally collected data can influence democratic processes. In the said case, Facebook Inc and Facebook Ireland Limited were fined £ 500,000 by the UK Information Commissioner Office. For more see <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/>.

which became applicable in May 2018 (hereinafter: GDPR or Regulation) (European Parliament and Council 2016).

It is a regulation the application of which is extremely broad. The rules apply to the processing of data in the context of the activities of an establishment of a controller or processor in the EU, but also those that are not established on the territory of the EU (when they are offering goods and services to individuals to the EU, as well as monitoring their behaviour). In other words, the legislation applies practically to the whole world that is doing business with the EU (ibid: Article 2).

GDPR is the general regulation in the field of data protection, which serves as a fundament for other relevant legislations which are or will be enacted in the future. The Regulation has led companies not only to change the basis of a certain business process, but to have in place clear procedures for situations where its provisions will be breached. Given that the aim of this article is to clearly define crisis management mechanisms in case of data breach, greater attention will be paid to this “first line of defence”.

## Data Breach

A personal data breach is defined as a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed. In other words, it is a situation where there is an unauthorised or unlawful removal of personal data (e.g. loss of personal data, sending a message to an incorrect electronic address or theft of personal data). For example, it is possible for one of the company’s staff to copy clients’ data to the USB and sell these data to another company or to a hacker using a malicious program — ransomware<sup>5</sup> — in order to block the company’s access to the data. These examples do not fall within the utopia, but are considered as a practically everyday occurrence. As we will see in the case of the scenario that has hit Uber and ultimately made it clear how not to act when it comes to modern business, and much less when it comes to personal data.

The European Union Agency for Network and Information Security (ENISA), in its *Threat Landscape Report* from 2018, identified 15 main cyber threats in the world: malware (malicious software designed to cause intentional damage to IT infrastructure – viruses, worms, spyware, Trojan horses); web-based attacks (through web systems such as browsers, extensions, websites and web services); web application attacks (using weaknesses in web services and applications); phishing (defrauding information by posing as a legitimate company and sending emails and messages with a malicious attachment, URL, etc.); disturbed denial of service – DDoS attack (disruption to the regular traffic of a server, service or network by overwhelming it with internet traffic); spam (flooding users with unsolicited emails or messages); botnets (connected devices

---

<sup>5</sup> See more about ransomware <https://www.cert.hr/19795-2/ransomware/>

that are running bots, i.e. software applications that run automated tasks like DDoS attacks); data breaches (successful outcomes of cyber threats as leakage or exposure of data); insider threat (within a company or organization); physical manipulation/damage/theft/loss (of a storage device); information leakage; identity theft; cryptojacking (or cryptomining – use of device processing power to mine cryptocurrencies); ransomware (ransom of blocked files and devices); and cyber espionage (ENISA, 2019: 9).

As we see cyber threats are numerous and very different, it is therefore essential to be prepared for data breach, but also to know how to recognise it. It is easy to recognise a theft of USB containing personal data, but the detection of a data breach can be much more subtle, to an extent that it can only be seen when significant damage has already occurred.<sup>6</sup> It is also necessary to set up a plan and a team with appropriate knowledge to guide the process when such a crisis occurs (Information Commissioner's Office of the United Kingdom 2018b). It is necessary to determine whether the appropriate technical and organisational measures have been implemented so as to determine immediately whether a data breach has taken place, and to inform the authority and the individuals concerned within a specified period of time (European Parliament and of the Council 2016: Preliminary provisions, paragraph 87).

A breach may potentially have a number of significant adverse effects on the individuals whose data are affected and may result in physical, material or non-material damage. The Regulation clarifies that it can be about the loss of control of data, limitation of rights, discrimination, identity or fraud, financial losses, reputational damage, as well as the loss of confidentiality that can be addressed (Article 29 Data Protection Working Party<sup>7</sup>, 2018).

Once the data breach has occurred, it is necessary to report to the national supervisory authority responsible for the protection of personal data (hereinafter: The supervisory authority), within 72 hours of being aware of it. Article 33 of the GDPR is worded as follows: The Regulation's report shall include the following: description of the nature of the data breach (what personal data are violated, number of individuals); name and contact details of the data protection officer (or in case the company does not have a data protection officer, then the contact person who can give more information); description of the likely consequences; description of the measures that the company

---

<sup>6</sup> It is possible to imagine cases of infringements arising from the passage of time. For example, an organisation providing children with a specific skill in enrolling a child's consent to be able to publish the photos on the organisation's official page. Once a child has reached adulthood, the organisation continues with the same practice, if he or she has obtained consent. While the initial treatment was in compliance with the statutory provisions, once the child has reached the age, the organisation sought to obtain the child's consent again in order to proceed with the lawful publication of the photograph on the official website.

<sup>7</sup> Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. After adoption of the GDPR it became the European data protection board.

takes or suggests to take in order to resolve the problem, including taking measures to reduce the effects thereof.

However, if a data breach is not likely to result in a risk to the rights and freedoms of individuals, then the organisation does not need to report to the supervisory authority, but it is important to bear in mind that such a breach has to be also documented, as well as the reasons why it is considered not to pose a risk to the rights and freedoms. It may be the case where the personal data have already been made public. The situation where personal data are essentially not readable to unauthorised parties is similar. However, at the outset a notification may not be required but the same may change over time and the risk should be re-assessed. If it is subsequently established that the key is compromised (in encryption) or a weak point in encryption software is detected, then notification could be required (Article 29 Data Protection Working Party, 2018).

We live in a globalised world where information travels faster than ever, where services are delivered from one country to all citizens of the world, personal data not only affecting citizens of one country, but more of them, may be misused. The Regulation states, in such cases, of cross-border infringements must be notified to each supervisory authority responsible for carrying out the task on the territory of its own Member State (European Parliament and of the Council 2016: article 55).

In doing so, the company must take care which supervisory authority is the leading one, since it will be the authority of the State where the company has its main establishment or the single establishment in the EU. Organisations should assess the lead supervisory authority when drafting their action plan, allowing them to react more quickly and fulfil their obligations in the light of the Regulation. This means in addition to inform the lead authority and the competent authorities in the countries where it is also has establishment (Article 29 Data Protection Working Party, 2018).

We see therefore how data breaches would not evolve into a crisis, i.e. if they are transformed into a crisis need to respond through a crisis manager, who must be aware of the requirements that are brought before them by this ‘colossal’ regulation — GDPR. In addition to knowing how to recognise the data breach, short time limits must be respected, as well as allocating sufficient resources to dealing with the breach. In the light of the rapidly changing digital world threats are an everyday case, and especially when we have the cyber threats cited by ENISA. Bearing in the mind the stages of the crisis management according to Luecke and other authors, but also any threats which exist in the realm of personal data, it is not a question of whether any potential crisis will occur, but only when they will happen.

### **Uber case study and manner of managing the crisis**

Looking at the Uber case, it is necessary to see the broader picture around this company’s security and privacy. And not just to observe the data breach from 2016, but also those that occurred in 2011 and 2014.

In fact, in 2011, Uber offered to the markets of large cities the ‘Black car’ and ‘Ride-sharing’ services. In doing so, the participants were able to track Uber’s “God’s view”, which allowed them to see all drivers, as well as all users who ordered driving. Although it was an anonymous version, at one of parties they decided to “honour” their guests with the so-called “Creepy Stalker View” which revealed identities and showed the position and movement of certain users in real time. That case led the authorities to open an investigation (Torre 2019).

In May 2014, hackers managed to enter the Cloud and access the data of more than 100.000 individuals and in addition, difficulties encountered with the monitoring of workers in which some workers access users’ personal data. These two cases resulted in settlements with supervisory authorities due to a lack of supervision of workers and lack of security measures. Uber has agreed to third party auditing in the next 20 years, and to adopt a robust privacy protection programme (Torre 2019).

These cases were already sufficiently aggravating, in relation to a relatively young company that started to break into the world market. However, in 2016 there was a new attack of cyber criminals and that is when the real agony began. Indeed, the attackers were able to gain access to the source code on GitHub (using stolen credentials). They found the Cloud credentials and by using them to download the company’s data in 16 large files containing personal data of 57 million users and drivers from all over the world. Affected by the aforementioned cases, the company “came up with a clever idea” and decided not to report the attack and paid the attackers USD 100,000 as a reward for the detected bug (Torre 2019; Somerville 2017; Frankel 2017).

However, as also mentioned by the regulator in the United Kingdom — ICO, Uber has paid a ‘reward’ to the attackers that were fundamentally different from the legitimate bounty. They were hackers who, instead of detecting vulnerability and reporting it, misused it and downloaded personal data (Hern 2018).

We are free to say that the 2016 data breach, i.e. the ‘Uber data breach’, become a synonym for a very serious infringement, as well as for non-compliant behaviour. The company decided neither to inform the authorities, nor the users that their personal data had been compromised by an unauthorised third party. In addition, in taking measures for reducing the risk to the rights and freedoms of individuals, the company started monitoring accounts 12 months after the attack in order to prevent possible fraud (Hern 2018).

Finally, in agreement with the authorities, Uber has adopted a data breach notification model, as well as data protection practices and a corporate integrity scheme for employees reporting unethical behaviour. In addition, it commissioned a third party to assess data protection practices at the time and paid a record high fine of USD 148 million (Torre 2019; Hern 2018).

In its public statement, the company emphasised that it has made significant changes in leadership to ensure an adequate level of transparency with regard to regulators and users. They highlighted how they learn from their mistakes and that they will

continue to work on gaining the trust of users (Hern 2018).

In August 2020, a criminal complaint against Josef Sullivan, formerly Chief Security Officer, was raised resulting from the obstruction of justice and covering up data breach. Sullivan engaged in concealment not only by the fact that hacking had taken place, but also that there had been a data breach of millions of users and drivers (Conger 2020).

Bearing in mind all of the above, it is clear that any similar treatment, such as Uber's, would fail to satisfy the requirements laid down by the GDPR. Apart from the poor preparation for the crisis, a series of wrong decisions, as well as non-transparency, led to a very high penalty, but also to the fact that today, 4 years after the last data breach, the case of this company is synonymous with "how not to act". Concealment of the data breach, i.e. false reporting to regulatory bodies and the public, which would be contrary to the GDPR, entails severe consequences. While it is possible to discuss the level of cyber security within the company itself, what has led to the final outcome of the case are the number of decisions which went in the direction of avoiding liability.

## Debate

As it is likely to see in the series of given incidents in Uber, as an epilogue there was not only a fine, but also criminal prosecution, certainly reputational damage, which is estimated to be, among other things, due to the cover-up in question, Uber has lost about USD 20 billion in value (Somerville 2017). Moreover, in some Member States of the European Union regulators, since there was data breach of their citizens, they have decided to impose a penalty. For example, the Dutch Data Protection Authority imposed a penalty of EUR 600,000, the French Data Protection regulator EUR 400,000 and the British Information Commissioner 385,000 pounds. It is necessary to highlight the penalties imposed for data breach that occurred before the application of the GDPR. The Commission Nationale de l'Informatique et des Libertés (CNIL), the French regulator stated on 20 October 2018, when they publicly disclosed the information on the imposition of a fine, that the penalty would be much higher if the Regulation was applicable at that time (Commission Nationale de l'Informatique et des Libertés 2018).

By doing so, Uber has practically shown a school example of what an organization should not do in the event of a data breach. Considering such a data breach in the light of the Regulation, there were a number of missteps that ultimately followed all those repercussions highlighted above.

In this type of a case, first, when such a breach occurs, there is an obligation to report it to the competent supervisory authority at the latest within 72 hours of becoming aware of it, unless the data breach is unlikely to result in a risk for the rights and freedoms of individuals. Accordingly, there is an obligation to notify the supervisory authority of the Member State where the organization has its main establishment, but

it is also a good practice to provide such information to the supervisory authorities of other Member States if the data breach has occurred in their territories or to their citizens. As we have seen, in the Uber situation, the company did not report a data breach for a certain period of time, and it decided to cover up the whole case. There was also a large number of affected individuals and set of personal data in this, so an exception would be considered out of the question.

In the Guidelines on notification of data breach under Regulation 2016/679, Article 29 Data Protection Working Party has highlighted that the data controller in the situation of data breach will have to notify the lead supervisory authority, in case of cross-border data processing. Organisations have to pay attention when drawing up the action plan, it must be assessed which supervisory authority is the lead authority. They also have to specify that, in the event of a data breach involving cross-border processing, the lead supervisory authority must be informed, which does not necessarily have to be the supervisory authority responsible for the territory of the affected subjects or on the location where the breach took place. It is recommended that the organization in such case should state whether the breach occurs in other Member States and in which Member States there are individuals who are likely to be affected by a data breach (Article 29 Data Protection Working Party 2018).

As we have seen, there is also an obligation to inform the data subjects in case of a data breach without undue delay, unless the breach is not likely to result in a high risk for the rights and freedoms of the individual, so that the notification threshold is higher than for the supervisory authority. However, in such situations where there is a data set (name, e-mail address, mobile phone number and driving licence number), as well as a large number of individuals, but also where there is a third-party criminal, there is certainly a high risk. Such data could be offered on the Dark Web and could achieve a significant price and may, in addition, be used for further criminal purposes. Individuals affected by a data breach can be informed directly, unless doing so would involve disproportionate effort, in the case of which they shall be given a public notice. Recital 86 of GDPR states the following: „The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication“ (European Parliament and Council 2016: Preliminary provisions, paragraph 86).

It is important to stress that the risk assessment should take into account several parameters: the type of infringement, the nature, the sensitivity and the amount of personal data involved, the ease with which the individuals are identified, the seriousness of the consequences for the individuals, the specific characteristics of the individual, the specific characteristics of the data controller and the number of individuals affected.

Organisations shall, upon request, cooperate with the supervisory authority in the performance of its tasks. In other words, the conduct, such as in Uber's case, is certainly not in line with the Regulation and constitutes a breach of the Regulation. Such non-cooperation may, in any event, also be reflected in the amount of the penalty that may be imposed by the supervisory authority. It is also necessary to document the infringement and to surrender such documents to the supervisory authority. Making false statements before the public and the supervisory authorities, as well as the cover up attempts, is certainly not in the direction of good cooperation with the supervisory authority.

When imposing an administrative fine, the supervisory body that could impose in such a case would certainly not be small. The supervisory authority shall be guided by the nature, gravity and duration of the breach, whether measures are taken to mitigate the damage suffered by the data subject, the degree of responsibility, relevant previous data breach, the degree of cooperation with the supervisory authority, the affected categories of personal data, the manner in which the supervisory authority became aware of the breach and any other aggravating or mitigating factors (Article 29 Data Protection Working Party, 2017). The penalty may be imposed up to EUR 10,000,000 or up to 2 % of the total worldwide annual turnover of the preceding financial year. In case of severe data breach the penalty could go up to EUR 20,000,000 or up to 4 % of the total worldwide annual turnover of the preceding financial year. In addition, in the event of a breach of several provisions of the Regulation, the total amount of the fine may not exceed the administrative amount set for the most serious infringement.

In 2015, Uber recorded an annual turnover of USD 1.5 billion, so that each individual supervisory authority could impose a maximum penalty of USD 60 million due to such data breach, as a number of provisions of the Regulation have been infringed. However, if such breach occurs in 2020, the fine could reach an amount of USD 564 million, given that the global turnover in 2019 was USD 14.1 billion.<sup>8</sup>

It must, of course, bear in mind the possibility of a group action for damages, but also a loss of reputation that may be reflected in a fall in the share price, boycotting the use of a service or a product, and such negative effects can have a very drastic effect on the company's business.

In the analysis of everything done by Uber, according to publicly available data and the set theoretical and methodological framework, we can point out that the company

---

<sup>8</sup> Annual traffic data extracted from <https://www.statista.com/statistics/550635/uber-global-net-revenue/>



did not successfully manage the crisis because it did not set the necessary framework to define the kind of crisis they faced, which would allow them to define and then to undertake appropriate strategies to address the crisis. Furthermore, the analysis found that Uber did not have a contingency plan at its disposal, so even if they considered realistic options available, they could not implement them effectively because they did not have a background or guide in the form of a contingency plan to respond better in relation to the way their executive management reacted.

Furthermore, the analysis showed that the company's management did not cope well with the crisis, over time their problem became bigger, they took root in their ranks and they could not overcome it on their own. While regarding communication in a crisis they did everything contrary to the recommendations they should follow and decided to cover up the situation which turned out to be the wrong decision. So the behaviour of Uber's executive management is a prime example of how not to act during a business crisis.

## **Conclusion**

Business crises show that most companies are unprepared for the crises that happen to them and that, as in the example of Uber, they do not have a developed crisis management as part of the company's strategic business processes. Many companies around the world are failing after the first major crisis in which they found themselves due to both financial losses and loss of reputation. Luck has helped Uber. Even after several crises (2011, 2014 and 2016) and despite the fact that they were not well managed, the company survived and continued to operate. But their case is very indicative both for them and for many others such as other companies, users, regulators, law enforcement agencies etc. The significance of this case study shows the importance of looking at such crises and justifies the reasons for its research.

The crisis in question and publicly available data confirm the correctness of the set theoretical and methodological framework, its design and composition, which is adapted to the research and analysis of this crisis. Crisis management theory and the scientific research methods used were applied in a way to extract key observations related to the crisis and Uber's handling of the crisis in which they found themselves. Although aware that no theory can explain all the facts and processes, especially in today's extremely fast, dynamic and multi-layered world, we still need theories as patterns by which to interpret the processes we have chosen to analyze.

Regarding the part of the discussion on this crisis, it is important to point out that the need and usefulness of regulation in all processes, including in the part of digital business, has been justified. Especially since the digital world is in exponential development, it brings us numerous advances but also significant challenges and dangers. Therefore, regulation is necessary and desirable in a way that protects users, companies, societies and states, and does not restrict them in their business. This is exactly what is being achieved through the GDPR. This is additionally important because it enables the regulation of the operations of companies that are established and registered outside the European Union and provide services around the world, including to the citizens of the Union.

The key recommendations of this research are that it is necessary to develop crisis management in addition to regulation at all levels and in all areas. The analysis showed that Uber did not have crisis management in place, so it did not even try to manage the crisis effectively,

but went along the line of least resistance, hoping that everything would somehow resolve itself with as little damage as possible. It turned out that they were not right and that with adequate crisis management they would certainly respond better and more successfully to the crisis, in which they found themselves, and thus, better protect the personal data of the customers and the value of the company. So investing in security, such as establishing a crisis management system is not a cost but a necessity of every business organization.

## REFERENCES:

- Article 29 Data Protection Working Party (2018) , Guidelines on Personal data breach notification under Regulation 2016/679, (adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018), [https://azop.hr/images/dokumenti/217/wp250rev01\\_enpdf-1.pdf](https://azop.hr/images/dokumenti/217/wp250rev01_enpdf-1.pdf), accessed 13 October 2020
- Article 29 Data Protection Working Party (2017), Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (adopted on 3 October 2017), [https://azop.hr/images/dokumenti/217/guide\\_lines\\_application\\_of\\_administrative\\_fines.pdf](https://azop.hr/images/dokumenti/217/guide_lines_application_of_administrative_fines.pdf) , accessed 20 October 2020
- Boin, A., Hart, P., Stern, E., Sundelius, B. (2005), *The Politics of Crisis Management: Public Leadership under Pressure*, New York: Cambridge University Press
- Commission Nationale de l'Informatique et des Libertés (2018), UBER: sanction de 400.000€ pour une atteinte à la sécurité des données des utilisateurs, <https://www.cnil.fr/fr/uber-sanction-de-400000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs>, accessed 12 October 2020
- Conger, K. (2020), Former Uber Security Chief Charged With Concealing Hack, The New York Times, <https://www.nytimes.com/2020/08/20/technology/joe-sullivan-uber-charged-hack.html> (accessed 28 October 2020).
- European Parliament and Council (2016), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HR>, accessed 2 October 2020
- European Union Agency for Network and Information Security (2019). ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>, accessed 12 October 2020
- Frankel, A. (2017), Data breach class actions are the least of Uber's problems, Reuters, <https://www.reuters.com/article/legal-us-otc-uber-idUSKBN1DM2Q3>, accessed 13 October 2020
- Hern, A. (2018), Uber fined £385,000 for data breach affecting millions of passengers, The Guardian, <https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked>, accessed 12 October 2020
- Information Commissioner's Office of the United Kingdom (2018a), Democracy disturbed? Personal information and political influence, <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>, accessed 25 September 2020
- Information Commissioner's Office of the United Kingdom (2018b), Personal data breaches, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>, accessed 28 October 2020

- Kešetović, Ž., Korajlić, N., Toth, I. (2013), *Krizni menadžement (Crisis Management)*, Sarajevo: University of Sarajevo, Faculty of Criminology, Criminology and Security Studies; Velika Gorica: University of Applied Sciences Velika Gorica
- Luecke, R. (2005), *Upravljanje kriznim situacijama (Crisis Management)*, Zagreb: Zgombić & Partneri (translation of the Harvard Business School publication)
- Ougustin, N. R. (2010), *Upravljanje kriznim situacijama (Managing Crisis)*, Beograd: Data Status (translation of the Harvard Business School publication)
- Somerville, H. (2017), Uber may have just lost \$20.5bn in value, Independent, <https://www.independent.co.uk/news/business/news/uber-shares-latest-update-value-lost-billinos-softbank-japan-discount-ride-sharing-taxi-a8079511.html>, accessed 12 October 2020
- Statista (2020), Global net revenue of Uber from 2013 to 2019, <https://www.statista.com/statistics/550635/uber-global-net-revenue/>, accessed 23 October 2020
- Sučević, D. (2010), *Krizni menadžement (Crisis Management)*, Zagreb: Lider
- Tkalac Verčić, A., Sinčić Ćorić, D., Pološki Vokić, N. (2010), *Priručnik za metodologiju istraživačkog rada (Manual for research methodology)*, Zagreb: M.E.P. d.o.o.
- Torre, L. (2019), The Uber Breach Story: On how security woes can lead to a criminal complaint, Medium.com, <https://medium.com/golden-data/case-study-uber-technologies-inc-data-breach-7261484d6471>, accessed 21 October 2020
- Yin, R. K. (2007), *Studija slučaja: dizajn i metode (Case study: design and methods)*, Zagreb: Faculty of Political Sciences

## TERRORISM OR INSURGENCY? THE MOST COMMON STRATEGIC FALLACY

Gjorgji VELJOVSKI<sup>1</sup>

**Abstract:** *The most repeated phrase today when discussing terrorism is that one man's terrorist is another man's freedom fighter. This perception has not only become annoying, but also very disturbing because it relativizes terrorism as one of the biggest problems of the civilized world. Terrorism completely dehumanizes the use of force. While states agreed upon certain rules of war in order to avoid killing non-combatants, the terrorist use unrestricted violence that deliberately targets civilians. It should never be that difficult to recognize which violence is an act of terrorism. The lack of universally accepted definition of terrorism is a serious gap in the international law that is often used by state and non-state actors to label terrorists as insurgents and vice versa, depending on the political interests. This article explains why confusing terrorism and insurgency is a dangerous strategic fallacy and compares the most viable definitions through the terminology used to describe them. The author identifies that the only true indicator which will never mistake a terrorist with a freedom fighter is the deliberate killing of civilians.*

**Keywords:** *terrorism, insurgency, definition, civilians, state.*

### Introduction

Terrorism is one of the biggest security challenges for societies globally. Although a relatively new term, first used after the French revolution as the “reign of terror”, (Durschmied, 2002) it is not a new strategy to make an adversary compel through fear. The very concept of pursuing political goals using coercion is old as war and politics itself. The reason why terrorism today is in the spotlight of the global politics is the obvious inability of the nation states to protect their citizens against such unrestricted violence. (Bhonsle, 2011)

The fact that the international law has not agreed upon universally accepted definition of terrorism is both frustrating and challenging. (Kulesza, 2016) Most of the time states simply cannot prevent terrorist attacks and tend to react after terrorists already do the damage. In many cases, the states are responding in all directions, like a wounded animal, making unnecessary damages without actually solving the problem. When perpetrators are difficult to find, states often choose to better blame someone than no one.

How the states perceive the threat of terrorism is crucial for application of genuine state strategy. Proper identification of the problem is the most important part of the solution. Aristotle said that it is easy to become angry, “but to be angry with the right person and to the right degree and at the right time and for the right purpose, and in the right way - that is not within everybody's power and is not easy”. (Laurent and Menzies, 2013) Using this famous

---

<sup>1</sup> The author is PhD, colonel at the Army of North Macedonia

quote one could as well explain the behaviour of the states, when they get the wrong response to the wrong degree at the wrong time for the wrong purpose, toward a wrong group of people.

It is necessary to have critical and comprehensive approach to identify the actors in the operational environment, as there should be different strategies to respond to different security threats. Governments must differentiate among the threats to national security if it is a subject of organized crime, insurgency, terrorism or other form of violence. In multiethnic and multireligious states such ambiguity, sometimes more than often, triggers a chain of inadequate policies that can exacerbate the interethnic mistrust based on false assumptions. In the cases of violence in multicultural societies which is suspected to be terrorism, the absence of universally accepted definition of terrorism can mislead understanding of the problem and how to properly respond.

### **Viable definitions of terrorism and insurgency**

The common misconception is that terrorism is a phenomenon that occurs as an anomaly in modern conflicts. However, it is a very common tactic of an extreme, far right use of violence often associated with irregular, unconventional or insurgency warfare. (Shultz and Dew, 2009) Thus, terrorism is more of a verb than a noun, because it is a means to an end, and not the end itself. Although there are many examples of state terror, today it is a weapon of choice for the non-state actors when they do not have other means to confront the state.

The international community discredits terrorism as illegitimate doctrine that has no moral boundaries. Because of this, states tend to label all violent, non-state actors as terrorists. It is a certain way to discredit their effort and undermine eventual sympathies among people, at the same time to obtain states' rights to use violence to destroy them. There are numerous definitions of terrorism. However, there is a pattern that repeats in most of them: a terrorist is not a combatant, but a criminal; he uses all forms of violence indiscriminately; with the sole purpose of spreading fear and seeking an audience to gain attention; in order to enforce political or ideological agenda upon the governments.

The United Nations (UN) General Assembly Resolution 51/210 defines terrorism as "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them." (The United Nations, 1996)

The United Nations Security Council defines terrorism as "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable

by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.” (The United Nations, 2004)

The North Atlantic Treaty Organization (NATO) defines terrorism as “the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.” (NATO, 2014)

The European Union (EU) definition of terrorism is “an intentional act that may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organization to perform or abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.” (EU, 2002)

The US Federal Bureau of Investigation (FBI) defines terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” (Chase, 2013)

Table 1 shows the analysis of these definitions using comparison of the key words. Although the perception of terrorism is clear and most of the key terms repeat, each of the definitions has different weight. While the UN definitions describe terrorism as “unlawful use of force”, NATO and FBI define it as a “criminal act”. Both are correct and overlap as “unlawful act” is a crime. The EU definition does not mention neither, although it is implied that such “intentional act” is probably unlawful, aiming to damage, destabilize and destroy “structures” of a country, which furthermore implies that it is aimed against property. Also the EU definition defines that terrorist acts aim to intimidate the population, which implies “civilians”, but the specific term is used only in the FBI and UN Security Council definition. All institutions clearly define terrorism as an act with political purpose or objective. Only the UN definitions question the act to have unjustifiable motive.

NATO defines insurgency as “the actions of an organized, often ideologically motivated, group or movement that seeks to effect or prevent political change of a governing authority within a region, focused on persuading or coercing the population through the use of violence and subversion.” (NATO, 2011) The US military definition is shorter and omits that insurgents achieve political objective through coercion of population: “the organized use of subversion and violence to seize, nullify, or challenge political control of a region.” (DoD JP 1-02, 2016) Table 2 shows the analysis of these definitions using key words, and their comparison with the key words from the definitions of terrorism from Table 1.

Both definitions highlight that insurgents use subversion to achieve political objectives. Although there is no universally accepted definition of subversion as well, (Rosenau, 2007) most of them suggests that its purpose is “to undermine a governing authority,” (DoD JP 1-02, 2016) which implies that it is probably unlawful use of

force, thus a criminal act. Also, if the author interprets “coercing the population” in the NATO definition as “intimidation of the civilians”, then the only true difference between terrorism and insurgency would be if the cause is justifiable or unjustifiable. Even this raises the question of morality - does the end justify the means or, even if the act of violence is justifiable, it does not necessarily mean that it is not unlawful, and thus the state may treat it as a criminal act.

This is the main reason why most of the times the states refuse to recognize the threat as an insurgency, pursuing the policy to portray the adversaries as terrorists. In the historical context of the past century, most of the time insurgencies were popular movements that waged wars for national liberation. Today’s states are reluctant to use the term “insurgency” because it might suggest to the international community that they are waging a “just war” against the state. (Smit, 2005) The insurgents always lean toward waging “just” wars, thus the cliché of the most cited statement that “one man’s terrorist is another man’s freedom fighter.” (Weinberg, 2009)

However, one of the differences between terrorists and insurgents is the battle for “hearts and minds.” Insurgents fight to build legitimacy for their cause through gaining support from auxiliaries and the civilian population. The insurgents are not necessarily coercive toward the local population, while the terrorist tactics is gaining obedience through fear and terror. This means that while the government shape information using strategic communication through the media, usually the public opinion will have a significant role in labelling the group as insurgent or terrorist.

Besides obtaining sympathies from the civilian population, insurgents must earn legitimacy in the eyes of the international community as well. This cannot be done if the insurgents use unrestricted violence. Often the insurgent strategy is to portray themselves as freedom fighters, a marginalized group that uses violence against the state that oppresses them as a last resort. Insurgencies usually challenge the government when they do not have any other options.

For the state, this is a test and an opportunity to prove that the insurgents wage an unjust war, and their demands are unreasonable. However, while this can be done through dialogue and negotiations, the most common states’ fallacy is to declare the insurgents as terrorist, rejecting the possibility of negotiation to discourage their tactics. (Faure and Zartman, 2010) By doing this, a state often overthrows the possibility of a peaceful resolution and escalates the conflict. There are many historical examples when states at first label the insurgents as terrorist, just to negotiate peace after several years. (Reuveny, 2010) All this could be avoided if a simply more critical approach is used in identifying the root of the violence and different strategies are employed if the adversary is an insurgent and not a terrorist. Rushing to declare war on terrorism in cases when the group does not fully fit the profile usually escalates the conflict as the response towards the group is inadequate.

Among many attempts to define the difference between terrorism and insurgency, Mueller and Stewart even suggest that fundamentally they are not much different

except in the frequency of violence. (Mueller and Stewart, 2016) According to them, many internationally recognized insurgencies throughout the twentieth century “often applied massacre, random violence, dismemberment, assassination, propaganda bar-rages, sabotage, ambush, torture, rape, ethnic cleansing, summary execution, and even genocide...but they just weren’t called terrorists.” (Mueller and Stewart, 2016)

### **Consequences of the fallacy**

The semantics that is used in the strategic communications is important for shaping public opinion. It is a common strategic fallacy to use false semantics to describe the threat. Words are powerful and drive strategic policies, but also create prejudice and stereotypes. When the state labels an insurgency as a terrorist organization, it influences both public opinion and the mindset of the security forces. (Veljovski, 2010) This is often an intentional projection of the enemy profile that misleads the policy makers to choose proper ways and means. False assumptions lead to false decisions, or improper identification of the enemy will probably generate improper solutions.

Such reflexive response to label an insurgency as terrorism most of the time does more damage than good. When facing insurgencies, states rush to declare war on terrorism for several reasons. Primarily, this is a defensive response to disclaim the lack of readiness because everybody accepts that terrorism is unpredictable and difficult to prevent. Second, claiming that the state has a terrorist problem opens more opportunities to use force with moral support from the international community because it is a global security threat. To successfully defend itself from the insurgency, the state needs moral and legal support from other states to use force.

The state also chooses to label insurgency as terrorism to strip them from the right to negotiate on equal terms as combatants. It is more humiliating to have insurgency in the country than terrorism. To have an insurgency problem suggest that the state might have oppressing policies on certain group of people, because usually insurgencies emerge to overthrow the government, change the political system or redistribute the centres of power among ethno-religious groups. In many cases an insurgency fights to secede from the state. This is the reason why the state will tend to portray the insurgents as terrorists, but rarely the opposite.

The war on terror unites democracies and gives them moral strength in the war against barbaric, archaic methods that the terrorists use. All states seek and expect full international support in the war against terrorism. So, if a state acknowledges the problem as an insurgency, it risks raising questions. True democracy should not have a problem with an insurgency. All internal disputes and demands should be solved peacefully and in the legal boundaries of the state. Whenever an isolated group decides to rebel, there is immediate suspicion if the state actually uses all means to find a peaceful resolution. Ultimately, Clausewitzian “war is the continuation of politics by other means” (Howard et al. 1984) is set in motion and only by using force one can impose the will on another.



The states confront the threat differently if they declare war on terrorism or insurgency, either using the framework of the state criminal law or the international humanitarian law. It is believed that by declaring war on terrorism, the state will nullify their external support by labelling the group or organization as criminals, thugs, lowlife and murderers that cause unrestricted and unjustifiable violence. But, if the government admits they are confronting an insurgency, the international community may recognize the problem as an armed conflict and the insurgents as combatants, where the law of armed conflict applies. (Crawford, 2010)

To win a war, it is crucial to properly identify the enemy's center of gravity (CoG). Insurgents and terrorist have a different CoG, thus the state security forces should apply different operational approach. While the terrorists' CoG is mostly their leadership that organizes the network, the insurgents' CoG is the people. In cases when the insurgents are declared terrorists, the states' security forces risk to build prejudice that all locals that sympathise with them are also potential terrorists. This is particularly dangerous in multiethnic societies where the root of the problem is an ethnic strife and the insurgents are member of a certain ethnic group. If the population is treated as an enemy, it often generates more supporters and more insurgents. There is a significant difference in using security forces against insurgents or against the terrorists. By pursuing the war on terror, the state applies wrong tools in the counterinsurgency effort. In addition, if once the state declares war on terror, it is difficult to go back and convince its own population that the enemies are in fact, insurgents.

To understand the source of internal conflicts involving insurgencies, it is necessary to take in consideration concepts like sovereignty, separatism, irredentism, ethnicity, religion, theories of accommodation, etc. Sometimes the reason is pure nationalism defined as a condition in which the individual feelings of the citizens grow into bound duty, responsibility and loyalty either to the group or to the nation state. Usually most of the conflicts start due to the commitment of the people to their nation or the state. Yet there is no rational limit to which a minority group may invoke the right to self-determination within the state. (Castellino and Gilbert, 2003) It creates a series of legal contradictions that eventually may lead to conflict. In most cases, the majority group opposes separatism. Because of the increased role of the international community to provide global security, the emergence of any violence in a sovereign state often causes interference from the outside, when perceived as a threat to the regional stability.

Despite the development of the international law, many countries still do not have a solution to overcome the relationship of the state and nationalism and addressing the demands of smaller groups through an adequate social and cultural approach. As long as there are differences between groups encouraged by nationalism, there is a possibility of a conflict that might become violent. In ethnically heterogeneous states, groups can easily get polarized over economic and political power. In such scenario the smaller group, if marginalized, might seek equal share and divide the power and resources, engaging in armed rebellion against the monopoly of the state institutions from the larger group.

This is the most common recipe for insurgency movements. The strategic challenge is that in such conflicts there is a limit of tolerance and the accepted amount of damage that the groups can cause to each other. Once this line is crossed, it will take much longer time to forget the hostilities as internal wars tend to be extremely violent. This is the main reason why the state needs to deescalate internal conflicts. Among other policies, it is crucial not to confuse insurgency with terrorism and vice versa. (Smith, 2008)

### **Proposed model to identify terrorism**

According to the UN charter, the use of force to solve disputes in the international community is highly restricted. It is prohibited that the UN member states attack one other, and the states are only allowed to use force in self-defence against an armed attack. (The United Nations, article 51) However, since the Charter was signed in 1945, the prohibition of using force did not prevent the states to engage in numerous wars. (Schachter, 1984) This means that even in a conventional interstate conflict, at least one of the belligerents violated the UN Charter and unlawfully used force. Also, in every conflict there are always political or ideological objectives. Furthermore, war itself has an intimidating effect on all citizens in the society, a threat of casualties and destruction of property.

That being said, war in general is usually an unlawful use of force that serves a political purpose, designed to intimidate the opponent's society to break its will to fight, almost always causing collateral damage to civilians and property. Most of the definitions of terrorism are deliberately broad to cover as many possible patterns to identify terrorism. However, this either unintentionally misguides the states, or allows them to be selective when determining if the act is terrorism or not. That is why every definition of terrorism needs the crucial indicator if the violence is a terrorist act: Terrorists deliberately kill civilians. Not as a collateral damage, but as planned, designated, direct targets.

Chart 1 demonstrates an attempt to improve the definition of terrorism. The proposed model is an algorithm that critically examines if the individual, group, organization, even a state, is committing an act of terrorism. The essence of the model is that if there is a pattern of deliberate killing of civilians as a strategy, it is undoubtedly 100% an act of terrorism.

Step 1. When an act of violence is committed, the first step is to answer the question of motive: Is there a clearly defined end state that has either political or ideological purpose?

If the answer is NO, then the act of violence is not an act of terrorism. There are many cases of violent acts performed by individuals or groups that do not have any political, nor ideological motives. There are people that commit violence driven from a wide range of other motives like thieves, murderers, violent criminals, psychopaths,

serial killers, etc. Many violent acts have never resolved why people did it. For example, the suicidal co-pilot that crashed the Germanwings flight 9592 in 2015 killing all passengers aboard did not have any political or ideological motive. His act was simply murder caused by personal grievances. Cases of mass shootings in schools in the US performed by frustrated teenagers are not a terrorist attack as the motive is personal. The list goes on with many examples where the violent act is simply a violent act.

Step 2. If the answer is YES, and the violence is committed with a political or ideological purpose, the next question is if there are civilian casualties?

If the answer is NO, then the act of violence is not an act of terrorism. The perpetrators of politically or ideologically motivated violence that aim at the security forces of a state (police or military) can have different labels: revolutionaries, insurgents, rebels, guerrillas, extremists, radicals, mercenaries, criminals, political or religious fanatics, etc. The fact that they do not target civilians does not mean that the act of violence is not an unlawful criminal act. However, if any group that pursues politically or religiously motivated end state and have a strategy not to target civilians, but only target uniformed security forces or their infrastructure, is a sign that they accept the law of armed conflict and treat civilians as non-combatants. It should not be confused with terrorism, even if their cause is unjust. One state's security forces (police and military) are armed for violence, and thus represent legitimate targets in war, even in an unjust one.

Step 3. If the answer is YES, and there are civilian casualties as a result of acts of violence committed with a political or ideological purpose, the next question is if the civilian casualties are deliberate?

If the answer is NO, then the act of violence should not be treated as an act of terrorism. There are many cases of collateral damage in war. Almost in every war most of the casualties are civilians, which is not necessarily a case of terrorism. Even the states' legitimate, security forces sometimes make mistakes and kill civilians. Accidental civilian casualties, even because of negligence are not enough to label the perpetrators as terrorists. There is much evidence of members of the security forces in many situations inflicting civilian casualties especially in urban warfare. Of course, this does not mean that violent groups and individuals that target state security forces and cause civilian casualties should not be held accountable according to state laws.

Step 4. If the answer is YES, there is strong evidence that the act of violence may be an act of terrorism. There still is one more question to confirm: Is there a pattern in the deliberate killing of civilians as defined strategy?

If the answer is NO, the act of violence is not necessarily a terrorist act. There are many cases of individuals or fractions of insurgents that choose this path, but it is not the official strategy of the group or organization. If killing civilians is not a common practice, but isolated incident from rogue individuals or fractions, this might not be a terrorist act, rather criminal outlaw behaviour. To support this thesis, there is

much evidence when soldiers deliberately kill civilians in a moment of stress, personal grievances or shock. Such incidents are treated as a war crime and punishable by law, but it is not an act of terrorism, but simply murder - a human rights violation. The non-state actors should be treated the same way. Isolated incidents should not be used to label a group as terrorist, if that is not their official strategy to pursue political and ideological objectives.

However, if the answer is YES, and there is a pattern in the deliberate killing of civilians as part of the groups' strategy, such action is clearly an act of terrorism. Killing of civilians as tactics is the essence of terrorism. Terrorist groups and organizations do not hide that they kill civilians. It is often in their official agenda, encouraging their followers to target civilians as combatants. Vivid example is the second fatwa that Al-Qaeda published on 23 February 1998, urging the followers "to kill the Americans and their allies, civilians and military..." (The Heritage Foundation, 2016) This indiscriminate tactics is the proof that the terrorists pursue their politically or ideologically motivated end state through means of terror on civilians.

## **Conclusion**

While insurgencies use violence to achieve political or ideological objectives, usually they lean toward using restricted violence because in order to be successful, insurgents need to gain legitimacy and public (international) support. In contrast, terrorists do not care about legitimacy, and tend to use unrestricted violence deliberately targeting civilians. Most of the states could benefit from accepting a simple algorithm that will differentiate if the security threat is insurgency or terrorism.

First, it brings the international community closer to agree upon universally accepted definition of terrorism, because even among allies, there is uncertainty. If this is achieved, there will be fewer ambiguities in the international politics when it comes to declare a terrorist individual, group, organization or state.

Second, in order to defeat either insurgency or terrorism, the states and their security forces need to apply adequate strategy and tactics. Counterterrorist and counterinsurgency operations may overlap in certain elements, but generally use different ways and means to achieve the end.

Third, having a clear definition of terrorism could be a deterrence strategy to protect civilians, projecting an international message to all potential insurgencies to reconsider their strategy and tactics considering civilians. Insurgents that choose to deliberately target civilians should know that they will be treated as terrorists.

Forth, it can help isolate and marginalize the terrorists from potential supporters and sympathizers. Not having a universally accepted definition is one of the reasons why terrorism is flourishing. It allows state and non-state actors to use terrorism as a convenient tool, concealed as an insurgency.

Although it is not likely that terrorism will perish as tactics in the near future, it is essential to treat the deliberate killing of civilians as an ultimate crime. Not being able to agree upon a universally accepted definition of terrorism is concerning, suspicious and provokes the question why the international community does not close this security gap.

## Appendix I – Tables

	Unlawful use of force	Criminal act	To intimidate	Against civilians	Against persons or individuals	Against property	Political purpose or objective	Unjustifiable act
UN General Assembly		x			x		x	x
UN Security Council		x	x	x	x		x	x
NATO	x		x		x	x	x	
EU			x				x	
FBI	x		x	x	x	x	x	

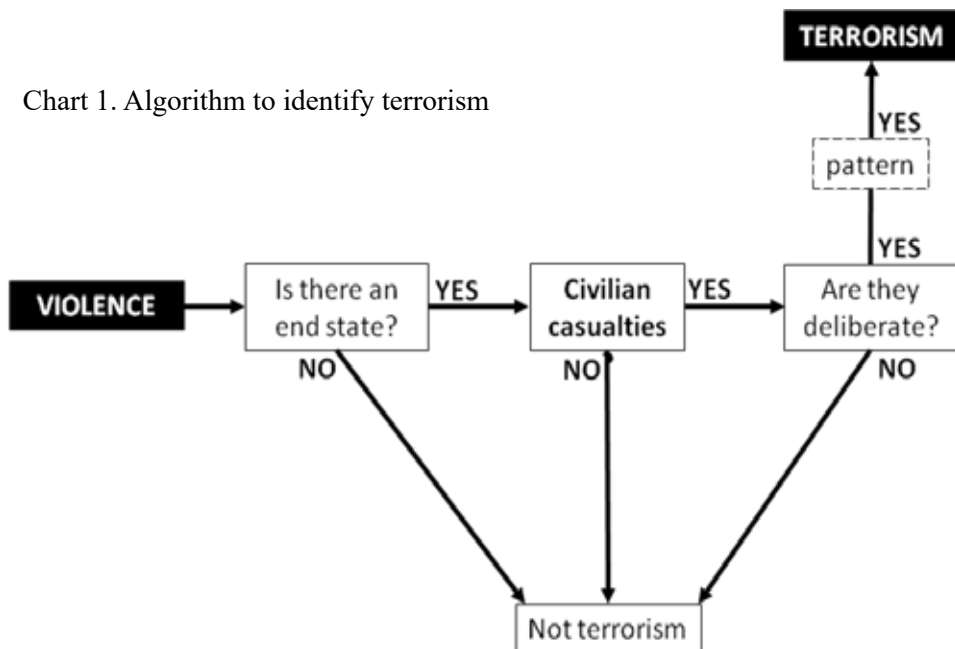
*Table 1. Analysis of definitions of terrorism*

Terrorism	Unlawful use of force	Criminal act	To intimidate	Against civilians	Against persons or individuals	Against property	Political purpose or objective	Unjustifiable act
Insurgency	Subversion and violence		Coercion of population		Against government authority			
NATO	x			x		x	x	
US military	x			x			x	

*Table 2. Comparison of definitions of terrorism and insurgency*

## Appendix II – Chart

Chart 1. Algorithm to identify terrorism



## REFERENCES:

- Bhonsle, K. Rahul, *Countering Transnational Terrorism* (Vij Books India Pvt Ltd, 2011 Aug 10):22.
- Chase, Eric, "Defining Terrorism: A Strategic Imperative", *Small Wars Journal* (Jan 24 2013).
- Decision, has adopted this framework, "Council Framework Decision of 13 June 2002 on combating terrorism" (Official Journal L 164, 2002):3
- Department of Defense, *Dictionary of Military and Associated Terms* (Joint Publication 1-02, 8 November 2010, as Amended Through 15 February 2016).
- Durschmied, Erik, *Blood of Revolution: From the Reign of Terror to the Rise of Khomeini* (Vol. 1964, Arcade Publishing, 2002).
- Emily, Crawford, *The treatment of combatants and insurgents under the law of armed conflict* (Oxford University Press, 2010): 128.
- Havialand, Smith, *Defining terrorism: it shouldn't be confused with insurgency* (American Diplomacy, 9 Dec 2008).
- Joanna, Kulesza, *Due Diligence in International Law* (Brill, 2016 Aug 8): 281.
- Joshua, Castellino, and Gilbert, Jérémie, *Self-determination, Indigenous Peoples and Minorities* (Macquarie Law Journal 3, 2003): 155.
- Laurent, Steven and Menzies, G. Ross, *The Anger Fallacy: Uncovering the Irrationality of the Angry Mindset* (The Anger Fallacy: Uncovering the Irrationality of the Angry Mindset, 2013: vi).
- Leonard, Weinberg, *Global terrorism* (The Rosen Publishing Group, 2009): 8.

- Michael, Howard, Paret, Peter, and West, Rosalie, Carl Von Clausewitz: On War (Princeton University Press, 1984): 87.
- Mueller, John and Stewart, Mark, Conflating Terrorism and Insurgency (The Lawfare Institute, February 28, 2016).
- NATO, Allied Joint Doctrine for Counterinsurgency (COIN) – AJP-3.4.4 (February 2011).
- NATO Glossary of Terms and Definitions (AAP-06 Edition 2014).
- Oliver, G. Faure and Zartman, William, Negotiating with terrorists: strategy, tactics, and politics (Routledge, 2010): 197.
- Oscar, Schachter, The right of states to use armed force (Michigan Law Review, 1 Apr 1984, 82(5/6): 1620-46.
- “Al-Qaeda: Declarations & Acts of War”, The Heritage Foundation. <http://www.heritage.org/research/projects/enemy-detention/al-qaeda-declarations> (accessed on 30 Nov 2016).
- Rafael, Reuveny, Coping with Terrorism: Origins, Escalation, Counterstrategies, and Responses (Sunny Press, 2010): 247-250.
- Shultz, H. Richard and Dew, J. Andrea, Insurgents, terrorists, and militias: the warriors of contemporary combat (Columbia University Press, 2009).
- The UN Charter, Chapter VII, article 51.
- The United Nations (UN) General Assembly Resolution, A/RES/51/210 (17 December 1996).
- The United Nations (UN) Security Council resolution 1566 (8 October 2004).
- Veljovski, Gjorgji, “The Effectiveness of the Counterinsurgency Operations during the Macedonian Conflict in 2001” (Army Command and General Staff College Fort Leavenworth KS, 2010): 80.
- William Rosenau, Subversion and Insurgency: RAND Counterinsurgency StudyÑPaper 2 (Rand Corporation, 6 March 2007): 4-5, at [http://www.rand.org/content/dam/rand/pubs/occasional\\_papers/2007/RAND\\_OP172.pdf](http://www.rand.org/content/dam/rand/pubs/occasional_papers/2007/RAND_OP172.pdf) (accessed on 30 Nov 2016).
- Wim, Smit, Just war and terrorism: the end of the just war concept? (Peeters Publishers, 2005): 126.





## THE INF TREATY - CROSSROADS OF INTERNATIONAL NUCLEAR STABILITY

Bojan MIKLOSH<sup>1</sup>  
Lazar DJUROV<sup>2</sup>

**Abstract:** *This article addresses the INF Treaty issue from a perspective enlarged with China's position, the New START agreement, and the broader political context in negotiating a solution. By understanding the history of the infamous Treaty from the Cold War, the article tends to answer the key questions regarding this issue: Why did the INF Treaty collapse and was the end of it anticipated? What is the Russian side of the story? What is the Chinese perspective and how is China affected by it? What should be expected in the future negotiations? The INF Treaty issue should not be perceived as an isolated bilateral misunderstanding between the U.S. and Russia. Hence, the negotiation process directed to resolving this issue is expected to encompass a broader political perspective in order to find the best suiting solution.*

**Keywords:** *nuclear tensions, international relations, armament, ballistic missiles.*

### Introduction

“For the first time in many years, arms control and disarmament are headline news – for the wrong reasons. One of the major achievements of international diplomacy is in grave danger. Decisive action is needed” (Guterres, 2019). This statement of the Secretary General of the United Nations addresses the latest nuclear issue between the United States and Russia – the collapse of the Intermediate-Range Nuclear Forces Treaty. The INF Treaty as the most important segment from the Cold War, and the paramount aspect of ending the arms race between the blocs, thirty years later resurfaced and reminded the international community of its essential role in maintaining world peace. Considering the contemporary security context, built by the international relations, country aspirations and national political agendas, this issue opens many aspects of discussion and contemplation. After the annexation of Crimea in 2014, the cooperation between the United States and Russia, as well as between NATO and Russia deteriorated substantially. In the same period, the Obama administration revealed information about the development of Russia's SSC-8 (9M729 system), a ground-launched cruise missile which breached the INF Treaty's provisions. Not only did this reopen a decades old issue, but it also drew the attention of the world to it. That is why, in order to understand the future of the INF treaty, its history should be taken in consideration.

---

<sup>1</sup> MSc of Strategic and Defense Studies

<sup>2</sup> Professor at the Military Academy “General Mihailo Apostolski”-Skopje

## Overview of the INF Treaty history

The 70's of the past century were known as a period in which the countries of the world, especially those from the Eastern and the Western bloc were enjoying the period of „détente“ in which the tensions among the two blocs were considerably lowered<sup>3</sup>, and diplomacy played a key role in the pursue of peaceful and transparent solutions of the eventual issues to come.

The thing that brought back the focus of NATO on the Soviet Union activities, was the deployment of 200 RSD-10 Pioneer (SS-20 Saber) missile systems on the territory of Eastern Germany. In this regard, the German Chancellor Helmut Schmidt expressed concern for the need of a NATO response to this security issue, pointing out two aspects: 1) the fact that wherever the missile systems were to be deployed, they would have an effect on every European capital, considering that the systems are effective in a 2300 kilometer radius; 2) in order to establish a nuclear balance in Europe, the burden of the issue should be carried equally by the European allies, considering that, at the time, aside from the U.S., the other NATO members did not have such a sophisticated nuclear arsenal.

The proposed solution consisted of deployment of 464 GLCM (Ground Launch Cruise Missiles) and 108 Pershing 2 systems<sup>4</sup> on the territories of Germany, Great Britain, the Netherlands and Italy. Reagan's presidency turned out to be a very influential and beneficial moment in this tense situation and contributed to the beginning of the end of the biggest nuclear crisis in history. Reagan's diplomatic capability, especially his tailored “zero-zero approach”, adequately contributed in the case of withdrawal of the Soviet missile systems on world level. This proposal consisted of means where NATO would not deploy its Pershing 2 systems, under the condition that the Soviet Union destroyed its already deployed missile systems.

Although Reagan's statement was welcomed with a high dose of skepticism and disbelief, the good will for cooperation of the new President of the Soviet Union – Mikhail Gorbachev, right after he took the function in 1985, flowed a substantial amount of faith and optimism to the world political authorities, especially those of NATO. Soon, in 1986 the possible elimination of all nuclear potentials until the year 2000 was discussed. This was an overture of what followed in 1987 – the official signing of the infamous Intermediate Range Nuclear Forces Treaty, between the United States and the Soviet Union<sup>5</sup>.

Not only did this agreement eliminate the Soviet SS-20 and the American Pershing 2 systems, but it also eliminated the Soviet SS-4 and SS-5, and the American

---

<sup>3</sup> Nato. “A Short History of NATO.” NATO. Accessed April 27, 2020. [https://www.nato.int/cps/en/natohq/declassified\\_139339.htm](https://www.nato.int/cps/en/natohq/declassified_139339.htm).

<sup>4</sup> Nato. “1979: The Soviet Union Deploys Its SS20 Missiles and NATO Responds.” NATO, January 9, 2013. [https://www.nato.int/cps/en/natohq/opinions\\_139274.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/opinions_139274.htm?selectedLocale=en).

<sup>5</sup> Nato. “NATO and the INF Treaty.” NATO, 2 Aug. 2019, [www.nato.int/cps/en/natohq/topics\\_166100.htm](http://www.nato.int/cps/en/natohq/topics_166100.htm).

Pershing 1. All this presented in numbers resulted in elimination of about 1,846 of these systems, followed by the withdrawal of nearly half a million Soviet troops from Eastern Europe, while according to the agreement, the United States was obliged to destroy 846 of its own missile systems, or 2,692 from both parties<sup>6</sup>.

Until this moment, the history had not recorded a bilateral agreement with such importance, which binds the parties of eliminating a whole class of the most modern and sophisticated armament in that period. Also, Gorbachev and Reagan agreed on openly sharing information upon which the Soviet Union granted secure flyovers of NATO aircrafts on its territory in order to observe the withdrawal and destruction of the systems, ensuring thus that both parties abide by the signed agreement. Although until then, this treaty was held to be an unseen political success, from today's perspective it can be concluded that this historical agreement officially marked the beginning of the end of the Cold War.

### Today's issue

Few decades later, in a period when the world saw terrorism and militant Islamism as the biggest threats to world security, in 2013, the Obama administration uncovered information which shifted the attention from terrorism to nuclear weapons again. Washington pointed out a possible Russian breach of the INF Treaty from 1987, based on the provided intelligence about the deployment of the Russian SSC-8 (9M729 system). This immediately caused unrest among the international community and the political authorities, to that extent that this was discussed at the Wales Summit in 2014 and the Warsaw Summit in 2016, at both calling Russia back to compliance to the treaty. Russia categorically denied all accusations, until 2017 when the existence of the SSC-8 system was admitted, followed by an explanation that it does not jeopardize the Treaty's provisions.

This statement was unacceptable for both NATO and the U.S., therefore every NATO member country expressed its concern about the development of the SSC-8 systems, and unanimously agreed that Russia violated the Treaty with its actions.

Russia's behavior did not change, so the United States started actively seeking a solution that would be measured (at the same level) to Moscow's actions. Hence, in October 2018, Washington announced that the U.S. is considering a withdrawal from the INF Treaty in accordance with Article 15 "Each Party shall, in exercising its national sovereignty, have the right to withdraw from this Treaty if it decides that extraordinary events related to the subject matter of this Treaty have jeopardized its supreme interests. It shall give notice of its decision to withdraw to the other Party six months prior to withdrawal from this Treaty"(INF Treaty, 1987). This will practically give Russia a period of six months to return to compliance to the treaty.

---

<sup>6</sup> Ibid.

The U.S. statement about ending the Treaty, was favorable for Moscow to some extent. As was expected, Russia stood its ground about their claims about not breaching the Treaty, so on the 1<sup>st</sup> of February 2019 the United States announced that they will execute its right granted by Article 15 of the Treaty. This was also in Russia's agenda of handling this issue. A month later after the U.S. announced that it was withdrawing from the Treaty, on the 4<sup>th</sup> of March 2019 Russian President Putin signed a decree which suspended Russian compliance with the INF Treaty and entered the six-month period of withdrawing from the treaty, as they claimed by mirroring the step of the United States<sup>7</sup>.

### **The end was expected**

Although Moscow's rhetoric gave serious indicators that one should expect in the near future that the eastern party of the Treaty will suspend its compliance, still this was a complex claim and even the thought of it happening was dangerous.

In 2007, at the Munich Security Conference, Putin pointed out the responsible step the United States and the USSR took by the INF Treaty, but at the same time expressed concern about the INF Treaty lacking a universal character. He elaborated that many other Asian countries possess, work on and plan to incorporate intermediate-range and short-range missiles as part of their weapon arsenal, but "only the United States and Russia bear the responsibility not to create such weapons systems"(Putin, 2007). The same year, Russian officials suggested to their counterparts in the George W. Bush administration that the two countries withdraw from the treaty, as former U.S. Defense Secretary Robert Gates wrote in his memoir (Colina, 2014). The main indicators materialized in 2016, when in a period of one month, three agreements addressing the US – Russian regulations on nuclear safety and security were suspended: The Plutonium Management and Disposition Agreement signed in 2000; The Research agreement on nuclear energy signed in 2013<sup>8</sup>; and The Deal on the conversion of six Russian research reactors signed in 2010<sup>9</sup>.

Another element worth of consideration, regarding the suspension of the Plutonium Management and Disposition Agreement is the fact that in the draft law

---

<sup>7</sup> Rfe/rl. "Putin Officially Suspends Russia's Participation In INF Treaty With U.S." RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 4, 2019. <https://www.rferl.org/a/putin-officially-suspends-russia-s-participation-in-inf-treaty-with-u-s-/29802816.html>.

<sup>8</sup> "United States, Russia Sign Agreement to Further Research and Development Collaboration in Nuclear Energy and Security." Energy.gov, September 16, 2013. <https://www.energy.gov/articles/united-states-russia-sign-agreement-further-research-and-development-collaboration-nuclear>.

<sup>9</sup> "Russian Research Reactors May Convert to LEU." World Nuclear Association - World Nuclear News, December 9, 2010. [https://www.world-nuclear-news.org/RS-Russian\\_research\\_reactors\\_may\\_convert\\_to\\_LEU\\_fuel-0912104.html](https://www.world-nuclear-news.org/RS-Russian_research_reactors_may_convert_to_LEU_fuel-0912104.html).

proposed by Russian President Vladimir Putin to the parliament, there was an outline of conditions which included lifting U.S. sanctions against Russia enacted in response to Moscow's actions in Ukraine, compensating Russia for the damage caused by the sanctions, and reducing the U.S. military presence on the territory of NATO member states that joined the Alliance after 2000" (Kingston, 2016). This behavior outlines the framework of expected behavior that should be taken in consideration in future negotiations.

As some were focusing on the necessity of reestablishing these agreements, others have translated this behavior as a threat to European and global security order and stated that therefore the West (that is, NATO) was no longer bound by agreements such as the INF treaty (Kühn, Péczeli, 2017).

Thus, two conclusions can be drawn – firstly, the violation of the INF Treaty can be seen as the last and at the same time most symbolic point in the sequence of Russian suspended nuclear agreements with the U.S., and secondly, Moscow's solution may consist of elements that address some other issues connected with the broader Russian politics and interests.

## The Russian perspective

From the first time the Obama administration announced that Russia has breached the INF Treaty, Moscow has been denouncing all accusations as unfounded, accusing at the same time the United States of its false and unfounded claims. For Russia, the issue addressing this kind of weapons, originates from 2002 when Washington withdrew from the Anti-Ballistic Treaty, which was regarded as a substantial factor in curbing the race in strategic offensive arms (Daryl, Reif, 2017). This Treaty allowed the two parties to deploy two fixed ground-based defense sites equipped with one hundred ABM launchers and interceptor missiles, one to protect the States' capitals and one to protect the intercontinental ballistic missile field<sup>10</sup>. In 2018, Russian President Vladimir Putin explained the Russian perspective on the issue by three aspects.

Firstly, he accused the United States of breaching the INF Treaty with the approval of the budget for research and development of intermediate-range and short-range missiles by the U.S. Congress. According to him, this indicated that Washington had already made a decision by approving the expenses implying taking further action.

Secondly, he expressed his concern about the Aegis system which is part of NATO missile-defense system. NATO states that the Aegis system is to be used only in defensive manner, and does not provide any offensive capability<sup>11</sup>, but Russia rejects

<sup>10</sup> "Treaty Between the United States of America and the Union Of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems", May 26, 1972, [https://media.nti.org/documents/abm\\_treaty.pdf](https://media.nti.org/documents/abm_treaty.pdf)

<sup>11</sup> Nato. "Aegis Ashore Ballistic Missile Defence System in Romania Completes Scheduled Update." NATO, August 8, 2019. [https://www.nato.int/cps/en/natohq/news\\_168377.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_168377.htm?selectedLocale=en).

this explanation. Therefore, Putin stated that the system is compatible for offensive engagement only if the proper software for such use is installed (Putin, 2018). Another perspective of this issue may be provided through the Russian military strategy, where NATO's location of its military infrastructure closer to Russian borders<sup>12</sup> is considered as a threat to national security.

Thirdly, the U.S. continuous use of Unmanned Aerial Vehicles (UAV), which “don't differ from Intermediate-range and short-range missiles at all” in terms of their capability for carrying nuclear warheads at the same distance as the INF missiles.

Furthermore, Russia has also asserted that many countries in its neighborhood possess IBMs and Russia does not. This statement does not imply the vulnerability of Russia to a possible threat in terms of the possession of such weapons, but the lack of such weapons in Russia's inventory. According to this, Moscow perceives all Asian countries with nuclear armament as a possible threat to its national security, although Russia has the largest nuclear armament in Asia, both qualitatively and quantitatively.

For example, China is the third largest nuclear- power in the world and intends to double its nuclear potential in the future<sup>13</sup>. Even if this were to happen, still China would not be even near both quantitatively and qualitatively to Russia's arsenal. Even though there are certain claims that Chinese economy is not the only worry of Moscow, and that China would not remain indifferent if Russia marks a significant buildup in its military power and would respond measurably (Pifer, 2016), the Sino-Russian cooperation is still very strong and exceeds the possibility of that taking place. Among other Central Asian states (Blank, 2013), both Russia and China are part of the Shanghai Cooperation Organization, and from Russian perspective, China is seen as a permanent strategic partner, and “a key factor of the maintenance of global and regional stability”<sup>14</sup>, as pointed out in the Russian National Strategy.

## **The Chinese Perspective**

China has not agreed on any restrictions on its nuclear arsenal, nor the ICBMs, unlike the United States and Russia, but is very vocal on criticizing the U.S. withdrawal from the INF Treaty. China is a country which believes that “the nuclear force is a strategic cornerstone for safeguarding national sovereignty and security”<sup>15</sup>.

---

<sup>12</sup> Decree N 683 of the President of the Russian Federation, *The National Security Strategy of the Russian Federation*, 31 December 2015, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.

<sup>13</sup> Rfe/rl. “U.S. Official: New START Treaty Should Cover Russian Weapon Systems Under Development.” RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 10, 2020. <https://www.rferl.org/a/us-official-new-start-treaty-should-cover-russian-weapons-systems-under-development/30479166.html>.

<sup>14</sup> *The National Security Strategy of the Russian Federation*, p.25.

<sup>15</sup> The State Council Information Office of the People's Republic of China. 2015. China's Military Strategy (2015), Beijing, <https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf>.

After the Trump administration took office, the relations with Beijing became more tense over myriad of questions mostly in the field of economics, but after the United States announced the withdrawal from the INF Treaty, China did not hesitate to express its dissatisfaction with Washington's decision. A simple explanation why China commented on the U.S. withdrawal from the INF Treaty is the fact that China advocates the view that it will never be the first to use any nuclear weapons, to enter in an arms race with another country, and at the same time, it will channel its diplomatic means to deter other countries from using or threaten to use nuclear weapons against China (China's Military Strategy, 2015). A solid fact is that this kind of behavior is provided in its military strategy, although it is not clear why there is no official opinion in terms of Russia's development of the SSC-8, which is the very essence of the issue about the INF Treaty. This connects to the strong traditional Sino-Russian relations, and the mutual/ similar views on American world politics, which is why China did not stay mute on the U.S. bold steps away from the agreement. From Beijing's aspect, this could present the initial move to a larger threat to China's national security, for several reasons.

Firstly, the United States nurtures and develops its bilateral relations with South Korea and Japan especially well (Baklitskiy, 2019). Beijing fears that, if the situation escalates, this cooperation will open the opportunity for these countries to allow the deployment of the American missile systems on their territory, which was prohibited by the INF Treaty<sup>16</sup>. This without a doubt will be recognized as a threat to China, which will intensify the tensions between the countries and will endanger the security of South-East Asia. This action will put a huge burden of responsibility on the United States, because if Washington decides on such a move, then North Korea will inevitably enter this equation.

Secondly, the withdrawal from the INF Treaty will lift the prescribed restrictions, and the two parties will again have the opportunity for uninterrupted development and widening of the already vast nuclear arsenal. This is China's second greatest concern, with respect to the United States rather than Russia. This issue has its qualitative and quantitative aspect for China. Considering the quantitative aspect, on the one hand, China has not agreed on any restrictions, and could enlarge its number of nuclear weapons, as well as ICBMs uninterruptedly. On the other hand, this will mean the same for the United States. The qualitative aspect is the one that concerns China more, because "if the United States shows that it is ready to put under threat Chinese strategic nuclear forces, including its submarines" (Baklitskiy, 2019), China would respond with doctrinal changes in regard to its current nuclear forces' strategy, which is based on deploying the bare minimum necessary to carry out a retaliatory strike in

---

<sup>16</sup> "Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles", December 8, 1987, <https://2009-2017.state.gov/t/avc/trty/102360.htm#diplomaticnotes>



order to maintain its national security (China's Military Strategy, 2015).

The Chinese attitude towards the INF Treaty challenge is not under the scope of the United States. Recently, the Trump administration has said it wants an extension of New START to also include China<sup>17</sup>, which would be a huge success, although the possibility of it happening is low. China is a serious military force, and a key factor in the East-Asian, and world politics, but in terms of nuclear weapons is far less equipped than the U.S. or Russia. With its modest nuclear inventory of around 300 pieces of nuclear warheads in its stockpiles (Kingston, Davenport, 2019), one cannot expect that China would agree on any restrictions regarding this matter. A much bigger success would be if China agrees on raising its transparency near the level of the U.S. – Russia relations on this matter. This will form the prerequisite for further strengthening the transparency, which then may be succeeded by an agreement similar to the New START. Even the rise of China's transparency level regarding its nuclear forces is questionable, since Beijing sees this as its vulnerability that needs protection the most, and at the same time, exactly this increases the uncertainty of other parties (Wu, 2016).

### **Negotiating a solution**

As elaborated before, the INF issue between the United States and Russia has a myriad of security dimensions, many perspectives and covers a very specific topic which is of colossal importance to the nuclear weapons control, but ironically enough it has only one solution – keeping the deal or negotiating a similar one.

The roughness of the path of negotiating a solution will be determined by Russian politics, but the direction of the negotiations will be the responsibility of the diplomatic skill set of the US and NATO. The UN Secretary General called upon the two parties of the treaty several times to lower the tensions and discuss a possible solution, reminding that today's world "cannot afford to return to the unrestrained nuclear competition of the darkest days of the Cold War" (Guterres, 2019). He also encouraged them to extend the New START treaty, praising its value, meaning and contribution to world security and nuclear stability. In 2019 the parties were also called to lower the tensions, by the man who did that himself in the eighties, the last Soviet President Gorbachev, reminding that "as long as weapons of mass destruction exist, primarily nuclear weapons, the danger is colossal. All nations should declare that nuclear weapons must be destroyed"(Gorbachev, 2019).

Considering the current situation, it is clear that Russia is ready to discuss the issue with the United States. Moscow believes that "the treaty is one of the most important instruments for maintaining international security and stability and that it is

---

<sup>17</sup> Rfe/rl. "U.S. Official: New START Treaty Should Cover Russian Weapon Systems Under Development." RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 10, 2020. <https://www.rferl.org/a/us-official-new-start-treaty-should-cover-russian-weapons-systems-under-development/30479166.html>.

very important to preserve it”<sup>18</sup>. Furthermore, they are ready to work with Washington without any hesitation. It is inevitable that tabling the problem will take place, because not only is this a too important and sensitive topic, just to be seen as a bilateral misunderstanding, but it is too important an issue to be left unsolved at all.

When discussing a possible solution, Brussels and Washington must choose if they are going to deal with this issue symptomatically by addressing the INF Treaty tensions separately, or to delegate a comprehensive solution that will address the overall aggressive behavior of Russia. Just as this problem cannot be addressed as an isolated U.S.-Russia issue, so it cannot be isolated from the broader Russian politics. This means that Russian diplomacy will even try to ease the tensions or to negotiate acceptance for the Crimea annexation of 2014, as part of its conditions for the deal. A similar thing happened in 2010 with Putin’s outline of conditions within the draft law.

For now, the New START is the last and only agreement between the United States and Russia, addressing the nuclear arsenal topic, and it will expire in February 2021. According to the provisions of this Treaty, it may be renewed for up to five years if both sides agree<sup>19</sup>. This agreement provides not only rigorous mutual inspections, but also limits the number of launching systems the nuclear triad is allowed to have, including submarine- and land-based ballistic missiles and strategic bombers (Sittlow, 2020). **Bottom of Form**

In regard to the ongoing issue, this agreement provides a legislative-backed-up time framework in which the possible changes are expected, meaning that the next critical point for a solution is February 2021. Until then, both Moscow and Washington need to work on solutions, and to find common ground about the issue. Currently, Moscow is ready for cooperation and agreed on extending the New START, although it did not assert if there are any additional conditions. One specific condition expected by Moscow in regard to the extension of the New START is to encompass the reduction of UAVs, which Putin mentioned in 2018, as military means of having similar capabilities as the intermediate-range missiles.

The U.S. already announced their strive to include China, as well as that there is a possibility for the new agreement to expand and encompass “new systems such as the nuclear-powered, underwater, nuclear-armed drone called Poseidon; the nuclear-powered, nuclear-armed cruise missile, air-launched ballistic missile”<sup>20</sup>. Although some think that it would be profoundly unwise and undesirable to link the extension of the

---

<sup>18</sup> “Astana: Putin and Others Meet For CSTO Summit; Nuclear Security in Jeopardy Because of US!”, YouTube video, 4:05,”Vesti News,”November 09, 2018.

<sup>19</sup> “Treaty Between The United States Of America And The Russian Federation On Measures For The Further Reduction And Limitation Of Strategic Offensive Arms”, April 8, 2010, <https://2009-2017.state.gov/documents/organization/140035.pdf>

<sup>20</sup> “Briefing With Senior State Department Official On the New START - United States Department of State.” U.S. Department of State. U.S. Department of State, March 9, 2020. <https://www.state.gov/briefing-with-senior-state-department-official-on-the-new-start/>.

New START Treaty to the fate of the INF (Katarzyna, 2018), at this moment both parties agree that it is the last legislative document that bounds them on this issue. Therefore, if the INF Treaty cannot be reestablished, then, not only should the New START be renewed, but it should be carefully expanded especially in terms of armament limitation, reduction and control. Thus, this agreement will serve as the main guarantee of arms control between the parties.

If Russia and the U.S. find common ground, that would form a strong basis for future dialogues and bring the other countries that possess nuclear armament into a process of control and reduction. The Russia and the United States issue is the first checkpoint on the path of nuclear armament control and security in the world. Their collaboration and positive example, which will derive from their discipline in compliance, will be the main guarantee of world nuclear security.

This period also represents a unique opportunity to bring China to join an arms control process, since Beijing did not hesitate to express its concerns about the U.S. INF Treaty withdrawal. At the same time, it is unimaginable that China would join the arms control process if the U.S. and Russia walked away (Pranay, 2019). China has a small number of nuclear weapons compared to that of Russia or the United States. Its strategy of employing these weapons lays on the thesis of last means for nuclear deterrence and retaliatory strike. Beijing's agreeing on any restrictions is highly doubtful, as is its agreement on raising the level of nuclear transparency. This is because China believes that the disclosure of any information regarding its nuclear armament "could undermine China's nuclear deterrence... and because rival powers could use this knowledge to launch a disarming strike on China" 238. In the long run, China agreeing to restrictions such as the ones in the New START is only possible if it first agrees on raising the level of its nuclear transparency. The New START extension is an opportunity to make the first step toward bringing China close to a future negotiation.

## **Conclusion**

After more than three decades, the nuclear armament issue is again on the agendas of world security and stability. The INF Treaty as a most remarkable agreement which put an end to the Cold War was breached by the development of the Russian SSC-8 (9M729 system) and triggered a process of accusations, denial, disbelief and nuclear tensions between the United States and Russia. Both countries withdrew from the Treaty even though the whole world expressed its concern about that. Considering the domino effect of termination of agreements, starting from 2002 with the termination of the Anti-Ballistic Treaty, the withdrawal from the INF Treaty could be anticipated, taking into consideration the Russian way of politics.

Without re-establishing compliance to the Treaty, or signing a similar one, the United States and Russia could expand their nuclear arsenal uninterruptedly, which would open new questions and issues on the international political scene, and will rise to the top of the list of priority threats to world security. This precisely represents the urgency of dealing with this matter, enhanced with the expressed concerns from China, the United Nations, and NATO.

The last remaining agreement addressing the topic, the New START cannot be isolated from the scope of the issue. On the contrary, it should be regarded as an opportunity that needs

to be seized in order to maintain the control on the arsenal of the United States and Russia. The U.S. ambitions on including China in the Treaty can open a path to start negotiations with Beijing, first on raising the level of transparency, and second on agreeing on restrictions, as the ones in the Treaty. The negotiations for a solution between the two parties will inevitably include discussions on a broader political topic, the elements of which may be considered as prerequisites determining the final solution.

Considering the fact that many aspects of the challenge made by the INF Treaty are already seen in the past, the outcomes from this crisis based on the principle of application may be anticipated from today's point of view. It is a fact that the end of these tensions will consist of discussing solutions; so the question remains, how much time would pass until the new détente, and hence, how much will the New INF Treaty cost?

## REFERENCES:

- “António Guterres (UN Secretary-General), High Level Segment - Conference on Disarmament” UN Web TV, 10:43, “The United Nations,” February 25, 2019.
- Nato. “A Short History of NATO.” NATO. Accessed April 27, 2020. [https://www.nato.int/cps/en/natohq/declassified\\_139339.htm](https://www.nato.int/cps/en/natohq/declassified_139339.htm).
- Nato. “1979: The Soviet Union Deploys Its SS20 Missiles and NATO Responds.” NATO, January 9, 2013. [https://www.nato.int/cps/en/natohq/opinions\\_139274.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/opinions_139274.htm?selectedLocale=en).
- Nato. “NATO and the INF Treaty.” NATO, 2 Aug. 2019, [www.nato.int/cps/en/natohq/topics\\_166100.htm](http://www.nato.int/cps/en/natohq/topics_166100.htm).
- “Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles”, December 8, 1987, <https://2009-2017.state.gov/t/avc/trty/102360.htm#diplomaticnotes>
- Rfe/rl. “Putin Officially Suspends Russia’s Participation In INF Treaty With U.S.” RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 4, 2019. <https://www.rferl.org/a/putin-officially-suspends-russia-s-participation-in-inf-treaty-with-u-s-/29802816.html>.
- “United States, Russia Sign Agreement to Further Research and Development Collaboration in Nuclear Energy and Security.” Energy.gov, September 16, 2013. <https://www.energy.gov/articles/united-states-russia-sign-agreement-further-research-and-development-collaboration-nuclear>.
- “Russian Research Reactors May Convert to LEU.” World Nuclear Association - World Nuclear News, December 9, 2010. [https://www.world-nuclear-news.org/RS-Russian\\_research\\_reactors\\_may\\_convert\\_to\\_LEU\\_fuel-0912104.html](https://www.world-nuclear-news.org/RS-Russian_research_reactors_may_convert_to_LEU_fuel-0912104.html).
- “‘Wars not diminishing’: Putin’s iconic 2007 Munich speech (FULL VIDEO)”, YouTube video, 30:40,”RT,”February 10, 2017. <https://www.youtube.com/watch?v=U4MAsh3zMA&t=16s>.
- Collina, Tom Z. “U.S. Raises INF Concerns With Russia.” Arms Control Association. Accessed April 22, 2020. <https://www.armscontrol.org/act/2014-03/us-raises-inf-concerns-russia>.
- Reif, Kingston. “Russia Suspends Plutonium Agreement.” Arms Control Association, November 2016. <https://www.armscontrol.org/act/2016-10/news/russia-suspends-plutonium-agreement>.
- Kühn, Ulrich, and Anna Péczeli. “Russia, NATO, and the INF Treaty.” Strategic Studies Quarterly 11, no. 1 (2017): 66-99. Accessed April 19, 2020. [www.jstor.org/stable/26271591](http://www.jstor.org/stable/26271591).

- “Treaty Between the United States of America and the Union Of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems”, May 26, 1972, [https://media.nti.org/documents/abm\\_treaty.pdf](https://media.nti.org/documents/abm_treaty.pdf)
- Nato. “Aegis Ashore Ballistic Missile Defence System in Romania Completes Scheduled Update.” NATO, August 8, 2019. [https://www.nato.int/cps/en/natohq/news\\_168377.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_168377.htm?selectedLocale=en).
- Decree N 683 of the President of the Russian Federation, The National Security Strategy of the Russian Federation, 31 December 2015, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.
- Kimball, Daryl, and Kingston Reif. “Arms Control Association.” The Anti-Ballistic Missile (ABM) Treaty at a Glance, July 2017. <https://www.armscontrol.org/factsheets/abmtreaty>.
- “Europe Will Become a Battlefield: Putin Bluntly Explains What Discarding INF Treaty Means,” YouTube video, 5:09, “Vesti News,” October 25, 2018. <https://www.youtube.com/watch?v=SJiQqMY7e-M>.
- “Europe Will Become a Battlefield: Putin Bluntly Explains What Discarding INF Treaty Means,” YouTube video, 5:09, “Vesti News,” October 25, 2018. <https://www.youtube.com/watch?v=SJiQqMY7e-M>.
- Rfe/rl. “U.S. Official: New START Treaty Should Cover Russian Weapon Systems Under Development.” RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 10, 2020. <https://www.rferl.org/a/us-official-new-start-treaty-should-cover-russian-weapons-systems-under-development/30479166.html>.
- The National Security Strategy of the Russian Federation, p.25.
- Pifer, Steven. “The Moscow Missile Mystery: Is Russia Actually Violating the INF Treaty?” Brookings. Brookings, July 28, 2016. <https://www.brookings.edu/opinions/the-moscow-missile-mystery-is-russia-actually-violating-the-inf-treaty/>.
- Blank, Stephen. “Making Sense of the Shanghai Cooperation Organization.” Georgetown Journal of International Affairs 14, no. 2 (2013): 39. [www.jstor.org/stable/43134410](http://www.jstor.org/stable/43134410).
- The State Council Information Office of the People’s Republic of China. 2015. China’s Military Strategy (2015), Beijing, <https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf>.
- China’s Military Strategy (2015), p.25.
- “Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles”, December 8, 1987, <https://2009-2017.state.gov/t/avc/trty/102360.htm#diplomaticnotes>
- Baklitskiy, Andrey. “What the End of the INF Treaty Means for China.” Carnegie Moscow Center, December 2, 2019. <https://carnegie.ru/commentary/80462>.
- The State Council Information Office of the People’s Republic of China. 2015. China’s Military Strategy (2015), Beijing, <https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf>.
- Rfe/rl. “U.S. Official: New START Treaty Should Cover Russian Weapon Systems Under Development.” RadioFreeEurope/RadioLiberty. Radio Free Europe / Radio Liberty, March 10, 2020. <https://www.rferl.org/a/us-official-new-start-treaty-should-cover-russian-weapons-systems-under-development/30479166.html>.
- Reif, Kingston, and Kelsey Davenport. “Arms Control Association.” Nuclear Weapons: Who Has What at a Glance, July 2019. <https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat>.

- Riqiang, Wu. "How China Practices and Thinks About Nuclear Transparency." In *Understanding Chinese Nuclear Thinking*, 219–50. Washington D.C., USA: Carnegie Endowment for International Peace, 2016.
- "António Guterres (UN Secretary-General), High Level Segment - Conference on Disarmament" UN Web TV, 10:43, "The United Nations," February 25, 2019.
- "Mikhail Gorbachev: World in 'colossal danger'" BBC Video, 2:52, "British Broadcast Channel," November 04, 2019.
- "Astana: Putin and Others Meet For CSTO Summit; Nuclear Security in Jeopardy Because of US!", YouTube video, 4:05, "Vesti News," November 09, 2018.
- "Treaty Between The United States Of America And The Russian Federation On Measures For The Further Reduction And Limitation Of Strategic Offensive Arms", April 8, 2010, <https://2009-2017.state.gov/documents/organization/140035.pdf>
- Sittlow, Brian L. "New START: The Future of U.S.-Russia Nuclear Arms Control." Council on Foreign Relations. Council on Foreign Relations, January 28, 2020. <https://www.cfr.org/in-brief/new-start-future-us-russia-nuclear-arms-control>.
- "Briefing With Senior State Department Official On the New START - United States Department of State." U.S. Department of State. U.S. Department of State, March 9, 2020. <https://www.state.gov/briefing-with-senior-state-department-official-on-the-new-start/>.
- Kubiak, Katarzyna. Report. European Leadership Network, 2018. Accessed April 29, 2020. doi:10.2307/resrep22118.
- Vaddi, Pranay. "The Importance of the New START Treaty." Carnegie Endowment for International Peace, December 4, 2019. <https://carnegieendowment.org/2019/12/04/importance-of-new-start-treaty-pub-80834>.



## DEMOCRATIC CONTROL OF ARGENTINA'S INTELLIGENCE SERVICE DURING THE KIRCHNERS' RULE (2003–2015)

Lidija KOS-STANIŠIĆ<sup>1</sup>  
Ante ŠUNJIĆ<sup>2</sup>

**Abstract:** *This paper presents the activities of Néstor Kirchner (2003-2007) and Cristina Fernández de Kirchner (2007-2015), which were to contribute to the formal and direct democratic control of the main intelligence service of Argentina, as well as to the activities of the media that are expected to informally and indirectly exert democratic control over intelligence. The authors conclude that the activities of both presidents and the media during the rule of the Kirchners are a continuation of the process of democratization, but that the results ultimately contributed only slightly to the democratic control of Argentina's intelligence service.*

**keywords:** *Argentina, intelligence, democratic control, democratization, Kirchners*

### Introduction

The democratization of Argentina began after the defeat in the Malvinas/Falklands War and the democratic elections in 1983, which, according to Caramani (2013: 548), represents a process of transforming non-democratic institutions or political communities into democratic ones. President Raúl Alfonsín came into power and began the process of democratization of the central intelligence service. The democratization process is considered to have commenced with the introduction of mechanisms for democratic control and oversight of the intelligence service. The Argentine intelligence system throughout its history has consisted of several intelligence services. There was a "principal" intelligence service responsible to the President (a civilian or a military officer), which changed its name over time (CIDE – *Coordinación de Informaciones de Estado* (1946-1956), SIDE – *Secretaría de Inteligencia del Estado* (1956-2001), SI – *Secretaría de Inteligencia* (2001-2015)), intelligence services of certain branches of the army, federal police intelligence services and security intelligence services, all of which developed under the great influence of the army up to the 1980s. The main goal of the undemocratic intelligence services was to protect the regime in power, in the absence of external enemies in Latin America, their main task was to fight domestic opponents of the regime, causing numerous crimes and human rights violations, especially during the military dictatorship and "Dirty War" against the opposition and "internal enemies" (1976-1982). During Alfonsín's rule, the national *Defense Law* was passed in 1988. It changed the doctrine of national security and appointed a civilian to the position of head of SIDE for the first time, but no significant reforms were carried out due to strong resistance. His successor, President Carlos Saul Menem, successfully placed the

<sup>1</sup> The author is professor at the University of Zagreb

<sup>2</sup> The author is MA, City of Zagreb



military under civilian control in the early 1990s and passed the *Internal Security Law*, which established bodies for the democratic oversight of intelligence services for the first time. The democratization of Argentine intelligence services can be divided into the period before and after 2001, i.e. the enactment of the *National Intelligence Law* which institutionalized the intelligence system and renamed SIDE into SI. But this law had not significantly changed the functioning of the services. The most important goal of the intelligence services in the first phase of democratization was, along with the military, not to be punished for crimes committed during the military rule. After achieving their goal, they voluntarily submitted to the executive branch to protect it from political opponents, coups and media criticism, while retaining their own maneuvering space (Kos-Stanišić and Šunjić, 2020).

The term service also implies that it is a public service that should serve the citizens. We define intelligence as a “state organization that collects, analyzes, and disseminates information regarding threats to national security” (Born and Geisler Mesevage, 2012: 6). National security should ensure a state in which there is a “freedom of the state and society, the territorial integrity and sovereignty of the state within internationally accepted arrangements, human freedoms and citizens’ rights, political and social stability of society and the state, stable economic development and the rule of law, stable public order and personal safety of citizens and healthy and stable ecological conditions” (Tatalović and Bilandžić, 2005: 32). The definition of intelligence includes a number of organizations, such as military and civilian intelligence, police intelligence, both internal and external, but also organizations within particular ministries. All these agencies taken together make up the “intelligence community”. The intelligence service, unlike other government agencies, has the power to gather information under special circumstances and with a court order “by intercepting communications, using covert surveillance, using secret informants and the power to enter premises” (Born and Geisler Mesevage, 2012: 6). The intelligence service, along with the military and the police, makes up the most important segment of the security sector.

Gill (2016: 4) believes that democratic governance of the intelligence system is manifested through two complementary processes – control and oversight. Control means that agencies are established and funded by the legislature and that ministers need to authorize intelligence activities. Oversight means that an internal and external body should monitor the legality, validity, efficiency and effectiveness of intelligence agencies. In the case of Latin America, Matei, Castro Garcia and Henfield (2016) conclude that reforms have been implemented that put the intelligence sector under civic prerogatives and that a new legal framework for intelligence institutions has been enacted, but that democratic civilian control and oversight have not yet been achieved.

The Intelligence Working Group (DCAF, 2006: 37-56) of the Geneva Center for the Democratic Control of Armed Forces uses the term “democratic control” for control and oversight, and lists several mechanisms for democratic control of intelligence services. They distinguish between formal and direct mechanisms – executive control and accountability, legislative oversight, and judicial control and oversight – and informal and indirect – oversight by the public, i.e. the media and civil society stakeholders.

In this paper, we will present the presidential decrees and laws passed during the rule of Néstor Kirchner (2003-2007) and his wife, President Cristina Fernández de Kirchner (2007-2015), which were to contribute to the formal and direct democratic control of the main intelligence service. We will also portray the activities of the media that are expected to informally and indirectly exercise democratic control over Argentina’s intelligence service.

The paper will attempt to confirm the thesis that the activities of both presidents and the media during the rule of the Kirchners are a continuation of the process of democratization of the central Argentine intelligence service, but that the results ultimately contributed only slightly to the democratic control of Argentina's intelligence service. The purpose of this paper is to analyze the actions of key actors in the process of democratization of the intelligence service, while the aim is to gain a deeper insight into the complexity of the process in question. This is important as many countries around the world are constantly looking for the most effective models of intelligence control and surveillance. The subject analysis can serve other researchers in considering a number of elements that were specific to Argentina from 2003 to 2015. The paper uses system theory that has its own tenets, and we analyzed the supervisory or control part that ensures that the system works properly. The paper presents a case study with one element of analysis – the intelligence service of Argentina, in which formal and informal control mechanisms acting as correctives for its functioning are analyzed.

The paper consists of an introduction, three sections and a conclusion. The first section provides a theoretical overview of the democratic control of the intelligence services, the second an overview of the democratic control of the executive during the rule of the Kirchners, and the third the role of the media in the democratic control of the intelligence service during the same period. The conclusion summarizes the research results and provides an evaluation of the success of the intelligence service democratization process in the analyzed time period.

### **Democratic control of intelligence services**

The key point of conflict between the principles of a democratic society and the principles by which the intelligence system operates lies in the very nature of democratic society that presupposes openness and transparency, as opposed to an intelligence system within which activities take place in secret. That is why an oversight system is important, which can also be defined as a process of supervision that does not deal with day-to-day management, but with ensuring that the policies and methods of an intelligence service are in line with its legal mandate. The process should consist of internal (within the agency and the executive) and external (parliament, judiciary and civil society organizations) oversight. Parliamentary committees represent a central element of oversight, but in the strong Latin American presidential systems they are extremely weak, without the right resources and power, and are thus largely ineffective (Gill, 2016: 176-183).

The aforementioned Intelligence Working Group (DCAF, 2006: 37-56) of the Geneva Center for Democratic Control of Armed Forces uses the term “democratic control” for the process of control and oversight. Systems of democratic control of intelligence services are emerging under the influence of various historical, political and other social circumstances which, each in their own way, condition, abolish the old or introduce new norms and practices. Therefore, there is no unified system of democratic control of intelligence services or exact norms. Nevertheless, given the different models accepted in democratic societies, formal and informal forms of intelligence control can be differentiated. Formal forms of intelligence control involve direct control by the executive, the legislature and the judiciary. However, the most

important actors in the formal control of intelligence services are the actors in the executive branch. It is the executive branch that gives direction to intelligence work and activities carried out within the intelligence community, which in turn must exclude the political goals of the political options exercising power. The executive, through the control of intelligence services, ensures the transparency, legality, accountability and ethics of their actions. For the purpose of conducting adequate control, the executive forms various institutional bodies such as committees, councils, advisors, inspectors general and the like. The legislature, as the elected representative of the people, also possesses various instruments to control the intelligence services. To the greatest extent, this control refers to monitoring the transparency of budget spending in intelligence services and the impact on the adoption and implementation of intelligence policies. The legislature usually exercises control by forming various standing committees, subcommittees or ad hoc oversight bodies consisting of a number of members of the legislature. The judiciary, on the other hand, bases its control of the intelligence services on assessing the legality and constitutionality of their actions. Furthermore, different courts may, depending on legal provisions, be an element that gives approval to intelligence services to carry out measures and actions that violate the privacy of citizens. Also, a certain form of control can be carried out by the attorney general, primarily through the analysis of intelligence reports and reporting to the executive on the legality of their activities (DCAF, 2006: 37-56).

In addition to formal, there are also informal or indirect forms of control exercised primarily by the media and various stakeholders in civil society. One of the ways of informing the public or conducting indirect supervision can be an instrument of declassification of certain information after a certain period of time. Otherwise, without adequate information, civil society actors would not be able to exercise intelligence control. Civil society organizations can warn of human rights violations, especially the right to privacy, but they can also inform the public about existing security threats, which can contribute to creating greater public support for the work of intelligence services. Furthermore, civil society organizations can provide additional knowledge to the media and encourage reporting in order to increase public understanding of intelligence.

It is the media that provoke controversy when it comes to informal oversight of intelligence services. The role of the media in oversight is most often reflected in the disclosure of classified intelligence, the indication of illegal activities, the non-transparent spending of funds and the failures of intelligence services. The danger lies in the lack of education of the journalists themselves, which can result in sensationalist reporting and potential threats to national security. There is also a possibility that the media, although in possession of certain information about the activities of intelligence services, do not report on them in order to preserve national security. Also, the media can be used for the purpose of misinforming the public through intelligence sources. Ultimately, it can be concluded that any intelligence leak allows the media to conduct informal surveillance, but also that more adequate formal surveillance mechanisms

with an appropriate balance between security and freedom would reduce the need thereof (DCAF, 2006).

### **Democratic control of intelligence services by the executive during the Kirchners' rule (2003-2015)**

Within the formal and direct democratic control of intelligence services, the highest importance belongs to the incumbent of the executive, which in the case of Argentina with a presidential system of governance is – the president, who should provide direction to intelligence activities, and ensure their transparency, legality, accountability and ethics of action. In presidential democracies, which are mostly located in Latin America, the head of government and the president of the state are the same person. He or she is elected by the people, thus elections for the legislature and post-election negotiations do not decide who will hold the executive branch. The ideal situation regarding the relationship between the executive and the legislature is when the president's party has the majority in the legislature and regularly supports him or her.<sup>3</sup> The ability of the president to influence the legislature lies in two types of power – party and constitutional power, i.e. the proactive issuance of decrees and the reactive veto power (Kos-Stanišić, 2009: 66-67).

The winner of the 2003 presidential election, Néstor Kirchner Ostoic was the candidate of the Peronist electoral alliance of the Front for Victory (*Frente para la Victoria*), which has since begun to identify with Kirchnerism. Kos-Stanišić (2014) states that Kirchnerism was a type of middle-class populism, within which conflicts prevail, arising at a time of a triple change. The country was hit by a wave of protest and mobilization of the people at the local level in 2001-2002, the validity of the recommendations of the Washington Consensus was questioned at the regional level, while a new economic cycle of booming commodity prices and the era of commodity consensus began at the global level. Néstor Kirchner distanced himself from the policies of his predecessors. He also managed to obtain the repeal of the law on amnesty for military officers passed during Alfonsín's rule, and during his incumbency a large number of criminals were prosecuted and sentenced to prison terms. However, Korstanje (2016: 129-135) believes that while Kirchnerism enabled the prosecution of crimes committed against human rights, it also used a discourse that was adapted to the interests of the Kirchners and their followers. Néstor Kirchner successfully dealt with economic problems, first restructuring debts and then canceling payments to the IMF. Political commentators accused him of concentrating power and excessive use of decrees (he passed 270 decrees), as well as friendship with Hugo Chávez and turning to populism. But Levitsky and Murillo (2008: 20-25) argue that Néstor's ability to concentrate power

---

<sup>3</sup> The Peronist electoral alliance of the Front for Victory had a majority in the House of Representatives and the Senate during Néstor Kirchner's rule in the period from 2003 to 2005, while it was in the minority from 2005 to 2007 (Wikipedia.org, 2020).

in his hands was limited by robust democratic institutions, a strong civil society, and the very nature of the Peronist coalition, including Néstor's respect for the letter of the law while violating its spirit.

By the time Kirchner took power in the intelligence sector, he had a slightly better situation than his predecessors because, thanks to the Intelligence System Law from 2001, he was greeted to an institutionalized intelligence community, if not in reality then at least on paper. It is important to mention that the new/old organization, SI, retained the mandate of intelligence activities in the country and abroad, and was under the direct control of the President. Part of the public felt that nothing significant had changed and that after two decades of democracy the intelligence community was still ruled by a policy of continuity, patronizing and friendly relations, lack of professionalism and control by the executive (Ginter, 2008: 78).

Kirchner set out resolutely, introducing major changes to the so-called secrecy policy, so during his tenure he issued fifteen presidential decrees related to the activities of the intelligence sector. The decrees usually included a waiver of the obligation to keep information gathered by covert intelligence activities, which required a request from a competent court on a case-by-case basis (Estévez, 2013: 226). They mainly concerned the release from the legal obligation to maintain the secrecy by former heads of intelligence services in connection with investigations of terrorist attacks and corruption cases. Some of the decrees also referred to refraining from destroying any document relating to the 1992 bombings of the Israeli Embassy and the 1994 bombing of the Jewish Community Center (AMIA) building.<sup>4</sup> Decree 490/2002 concerned the release of former intelligence chief Hugo Anzorreguy from the legal obligation to keep records of intelligence activities carried out during the investigation of the attack on the AMIA. However, Decree 116/2003 defined certain documents signed by the Secretary of Intelligence as strictly confidential (Argentina.gov.ar, 2003a). This nullified the effect of other presidential decrees relating to the disclosure of classified documents. Later that year, Decree 116/2003 was declared unconstitutional. President Kirchner, however, still found a way to omit the disclosure of certain information. He issued Decree 291, which omitted, for example, the identity of intelligence officers, but also the methodology of SI's operations. This made it possible to cover up certain illegal activities in the intelligence community. Decree 291, according to Clarin (2003), specifies that the former head of SIDE Anzorreguy "is not authorized to disclose facts involving third-country nationals or facts that mean disclosing of secrets which could endanger the security of the state." A number of decrees related to the release

---

<sup>4</sup> Argentina was the target of two terrorist attacks in the 1990s. The first occurred on 17 March 1992, when the Israeli Embassy in Buenos Aires was attacked and 29 people lost their lives. The second attack took place on 18 July 1994, when the building of the Jewish Community Center (AMIA) in Buenos Aires was attacked. At that time, 85 people lost their lives and hundreds were injured. No one has been prosecuted for committing these crimes. Hezbollah has been indicted, and Israeli authorities see the culprit for these attacks in Iran (Mfa.gov.il, 2003; Mfa.gov.il, 2007).

of intelligence officers, as well as the police and the military, from keeping secrecy, when summoned in connection with criminal proceedings for human rights violations during the reign of the last military regime (1976-1982), during which 10,000-30,000 citizens went missing or were killed. In this context, Decree 715/2004, which established a special body to investigate the disappearance of children during the “Dirty War” (Argentina.gob.ar, 2004a), is significant. For this purpose, access was provided to the archives of the entire executive branch. Also, a number of decrees were related to the access to secret expenses and financial reports based on court requests for a certain period and a certain part of the intelligence system. For example, Decree 249/2003 exempted Hugo Anzorreguy from the obligation to maintain secrecy in order to testify in a case dealing with the misuse of certain parts of the intelligence system (Argentina.gob.ar, 2003b), while Decree 1076/2006 provided access to military intelligence (Argentina.gob.ar, 2006). This even included data relating to the misuse of intelligence budgets during some of the previous governments. Thanks to this decree, an indictment against former President Carlos Menem for obstructing an investigation into a terrorist attack on a Jewish Community Center building was confirmed in December 2009 (Estévez, 2013). The decree also provides for exemption from the legal obligation to maintain secrecy in the “La Tablada” case.<sup>5</sup>

The most controversial act implemented by Kirchner is the so-called “Spy Law” (Ley espia). Law No. 25.873 on data protection which was adopted in December 2003 by the Congress, in which his Peronist party held a majority. Decree 1563/2004 further regulated this controversial law (Argentina.gob.ar, 2004b). Estévez (2013: 226) states that the law provoked sharp reactions from the public and the media. The law stipulated that telecommunication operators must make all resources available at the request of the judiciary and the ministries for the purpose of intercepting communications. Due to great public pressure, President Kirchner was forced to suspend with a decree in 2005 the application of the law that was declared unconstitutional by a 2009 decision of the Supreme Court of Justice.

Law No. 26.134 which regulated the issue of the laws of secrecy and reserved nature (*leyes secretas y reservadas*) was also adopted during Néstor’s mandate.<sup>6</sup> It made all such existing laws publicly available, and at the same time prohibited their adoption in the future. The existing rules relating to secret expenditures had also been repealed, and the Bicameral Commission on the Oversight of Intelligence Bodies and Activities of the National Congress was mandated to oversee the intelligence budget (Estévez, 2010: 61). It was one of the most significant shifts towards democratic control of the

---

<sup>5</sup> This case relates to an attack that occurred on 23 January 1989 when the barracks of the Third Mechanized Infantry Regiment (RIM3) in the city of La Tablada in the province of Buenos Aires was attacked by 42 members of the revolutionary group Movimiento Todos por la Patria (MTP). A total of 39 insurgents and members of the army were killed in the clash. See more in: Sheinin (2017).

<sup>6</sup> See more on reform of the secrecy policy in Argentina in: Estévez (2007:14-17) and Estévez (2010:61-62)

intelligence system during Néstor Kirchner's rule. However, a lack of political will resulted in an inadequate approach in practice. Despite the improved legal framework, intelligence oversight of the intelligence budget was conducted exceptionally, and there was still room for manipulation of secret funds.

Although Néstor Kirchner had high public support during his term, in 2007 he left the presidential candidacy to his wife, Senator Cristina Fernández de Kirchner, who became Argentina's first democratically elected president. Her presidential term was secured by a combination of the popularity of her husband, a strong Peronist party with a stable electorate and a weak opposition (Kos-Stanišić, 2014). In the first half of 2007, a court investigation was launched into illegal wiretapping, and a series of searches were ordered, including the residence of former SIDE Chief Juan Bautista "Tata" Yofre.<sup>7</sup> President Fernández de Kirchner continued to pursue her husband's intelligence policy and, like him, issued a series of decrees on these issues. A scandal emerged in 2009 within the intelligence community, when a court investigation revealed the illegal wiretapping of as many as 400 people,<sup>8</sup> which pointed to shortcomings in the control measures provided by the National Intelligence Law and the need to review judicial proceedings related to interception of communications (Estévez, 2010). The focus in this situation was on prosecuting those responsible without adequate analysis and detection of errors within the system. Furthermore, in 2010, the President issued the Decree 4/2010 on the declassification of data on the activities of the armed forces during the last military rule at the request of a judge investigating human rights violations (Argentina.gov.ar, 2010). Interestingly, this decree excluded information on the Malvinas/Falklands War and strategic military intelligence activities from the declassification process (Estévez, 2014). It was only in 2015, in the last year of her term, that the President launched a major reform of the intelligence system. She proposed the dissolution of the SI as a key player in the intelligence system and the formation of a new service called the Federal Intelligence Agency (Agencia Federal de Inteligencia – AFI). The key argument for reform was the failure to implement structural reforms in this sector since the end of the military dictatorship (Brito, 2016). The reforms were also supported by the fact that the AFI was envisaged as significantly smaller than the SI with more transparent funding. Speaking about the need for reform, former Néstor Security Minister Marcelo Sain told the media that intelligence services were used for spying for political purposes, funding political campaigns and establishing control over the judiciary. He also said that there are a number of judicial and political officials associated with SIDE. The very fact that many high-ranking officials of the then SI often referred to it as SIDE (a name associated with military-era intelligence), as Sain did, speaks volumes about the necessity of reform (Brito, 2016). In addition to the old intelligence structures, the SI was linked to old personnel who often held managerial

---

<sup>7</sup> See more in: [Página12.com](http://Página12.com) (2007).

<sup>8</sup> See more in: [Clarín.com](http://Clarín.com) (2009).

positions within the system. It can be assumed that the inherited patterns of carrying out intelligence activities are indirectly caused by this, at least in part. At the time the reform was proposed, almost 32 years had passed since the return of democracy to Argentina and the system definitely required structural change. But the moment when this reform was proposed was indicative. Just before that, Argentina was shaken by the news of the death or suicide<sup>9</sup> of Federal Prosecutor Alberto Nisman, who issued several days before serious accusations against President Fernández de Kirchner for covering up the involvement of senior Iranian officials in the attack on AMIA.<sup>10</sup> The accusation was also proof that presidents really do not always know what their intelligence services are doing. Namely, Cristina Fernández de Kirchner did not know that SI was exercising widespread surveillance over politicians, judges, prosecutors and journalists, until Nisman accused her of conspiracy, i.e. an agreement with Iran to cover up their involvement in a terrorist attack (Gill, 2016: 163-164). Opponents of the reform felt that Fernández de Kirchner's reform was intended to prevent further investigations against her administration and to cover up Nisman's death. They also questioned the manner and transparency of financing the new intelligence service. Also, a number of public reactions were provoked by the announcement of the transfer of jurisdiction over wiretapping from the intelligence service to the Attorney General's Office, which was particularly controversial due to links between Cristina Fernández de Kirchner and Attorney General Alejandra Gils Carbó, who was considered loyal to the ruling Peronist party.<sup>11</sup> Common to all criticism was the indication of certain political reasons the President had that went beyond the democratization of intelligence services, which was cited by the Government as the purpose of the reform (Brito, 2016). Although the reform was necessary, the motives for its implementation and the effects it sought to achieve were questionable. The reform passed despite all the criticism and the amendments were adopted.

The National Intelligence Law was amended in Congress<sup>12</sup> in March 2015 by the Federal Intelligence Agency Law. With these changes, the Federal Intelligence Agency – AFI was formed, replacing the former SI. Consequently, the AFI became the supreme body within the Argentine intelligence system. The collection and analysis of information for the purpose of protecting national security and the collection and analysis of criminal information were identified as key AFI activities to be carried out through other intelligence bodies and by means of its own resources. The AFI Director, who has the rank of a minister, and his or her deputy, who has the rank of secretary of state, are appointed by the President under the new law with prior approval from the

---

<sup>9</sup> A 2017 police investigation concluded that Nisman had been killed (Guardian.com, 2017).

<sup>10</sup> See more in: Taylor (2015) and Guardian.com (2017).

<sup>11</sup> See more in: Partlow and Caselli (2015).

<sup>12</sup> The Peronist electoral alliance of the Front for Victory had a majority in the House of Representatives and the Senate during Cristina's rule only in the period from 2013 to 2015, while it was in the minority from 2005 to 2013. (Wikipedia.org, 2020).



Senate. Furthermore, the National Directorate of Criminal Intelligence and the National Directorate of Strategic Military Intelligence are under the jurisdiction of the Ministry of Security and the Ministry of Defense, respectively. Brito (2016: 31) concludes that the reform was primarily politically motivated, and Tello and Sopta (2015) believe that the accusations made in public by some politicians and journalists, that the state of Argentina conducts illegal counterintelligence activities in order to achieve political goals, were true.

### **Democratic control of intelligence services by the media during the Kirchners' rule (2003-2015)**

Considering the role of the President in the democratic control of the Argentine intelligence system in the period of Kirchnerism, we reach the issue of the role of the media and the impact of media reporting on the democratization of the intelligence system.

Gill (2016: 151-152) states that in democracies, the media should act as a “public forum” where different opinions can be heard, especially those that are critical towards the government. Namely, the media can be considered the fourth branch of government whose role should be that of a key informal accountability mechanism. The media should be “watch dogs”, i.e. fighters against corruption, abuse of power and position and a place where whistleblowers are able to reveal relevant information. Since the formal mechanisms of democratic control are often very weak, it is the media that bring abuse of power into the light of day. The relationship between the media and democracy is complex, especially when it comes to security and intelligence issues. In Latin America, it is also a dangerous business, as 262 journalists were killed between 1988 and 2002 (Gill, 2016: 152).

Security sector reforms are probably the last and most complicated area exposed by the mass media. During democratic consolidation, the public should stop fearing the institutions of the old regime that sowed fear and trepidation in society, and the media should play a significant role in restoring confidence in the security sector and reassuring citizens that they are under democratic control. The problems that the media face when reporting on the activities of the security sector, to name just a few, are: expensive research that experienced and skilled investigative journalists need to spend a lot of time on; provoking revenge (from denial of information to murder) of a person or institution that has been compromised by media coverage; the possibility of being tricked by deliberate “leaks” of compromising information about rivals, thus becoming *proxies* in the internal struggle of various factions within the services or the government (Reljić, 2010: 15-23).

According to Hilldebrand (2012) the media have an obligation to scrutinize and investigate government activities, and identify three media roles in the democratic control of intelligence services. The first is the role of transmitter of information and

stimulator of formal oversight, the second is that of a substitute guard dog, and the third is the legitimization of the institution. She also mentions the limitations that the media face with democratic control, such as: turning into a government lapdog, which only transmits government information and policies without question; a legal regulatory framework that restricts access to classified information in the name of national security; a high degree of government secrecy; and the agenda, that is, the intelligence service's own strategy on how to communicate with the public (Hildebrand, 2012: 690-704).

The role of the media as key stakeholders in civil society in the process of democratic control is enormous. Given all the pitfalls that states may face during democratization, it is necessary to give the media autonomy and independence, while the media should support the government in consolidation processes and at the same time check the government to prevent possible abuses of power. We will present only the key aspects of the above issue in the period of Kirchnerism. Estévez (2010: 74) states that since the democratization of Argentina, journalists have valiantly followed topics related to intelligence services, illegal wiretapping and other intelligence scandals. He identifies two Argentine dailies, *Clarín* and *La Nación*, as very critical of the intelligence services and of the attitude of governments towards them. Gerard Young, as well as Carlos Juvenal and Jorge Boimvaser stand out among the journalists who have dealt with this area and wrote about these topics earlier. Media coverage of the intelligence system during Néstor Kirchner's tenure was critically covered by the Argentine media. Thus, the most controversial reform, the so-called "Spy Law", provoked a massive reaction from the media and the public and was criticized until the law was withdrawn in 2005.<sup>13</sup> The media also uncovered a drug smuggling scandal involving the PAN airport security police (Dandan, 2005), prompting Néstor Kirchner to reform it. Following the outbreak of an intelligence scandal within the Navy, articles appeared in the media questioning security sector reforms.<sup>14</sup> During the Kirchners' rule, the media participated in the discovery of several intelligence scandals, but did not encourage significant changes in the direction of system democratization. With the exception of the "Spy Law" scandal, media influence did not prove crucial in exercising democratic control over the intelligence system. Also, there was a lack of serious text analysis and questioning the actions of the executive in this period. The exception was the intelligence scandal in the Navy. The scandal was uncovered by the non-governmental organization CELS, which also presented a detailed analysis of the case, with the expectation that some media outlets would offer a review of that analysis. The question arises as to why the media themselves did not delve deeper into analyzing these issues since access to information analyzed by CELS should not have posed a problem to serious investigative journalism. It can be assumed that the possible reasons could be a lack of both interest and resources to investigate the issues. When it comes to media coverage

---

<sup>13</sup> See more in: Ybarra and Colonna (2005).

<sup>14</sup> See more in: Chillier (2006).

of the intelligence system in the mandates of Cristina Fernández de Kirchner, it is necessary to make a distinction between media headlines before and after the President's conflict with the media.

Cristina Fernández de Kirchner had a series of conflicts with the media during her two presidential terms. When she made a decision in 2009 depriving the leading media house Grupo Clarín of the right to broadcast football matches and awarding it to the state television, she provoked fierce reactions. Analysts characterized the move as populist and it caused open conflict with the media.

By proposing media reform, the President got on Grupo Clarín's bad side, given that up until then it had been reporting favorably on the Kirchners. After an article was published insinuating irregularities in donations for her campaign, President Fernández de Kirchner "accepted the challenge of positioning the media as a political opponent who criticized her for using irrelevant, gender-specific comments" (Van Dembroucke, 2014: 1066). This resulted in the proposal of a new "Audiovisual Law" (Brito, 2016). The bill included a series of changes that went in favor of the Government, contrary to the interest of the media. One of the key innovations was "the establishment of a new communications regulatory agency, the Federal Authority for Audiovisual Communication Services (AFSCA)" (Brito, 2016: 58). There were a number of critiques from the opposition accusing the Government of taking control of the media and taking away a market share from major media outlets such as Grupo Clarín. Furthermore, controversy was caused by the large number of licenses granted to new pro-government media outlets (Brito, 2016). The new law allowed for the instrumentalization of the media by the Government, and large media companies were losing market share. The question arises as to whether the impact of media reporting on the democratization of the intelligence system can be analyzed when the media themselves have been instrumentalized.

After President Fernández de Kirchner came to power, the media continued to investigate illegal wiretapping, and events such as investigations against certain former intelligence officials were covered. Furthermore, in 2009 the media reported on a scandal involving the illegal wiretapping of as many as 400 people. That same year, one of the senior intelligence officials filed a defamation lawsuit against the director of the newspaper *La Nación*. The reason for this was information published by *La Nación* regarding the obstruction of the judicial investigation into the bombing of AMIA using intelligence operations.<sup>15</sup> This, in turn, provoked new reactions from the media.<sup>16</sup> Given the aforementioned conflict with the media, it can be concluded that at that time, media reform played a key role in changing the way and scope of reporting on both government policies in general and on intelligence-related issues. The reform of the intelligence system was criticized in the reports of predominantly foreign media.

---

<sup>15</sup> See more in: Morales Solá (2009).

<sup>16</sup> See more in: Clarin.com (2009) and Perfil (2009).

In January 2015, The Guardian reported on the proposed reform of the intelligence system, referring to the unexplained death of State Prosecutor Alberto Nisman and suspicious activities in the Argentine intelligence service.<sup>17</sup> One of the few domestic media outlets to report critically on the subject at the time was the Buenos Aires Herald, whose journalist Damián Pachter was the first to publish the news of Nisman's death. Buenos Aires Herald Editor-in-Chief Sebastián Lacunza subsequently published an article in which he pointed out that Pachter left the country due to threats and that they would provide him with the necessary protection as well as investigate the threats he received (Lacunza, 2015). We can conclude that the Argentine media critically reported on intelligence scandals up until their conflict with the President. After the media reform, the influence of large media companies was reduced, and the government-controlled media came to the fore. In that period, foreign media were most critical of the reforms of the intelligence system, and the democratic control of the President. Eventually, this politically motivated reform was adopted, and media coverage failed to drive change. We find the main cause in the tight control of the media by the authorities. It can be concluded that the impact of media coverage on the democratic control of the Argentine intelligence system in the Kirchnerist period was insufficient, i.e. that the media failed to find a way to adequately report on the shortcomings of the system.

## Conclusion

We divide the democratization of Argentina's intelligence services into the period from 1983 to 2001 and the period after 2001 and the enactment of the *National Intelligence Law*. In the first period, the intelligence sector was placed under civilian prerogatives and a new legal framework for the activities of intelligence institutions was adopted, but democratic control, both formal and direct, as well as informal and indirect, was not achieved. In this paper, we analyze the second period of democratization of Argentina's primary intelligence service, i.e. the role of two actors in the process of democratic control – the President and the media during the Kirchnerism period, i.e. the mandates of Néstor Kirchner (2003-2007) and Cristina Fernández de Kirchner (2007-2015).

Regarding the democratic control of President Néstor Kirchner, we can conclude that he was greeted, on paper, by an institutionalized national security system, and that he had the opportunity to improve the functioning of the intelligence system burdened by authoritarian legacies and scandals from the past. But instead of reforms, he regulated the functioning of the intelligence service using decrees that had dual effects. They have had a positive effect on the prosecution of those responsible for terrorism, corruption, human rights violations and a number of other crimes, but particular decrees have also made it possible to cover up certain illegal activities in the intelligence community. Most of them had to do with events from the relatively recent past that needed to be investigated. The adoption of the so-called "spy law" meant the continuation of the policy of politicization of the intelligence system, but thanks to the reaction of the media and the public, it was later declared unconstitutional.

---

<sup>17</sup> See more in: Guardian.com (2015).

Kirchner's law, which abolished the existence of secret laws and gave new powers to the Bicameral Commission on the Oversight of Intelligence Bodies and Activities of the National Congress with regard to the control of secret funds, contributed the most to democratic control, but unfortunately the legal framework was not adequately applied in practice. President Cristina Fernández de Kirchner continued her policy of issuing decrees introducing minor changes to the intelligence sector. Decree 4/2010 on the declassification of information, which excluded certain data on the Malvinas/Falklands War, raised doubts regarding the transparency of democratic control. With accusations of putting the intelligence service under her control and the suspicious death of State Prosecutor Albert Nisman, the 2015 reform was assessed as motivated solely by political reasons.

We can conclude that the Kirchner presidential couple played a dual role in the formal and direct control of the intelligence service. They passed decrees and laws that were supposed to increase, at the same time, the responsibility for past activities and the transparency of future activities, but also their concealment and instrumentalization.

Regarding the role of the media in informal and indirect democratic control, it was concluded that the media during Néstor Kirchner's tenure participated in the discovery of several intelligence scandals, which, however, did not encourage significant changes in the direction of democratization. Media coverage of intelligence reforms in the mandate of Cristina Fernández de Kirchner is divided into the period before media reform and the period after media reform. In the first period, the Argentine media were critical of the reforms, but after the establishment of tight control of the media by the authorities, the role was largely taken over by the foreign media. We can conclude that the impact of media coverage of the intelligence community in the Kirchnerism period was not overly significant, i.e. that the media failed to find a way to adequately analyze and argue all the shortcomings of the intelligence system.

We believe that the purpose and aim of this research have been confirmed.

### REFERENCES:

- Born, Hans. and Geisler Mesevage, Gabriel. (2012). Uvod u nadzor nad obavještajnim službama. In: Hans Born and Aidan Wills (ed.), Nadzor nad obavještajnim službama – Priručnik, Ženeva: DCAF.
- Brito, Anna C. (2016). Misuse of Executive Power as an Obstacle to Democratic Institutional Reform in Argentina. CMC Senior Theses. available at: [http://scholarship.claremont.edu/cmc\\_theses/1366](http://scholarship.claremont.edu/cmc_theses/1366) (accessed 21 May 2019).
- Caramani, Daniele. (2013). Komparativna politika, Zagreb: Političke analize.
- Estévez, Eduardo E. (2007). Developments of the democratization of intelligence in Argentina: Trends in secrecy policy. Implications for comparing transitional settings, Paper to be delivered at the 4th ECPR Conference, available at: <https://fas.org/irp/world/argentina/trends.pdf> (accessed 21 May 2019).
- Estévez, Eduardo E. (2010). Argentina's Intelligence in the Twenty-First Century / After Twenty-five Years of Democracy, Paper to be delivered at the 51st ISA Annual Convention, given by author – unpublished.
- Estévez, Eduardo E. (2013). Intelligence Community Reforms: The Case of Argentina. In: Philip H.J. Davies & Kristian C. Gustafson (ed), Intelligence Elsewhere – Spies and Espionage outside the Anglosphere. Washington: Georgetown University Press. pp.219-237.

- Estévez, Eduardo E. (2014). Comparing Intelligence Democratization in Latin America: Argentina, Peru, and Ecuador Cases. *Intelligence and National Security*, 29(4): 552-580.
- Estévez, Eduardo E. (2017). Criminal Intelligence and the Challenge of Transnational Organized Crime in Latin America. *Journal of Mediterranean and Balkan Intelligence (JMBI)*, pp. 87-104.
- Gill, Peter (2016). *Intelligence Governance and Democratization: A comparative analysis of the limits of reform*. London: New York Routledge.
- Ginter, Kevin (2008). Latin American Intelligence Services and the Transition to Democracy, *Journal of Intelligence History*. (8)1, pp. 69-93.
- Hillebrand, Claudia (2012.) The Role of News Media in Intelligence Oversight, *Intelligence and National Security*. 27(5), pp. 689-706.
- Korstanje, Maxmiliano (2016). The politics of Argentina today: human rights and Kirchnerismo, *Int. J. Human Rights and Constitutional Studies*, 4(2), pp. 129-137.
- Kos-Stanišić, Lidija (2009). *Latinska Amerika – povijest i politika*, Zagreb: Golden marketing - Tehnička knjiga.
- Kos-Stanišić, Lidija (2014). Populizam u Argentini – sedam desetljeća peronizma, *Političke perspective*, 4(1), pp. 31-55.
- Kos-Stanišić, Lidija and Šunjić, Ante (2020). Razvoj i demokratizacija obavještajne službe Argentine (1946.-2001.), *Međunarodne studije* 20(1-2) - accepted for publication.
- Levitsky, Steven. and Murillo, Maria Victoria. (2008). From Kirchner to Kirchner, *Journal of Democracy*, 19 (2), pp. 16-30.
- Matei, Florina Cristiana (2014). The Media's Role in Intelligence Democratization, *International Journal of Intelligence and CounterIntelligence*, (27), pp. 73–108.
- Matei, Florina Cristiana. de Castro Garcia, Andres. and Henfield, Darren. (2016). Balancing civilian control with intelligence effectiveness in Latin America and the Caribbean: current trends and lessons learned, *Journal of Mediterranean and Balkan Intelligence*, 7(1), pp. 7-29.
- Radna grupa za obavještajne službe (DCAF (2006.) Obavještajna praksa i demokratski nadzor praktični pogled, *Varaždin: Prudens consilium*.
- Reljić, Dušan (2010). Mass Media, Post-conflict Transformation and Transition: Why Is It Bodo and Not Katherine? In: Djurdjević-Lukic, Svetlana (ed) *The Media and Security Sector in the Western Balkans*, DCAF:13-26.
- Sheinin, David (2017). The La Tablada Attack and the Erosion of Civil Rights in Argentina, *Middle Atlantic Review of Latin American Studies*, 1(1): 77–96.
- Tatalović, Siniša and Bilandžić, Mirko (2005). *Osnove nacionalne sigurnosti*. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske.
- Tello Angel Pablo. and Sopta, Julio Cezar (2015). Discusiones en torno al rol asignado a la inteligencia military en la Argentina contemporanea, *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 10(2).
- Van Dembroucke, Celina (2014) Exploring Media Representations of Argentina's President Cristina Fernández de Kirchner, *Feminist Media Studies*, 14(6), pp. 1056-1070.
- Web reference:
- Argentina.gob.ar (2004a) <https://www.argentina.gob.ar/normativa/nacional/decreto-715-2004-95658> (accessed 10 October 2020).
- Argentina.gob.ar (2004b) <https://www.argentina.gob.ar/normativa/nacional/decreto-1563-2004-100806>

- Argentina.gob.ar (2003a) <https://www.argentina.gob.ar/normativa/nacional/decreto-116-2003-81638> (accessed 10 October 2020).
- Argentina.gob.ar (2003b) <https://www.argentina.gob.ar/normativa/nacional/decreto-249-2003-86364> (accessed 10 October 2020).
- Argentina.gob.ar (2006) <https://www.argentina.gob.ar/normativa/nacional/decreto-1076-2006-119006> (accessed 10 October 2020).
- Argentina.gob.ar (2010) <https://www.argentina.gob.ar/normativa/nacional/decreto-4-2010-162573> (accessed 10 October 2020).
- Chillier, Gastón (2006) Inteligencia en democracia, [http://www.lanacion.com.ar/nota.asp?nota\\_id=796483](http://www.lanacion.com.ar/nota.asp?nota_id=796483) (accessed 21 May 2019).
- Clarín.com (2003) [https://www.clarin.com/ultimo-momento/caso-amia-kirchner-ordeno-levantar-secreto-side\\_0\\_ryJlJbIcTe.html](https://www.clarin.com/ultimo-momento/caso-amia-kirchner-ordeno-levantar-secreto-side_0_ryJlJbIcTe.html), (accessed 10 October 2020).
- Clarín.com (2009a) Demanda contra el diario La Nación, [https://www.clarin.com/opinion/demanda-diario-nacion\\_0\\_S1\\_KzFRaFx.html](https://www.clarin.com/opinion/demanda-diario-nacion_0_S1_KzFRaFx.html) (accessed 21 May 2019).
- Clarín.com (2009b) Según el juez Oyarbide en la ciudad había “una verdadera Gestapo”, <http://www.clarin.com/diario/2009/11/18/elpais/p-02043242.htm> (accessed 21 May 2019).
- Dandan, Alejandra (2005) Las Valijas Salieron por un Mecanismo Aceitado’ <https://www.pagina12.com.ar/diario/elpais/1-47367-2005-02-15.html> (accessed 21 May 2019).
- Guardian.com (2015) The shady history of Argentina’s Intelligence Secretariat, <https://www.theguardian.com/world/2015/jan/27/argentina-intelligence-secretariat-shady-history> (accessed 21 May 2019).
- Guardian.com (2017) Argentinian lawyer Alberto Nisman was murdered, police report finds, <https://www.theguardian.com/world/2017/nov/06/argentinian-lawyer-alberto-nisman-was-murdered-police-report-finds> (accessed 21 May 2019).
- Lacunza, Sebastián (2015) Dirty intelligence games, <http://sebastianlacunza.blogspot.com/2015/01/dirty-intelligence-games.html> (accessed 21 May 2019).
- Mfa.gov.il (1992) Terror attack on the Israeli Embassy in Buenos Aires, <https://mfa.gov.il/MFA/ForeignPolicy/Terrorism/Hizbullah/Pages/Terror-attack-Israeli-Embassy-Buenos-Aires-17-Mar-1992.aspx> (accessed 21 May 2019).
- Mfa.gov.il (2007) 13th Anniversary of the terrorist attack on the AMIA Jewish community center in Buenos Aires-18 July 1994, , <https://mfa.gov.il/MFA/PressRoom/2007/Pages/13th%20Anniversary%20of%20terrorist%20attack%20on%20AMIA%20Jewish%20community%20center%20in%20Buenos%20Aires%2018-Jul-2007.aspx> (accessed 21 May 2019).
- Morales Solá, Joaquín (2009) La SIDE presentó dos querellas contra LA NACION, [http://www.lanacion.com.ar/nota.asp?nota\\_id=1157899](http://www.lanacion.com.ar/nota.asp?nota_id=1157899) (accessed 21 May 2019).
- Página12.com (2007) Los hackers se quedaron sin claves, <http://www.pagina12.com.ar/diario/elpais/1-106021-2008-06-14.html> (accessed 21 May 2019).
- Partlow, Joshua & Caselli Irene (2015) In Argentina, distrust over president’s move to abolish intelligence agency, [https://www.washingtonpost.com/world/the\\_americas/in-argentina-distrust-over-presidents-move-to-abolish-intelligence-agency/2015/01/27/c46c5b1e-a632-11e4-a162-121d06ca77f1\\_story.html?utm\\_term=.06b5e1ac3b93](https://www.washingtonpost.com/world/the_americas/in-argentina-distrust-over-presidents-move-to-abolish-intelligence-agency/2015/01/27/c46c5b1e-a632-11e4-a162-121d06ca77f1_story.html?utm_term=.06b5e1ac3b93) (accessed 21 May 2019).
- Taylor, Adam (2015) Why the death of an Argentine prosecutor is captivating the world, [https://www.washingtonpost.com/news/worldviews/wp/2015/01/21/why-the-death-of-an-argentine-prosecutor-is-captivating-the-world/?utm\\_term=.629228686a0d](https://www.washingtonpost.com/news/worldviews/wp/2015/01/21/why-the-death-of-an-argentine-prosecutor-is-captivating-the-world/?utm_term=.629228686a0d) (accessed 21 May 2019).

Ybarra, Gustavo & Colonna, Lucas (2005) Sigue en Vigor la Polémica “Ley Espía”, <https://www.lanacion.com.ar/politica/sigue-en-vigor-la-polemica-ley-espia-nid700765/> (accessed 21 May 2019).

Wikipedia.org (2020). [https://en.wikipedia.org/wiki/Front\\_for\\_Victory](https://en.wikipedia.org/wiki/Front_for_Victory), (accessed 10 October 2020).





Scientific article

0045.334:621(497.11)

616.98:578.834]-036.22(100)

## CONTINUITY OF WORK IN THE ENERGY SECTOR IN THE REPUBLIC OF SERBIA DURING THE COVID-19 PANDEMIC

Nataša MILETIĆ<sup>1</sup>

**Abstract:** *The World Health Organization (WHO) declared the Coronavirus (COVID-19) a global pandemic, and the whole world found itself in a crisis. No state or organization is ready to face the situation. Organizations must meet the problem in the right way; they must ensure the application of best practices. An essential prerequisite for crisis management is preparedness, as well as recognizing the crisis before it occurs. The situation can take many forms. The most sensitive branches for the problem's outbreak are critical infrastructures - water, food, energy, health, transport networks, chemical industry, nuclear industry and information and communication technologies. ISO Standard 22301:12 details what an organization needs to identify, document and establish to understand the organization and its context. Its application allows the organization to respond to emergencies and continue to operate in emergencies. Electricity was recognized as one of the most critical segments of infrastructure during the COVID pandemic. Since "Electric Power Industry of Serbia" is the Republic of Serbia's energy pillar, the paper aimed to show how it manages to maintain the supply of society and the state with electricity without interruption in emergency conditions.*

**Keywords:** *COVID-19, ISO 22301:12, business continuity, energy sector, Electric Power Industry of Serbia.*

### Introduction

Throughout its history, human society has faced various dangers that threaten its survival, whether natural or caused by human activity. Today, these natural, deliberate, organized incidents are occurring more often, and we are witnessing the significant consequences they have on people, property and the environment.

At the end of 2019 and the beginning of 2020, the whole world found itself in a crisis caused by the coronary virus pandemic, COVID-19.

No state is ready to face the crisis because no crisis announces its arrival. Crisis management has an essential task. Different security systems of the countries gave other answers to the problem, prescribed and adopted additional security measures to prevent the coronavirus spread, each based upon its own conditions.

The Republic of Serbia has been very rigorous in adopting security measures. A state of emergency has been declared, and a state of emergency is activated when a public danger endangers the country's survival or citizens. This further implies that some typical government

---

<sup>1</sup> MSc, Faculty of Security Studies, University of Belgrade, Republic of Serbia

and society functions are suspended, which means that the state's entire system of functioning must be adapted to the conditions that correspond to the crisis. The prescribed measures include quarantine, self-isolation, prohibition of movement, prohibition of gathering, physical distancing, closing of educational institutions, institutions of entertaining character and the obligation to wear protective equipment, specifically masks and gloves. Human life and human health are the most critical protected value. Still, for the prescribed measures to be implemented, it is necessary to protect the infrastructure's function.

Critical infrastructure means systems, networks, facilities, or their parts and the interruption of delivery of goods or services can have severe consequences for national security, human health, and life, property, environment, the safety of citizens, economic stability, or may jeopardize the functioning of the Republic of Serbia (Law on Critical Infrastructure, 2018).

Sectors in which critical infrastructure is identified and determined are energy, transport, water, and food supply, health, finance, telecommunications and information technologies, environmental protection, the functioning of state bodies (Law on Critical Infrastructure, 2018).

Council of Europe Directive 2008/114/EC also defines energy as a sector that needs to have defined critical infrastructure. Electricity, oil, and gas are singled out as sub-sectors in that sector (COUNCIL DIRECTIVE 2008/114/EC).

Electricity is defined as critical infrastructure because electricity is necessary for the production and transmission of electricity; it is for society's normal functioning.

We recognized electricity as one of the vital infrastructure segments during the COVID-19 pandemic because electricity production and distribution is of paramount importance for the operation of health centers, hospitals, pharmacies, conducting "online classes", and the like.

Although electricity supply in the region is uninterrupted, there are several risks to its functioning. One of the problems is whether the necessary maintenance work will be done on time, whether the financial liquidity of energy companies will be jeopardized due to falling billing and reduced consumption and electricity prices. Simultaneously, the largest problem facing energy companies is the employees' organization (Todorovic, 2020).

All power systems in the region and the Republic of Serbia's power system have introduced emergency procedures to mitigate the consequences of the coronavirus spread.

### **ISO 22301: 2012 Societal security - Business continuity management systems - Requirements**

The growing complexity and unpredictability of crises have given impetus to international standardization in social security. Within the International Organization for Standardization ISO in 2006, work was established on the adoption of international standards from the ISO/223 series. One of them is the ISO 22301 - business continuity management system (Risk Analysis and Crisis Management Center).

ISO/TC223 develops international standards to increase social security, i.e., society's protection and response to accidents, emergencies and disasters caused by intentional and unintentional actions of the human factor, natural and manmade disasters and hazards. It is a comprehensive approach that includes adaptive, proactive, and reactive strategies in all phases before, during, and after the end of an emergency. Social security is a multidisciplinary field and includes actors from the public and private sectors and civil society organizations (Risk Analysis and Crisis Management Center).

ISO 22301:2012 Societal security - Business continuity management systems - Requirements is a standard related to business continuity management, applying a holistic management process that identifies potential threats to the organization, including their consequences.

A business continuity management system refers to a systematic approach to business continuity management in a company. ISO 22301:12 details what an organization needs to identify, document, and establish to understand the organization and its context.

The main goal of such a system is to ensure business continuity for all products and services.

The main goals of ISO 22301 are:

- identification and protection of crucial products and services while ensuring their continuity;
- the ability to manage the incident allows for an effective response;
- only an understanding of the organization and its relations with other organizations, relevant supervisory or management boards, local authorities, and intervention services is developed, documented, and understood correctly;
- staff are trained to respond effectively to an incident or interruption through proper exercises;
- understanding the requirements of interest and the ability to deliver;
- in case of disruption, the staff receives adequate support;
- the procurement chain of the organization is provided;
- the reputation of the organization is protected and
- the organization remains compliant with legal and contractual obligations (Kurika, 2013).

This system helps establish a clear understanding of how business works and where it can be if a failure occurs. It provides opportunities to improve business processes.

It is vital to apply the ISO 22301 standard of business continuity management systems, especially in high-risk areas, such as oil and gas transportation works, public services, financial services, telecommunications and food production.

Extraordinary events can cause a standstill or disruption in the functioning of the organization at any time. This standard application allows the organization to respond to exceptional circumstances and continue to operate in emergency conditions. Events have different dimensions and forms, ranging from great natural dangers to terrorist activities, technical accidents with economic, environmental and other consequences and losses. Many adverse events are not large in scale. Nevertheless, they can have significant implications to business continuity, so public and private sector organizations are expected to prepare for and respond to unexpected events (ISOTC 292).

The ISO 22301 standard contains a framework for planning, establishing,

implementing, monitoring, supervising, maintaining and continuously improving the business continuity management system (BCMS). It helps an organization, regardless of its type and size, to protect itself from unexpected events (Risk Analysis and Crisis Management Center).

It provides a framework for the development and achievement of operational resilience of companies whose implementation contributes to:

- protection against incidents,
- reducing the likelihood of incidents,
- preparing and responding to incidents, and
- recovery from incidents in the event of their occurrence.

The critical components of BCMS are:

- business continuity policy,
- people with defined responsibilities,
- process management related to:
  - policy,
  - planning,
  - introduction and functioning of business continuity management,
  - performance evaluation,
  - management recommendations,
  - business continuity management improvements,
- a set of documents subject to audit and
- all other business continuity management processes that are relevant to the organization (Labus, 2014).

## **The electric power industry of Serbia applies a business continuity management system**

Serbia's electric power industry is a public enterprise for electricity production, distribution and trade in electricity. The public enterprise "Electric Power Industry of Serbia" is the largest in Serbia, the country's economic and energy support. PE EPS's share in the electricity market is around 97 percent, even though more than 70 suppliers currently operate in Serbia (Elektroprivreda Srbije).

The principal activity of PE EPS is electricity trade, as well as electricity generation, electricity distribution, management of the production and distribution system, coal processing and transportation, steam and hot water production in combined processes performed in related companies founded by PE EPS for accomplishing the mentioned activities.

"The mission of Serbia's PE Electric Power Industry is to securely supply customers with electricity, under market conditions, based on continuous production by raising the quality of services and customer satisfaction, improving environmental care

and increasing the general welfare of the community” (Three-year business program of the Public Enterprise “Electric Power Industry of Serbia”, Belgrade for the period 2020-2022).

“The vision of PE Electric Power Industry of Serbia is to be a socially responsible, market-oriented and profitable company, competitive in the regional market concerning the highest standards of business and sustainable development, recognized as a reliable partner to domestic and international companies” (Three-year business program of the Public Enterprise “Electric Power Industry of Serbia”, Belgrade for the period 2020-2022).

PE EPS defines in this document the fundamental goals of its business policy, as follows:

- “reliable production and supply of electricity to the customers based on the terms of delivery,
- organizational, technical-technological and economic-financial improvement,
- improvement of environmental protection according to the national and the regulations of the United Nations and the European Union,
- corporatization of EPS while preserving and strengthening the integrity of the company,
- participation in the internal and regional electricity market and the establishment and maintenance of an influential position in the region” (Three-year business program of the Public Enterprise “Electric Power Industry of Serbia”, Belgrade for the period 2020-2022).

### **Program for the improvement of integrated management systems**

One of the most critical priorities of PE EPS is the regulation of the company’s business and harmonization with international standards’ requirements by implementing projects for the introduction and certification of management systems and their integration into a single integrated management system. By implementing, maintaining and continuously improving various management systems, PE EPS improves its business efficiency and effectiveness, continually works to meet the expectations of customers and all other stakeholders, identify and reduce risks and understand the business context of the company (Elektroprivreda Srbije).

The purpose of the business continuity management system is to improve the resilience of PE EPS, inter alia, by developing mechanisms and timely identifying risks, minimizing and ultimately preventing the effect, i.e., the impact of adverse events, incidents, emergencies or crises. The development of such mechanisms in PE EPS creates protection against harmful events, experiences, troubles or concerns that cause or could cause disturbances in the business processes. It reduces the likelihood

of incidents, emergencies or crises. Considering the objective facts and circumstances, it prepares a timely response to act in situations where these occurrences take place, including a recovery strategy after their occurrence. In the period following incidents, harmful events, emergencies or crises, the existence, application, maintenance and improvement of the business continuity management system creates the possibility for the PE EPS to continue the ordinary course of business processes. On the other hand, in the event of large-scale adverse events, in the long run, the established business continuity management system supports faster recovery and return of business activities to normal as soon as possible. The goal of PE EPS is to develop, implement, and maintain business continuity management programs to prepare responses and manage all types of business process disruptions.

The key objectives of the business continuity management system include the following:

- emphasizing the importance of the business continuity management system within PE EPS, ensuring that the staff engaged in all activities of the PE EPS is instructed on the existence of business continuity plans and their role in them,
- incorporation of elements of a business continuity management system into the corporate culture of PE EPS so that it becomes an integral part of every strategic decision-making process,
- ensuring that critical activities and complex processes are identified, and that there are appropriate business continuity programs for such activities and operations, developed precisely about the specifics of these activities and functions,
- formulating methodological and structural responses for planning and preparing responses to adverse events, incidents, emergencies and crises,
- providing a regular review, adjustment, i.e., change and improvement, as well as testing, i.e., training and simulation of the established business continuity management system,
- developing and reviewing plans and programs for continuous improvement based on acceptable business practices, the established business practice, as applicable. It applies legal and other regulations and the requirements of the international standard ISO 22301 (Elektroprivreda Srbije).

### **The work of the Electric Power Industry of Serbia during the state of emergency**

All activities of the “Electric Power Industry of Serbia” are directed in such a way as to ensure stable production and uninterrupted supply of electricity for the economy and citizens of Serbia. Even in these extraordinary circumstances.

EPS' goal is to enable the system's smooth functioning and ensure continuous production and supply of electricity for all citizens and the economy by applying all necessary measures to limit the spread of coronavirus to a minimum (Elektroprivreda Srbije).

It is imperative and challenging to ensure electricity production without interruption. If there is no electricity, a problem will arise in hospitals and health centers, online classes and the whole functioning would be in trouble. EPS does a responsible job, which is always, and especially in this situation, of crucial importance for the life in Serbia. Someone's life depends on them, the life of someone who is lying connected to a ventilator, because if EPS and the production and distribution of electricity stops, then everything will stop.

After declaring a state of emergency, PE EPS established a crisis headquarters to ensure the system's stability and employee protection during the coronavirus spread. EPS was among the first to adopt measures to be applied in the entire business system. Clear procedures for behavior, employees and managers are defined to maintain all energy companies' smooth operation and ensure a reliable supply of key energy sources.

Teams have been formed to organize the work in production and distribution. An order has been issued to define all work processes. Additionally, the employees who are indispensable in the process so that all the work goes smoothly are also defined. Priorities have been set and the number of people coming to work has been reduced.

As employees are the most outstanding value of EPS, taking care of them comes first. All protective equipment has been provided and the company strictly adheres to the measures that protect workers' health during this challenging time of the fight against the coronavirus. The possibility of contact has been reduced and employees who stayed abroad were sent to self-isolation. All protective equipment for the employees indispensable to the system's operation has been provided and the application of measures is continuously monitored.

Disinfectants have been placed in all EPS premises and continuous procurement of additional quantities is provided. The employees exposed to an increased risk of coronavirus infection at their workplaces are supplied with other protective equipment. Protective masks and gloves were distributed to all EPS employees throughout Serbia.

As a socially responsible company, EPS has met the citizens' needs to the maximum in these difficult times. Every effort has been made to read all customers' meters as part of regular activities, respecting all protection measures. To reduce the possibility of contact and protect citizens' health, the "Electric Power Industry of Serbia" has provided customers with the opportunity to read their electricity meter and indicate the state of the meter and the date of reading in a visible place at the entrance to their homes. According to the electricity meter's location, the phone number is printed on the invoice or in an e-mail by sending the data to the e-mail addresses. If the users are late with the bill's payment during the state of emergency, they will not be charged any interest and the deadline for pensioners has been extended with a discount of five percent.



Thanks to the responsible and professional engineers, miners, fitters, dispatchers and all EPS workers, EPS stably supplies electricity to all hospitals, households, police, army, food, medical equipment warehouses, grocery stores and pharmacies. All critical consumers must have a stable supply of electricity. The supply routes for COVID-19 hospitals have been strengthened, so as to ensure their regular supply at all times, said the Minister of Mining and Energy.

Electricity consumption is between five and seven percent lower than in previous years in the same period, probably because the economy is operating with a slightly reduced capacity, which is not terrible because it shows that the economy is working. The mining and thermal sector of “Electric Power Industry of Serbia,” even during difficult situations, works reliably. With all employees’ outstanding commitment, excellent production results are achieved every day, which is crucial for the Serbian power system.

Even during a state of emergency due to the coronary virus pandemic, the entire EPS system functions reliably and stably. According to Milorad Grčić, c. d. Director of Serbia’s Electric power industry, “the situation in “Electric Power Industry of Serbia” and other energy companies is stable. There are no problems with the functioning and supply. Severe measures are being taken to maintain this situation. The possibilities for additional steps that could be applied in the coming period, in case of aggravation of the condition with the spread of the virus, have also been considered” (Elektroprivreda Srbije).

## Conclusion

Today’s threats require managing the process in a way that ensures the survival and sustainability of the organization’s core activities before, during and after the disruption. An organization’s ability to recover from a disorder is directly related to the degree of business continuity planning before the condition occurred.

The ISO 22301 Business Continuity Management System provides an efficient and rapid response to unexpected events based on the processes applied before, during, and after these events. The fact that companies have prepared business continuity plans means that they are ready for unexpected situations. Business continuity plans ensure that the business can continue without significant impact and losses.

Developed integrated management systems contribute to significant savings at the national level and provide recognizable benefits to society. PE EPS is committed to the business, the care for environmental protection, safety and security at work, raising awareness of the importance of energy efficiency and information security and social responsibility.

Thanks to the good organization and business continuity plans, PE EPS managed to stop the spread of the coronavirus in companies and accomplish its fundamental goal of enabling the system’s uninterrupted functioning and ensuring continuous production and supply of electricity to citizens and the economy.

It was stated that the energy supply in the region is uninterrupted. Still, if we make a parallel, we can say that the Republic of Croatia is the country that has done best in the fight against COVID-19.

As a crucial critical infrastructure of strategic importance for the Republic of Croatia, the Croatian Electric Power Industry also operates according to the regulations of ISO standard 22301. HEP, by the National Civil Protection Headquarters' decisions and the recommendations of other public health bodies, ordered all subsidiaries to take the necessary measures to combat the spread of diseases caused by the coronavirus. There was a reorganization of the business. The new work organization's primary goal is to ensure optimal implementation of the investment plan and ensure the continuity of service provision by the protocols on worker safety and prevention of the spread of COVID-19. We continuously review key activities, assess implementation plans, anticipate potential risks, and devise measures to eliminate them (Elektroprivreda Hrvatske).

Today, this standard has become a bestseller in the field of standardization and certification. Studies show that two out of five companies go out of business within five years of the adverse event. Also, the latest developments indicate that most companies in the future will be in a situation to react to a disturbance that may interrupt or jeopardize their daily business. To recover from the disaster, i.e., to manage to maintain their business, more and more companies decide to apply the ISO 22301 standard - business continuity management. The costs of introduction are incomparably lower than the potential losses.

## REFERENCES:

- Law on Critical Infrastructure, "Official Gazette of RS" No. 87/2018, Article 4.
- Law on Critical Infrastructure, "Official Gazette of RS" No. 87/2018, Article 6.
- COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Annex I [online]. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2008.345.01.0075.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG) [accessed: 29 October 2020].
- Todorovic, I. (2020) Power systems in the region in crisi mode due to coronavirus, Balkans green energy news, available: at <https://balkangreenenergynews.com/rs/elektroenergetski-sistemi-u-regionu-u-kriznom-rezimu-zbog-korona-virusa/> [accessed 29 October 2020].
- International standards, The Center for Risk Analysis and Crisis Management, available: <http://www.caruk.rs/medunarodni-standardi/> [accessed 29 October 2020].
- Kukrika, M. and Delic, Z. (2013). Business continuity management - Practical application of ISO 22301: 2012 Social security - Business continuity management systems – Requirements [e-book]. Available at: <https://www.scribd.com/doc/152052499/Kukrika-Upravljanje-Kontinuitetom-Poslovanja> [accessed: 29 October 2020].
- ISO 22301 Security and resilience - Business continuity management systems – Requirement, ISOTC 292, available: <https://www.iso292online.org/published-standards/iso-22301-ed2/> [accessed: 29 October 2020].
- Labus, M. (2014). Business continuity management according to ISO 22301 standard, available: <https://www.slideshare.net/goranvranic/milica-labus-belox-srbija-upravljanje-kontinuitetom-poslovanja-po-iso-22301-standardu> [accessed 29 October 2020].
- Elektroprivreda Srbije, available: <http://www.eps.rs/eng/Pages/Main-information.aspx> [accessed 30 October 2020].

Three-year business program of the Public Company “Electric Power Industry of Serbia”, Belgrade for the period 2020-2022, “Official Gazette of RS”, No. 094/2019 of December 27, 2019.

Elektroprivreda Srbije, available: <http://www.eps.rs/cir/Pages/Kvalitet.aspx>, [accessed 30 October 2020].

Elektroprivreda Srbije, available: [http://www.eps.rs/lat/tent/Stranice/Politika\\_kvaliteta.aspx](http://www.eps.rs/lat/tent/Stranice/Politika_kvaliteta.aspx) [accessed 30 October 2020].

Elektroprivreda Srbije, available: <http://www.eps.rs/lat/vesti/Stranice/krizni-stab.aspx>, [accessed 01 November 2020].

Elektroprivreda Srbije, available: <http://www.eps.rs/eng/vesti>, [accessed 01 November 2020].

Elektroprivreda Hrvatske, available: <https://www.hep.hr/> [accessed 04 November 4 2020].

## HUMANITARIAN DIPLOMACY AND ITS IMPACT IN TIMES OF PANDEMICS AND HEALTH CRISES

Igor GELEV<sup>1</sup>  
Biljana POPOVSKA<sup>2</sup>

**Abstract:** *We are witnessing a health crisis caused by a virus. Its planetary dimensions have brought fear and unrest to both national governments and the world's population. The world has taken a few steps back while almost every segment of human life has stagnated. Economy, social life, education, and even politics for a moment seem to be on the margins of the social life, while each of the national governments are struggling to successfully deal with the virus called COVID 19.*

*As the world faces a global threat, some countries have taken advantage of the health crisis to exert their own influence on the international diplomatic scene. China has used humanitarian diplomacy and soft power to increase its influence in the countries of interest that are not of immediate surroundings. Selflessly giving medical support to the countries which were most affected by the virus China was seen as a country and economic partner that each country would like to have.*

**Keywords:** *humanitarian diplomacy, soft power, fake news.*

### Introduction

This paper focuses on the soft power as a tool for achieving political, economic, and military influence in times of pandemics and health crises with special emphasis on China and its humanitarian diplomacy amid a global health crisis.

When we talk about soft power the best example of its successful implementation is China. Hence, the application of soft power will be explained through the example of China.

In terms of public diplomacy or specifically in the area of micro regional public diplomacy in Asia and Africa, China is ahead even before the United States. Moreover, this type of diplomacy determined by the principle of conquest (in economic and trade terms) makes the United States a vulnerable giant. As an illustration, it is worth to mention that despite the US military campaigns in the Muslim world accompanied by numerous scandals in the past (Guantanamo, Abu Ghraib), China has conquered markets in the Muslim world, making them dependent on its own products and culture.

---

<sup>1</sup> Dr. Igor Gelev is an officer in the rank of lieutenant colonel, employed in the Army of the Republic of North Macedonia. Research and reflection in the paper are the author's personal views and are not related to the institution he comes from.

<sup>2</sup> Biljana Popovska, MA, is an advisor at the Ministry of Defense, PhD student at the University of Bucharest, Romania.

Soft power as an alternative to hard power in China was initiated as a result of its political, academic and business ties with the far-off world, as well as Europe, America and Africa. China's fast-growing military power was a guarantor of the stability of its external borders in Asia. However, the powerful China could not be satisfied with being only a superior force in Asia. This economic and military giant sought dominance in the area of interest (described in military terms). Thus, after the economic conquest of Europe and the United States, its next destination was Africa, where its first military base outside its own borders was built.<sup>3</sup> Hence, Africa could be the place and the cause for the next multilateral Cold War.

### **China's Humanitarian Diplomacy in Africa**

Great industrial potential, natural resources, alternative bio-fuels, exploitation of mineral wealth and other natural resources pushed the race to conquer Africa.

Africa, the second largest continent, is known for its colonialism, extreme poverty, and numerous civilian i.e. civil wars, that kill children, soldiers, and civilians on a daily basis. The tradition of friendship and economic opportunities of African countries with China dates back a long time through the Chinese aid project to Third World countries. However, during the last two decades it gained in intensity that (will) cause a new cold war between the West and China.

China's relations with Africa date back to the formation of the "new China" in 1949. During the Cold War in the 1960s, China supported liberation movements in several African countries, designing a socialist environment by building hospitals, railways, exchanging engineers and promoting the *Doctors without Borders* project.<sup>4</sup>

### **Building a "Win-Win" interactive relationship between China and the African Countries**

At a time when the West was engaged in global wars, export of democracy and military engagement in the Middle East, China got engaged and replaced the former political and social colonialism in Africa with an economic win-win interactive relationship. The Institute of Public Diplomacy in China promoted Public Diplomacy towards Africa or the Beijing Consensus project for long-term socio-economic cooperation with African countries by fully respecting the territorial integrity and political sovereignty of the states. Instead of creating different political systems and governments according to its own taste, China supported the existing governments by offering benefits and assistance to the entire country. Thus providing in the med-term

---

<sup>3</sup> For the first time in its history, China has built a military base on the Somali peninsula known as the African Horn or African Cape (this region is the only place for logistical access to the common market in East and Southeast Africa for more than 20 continental countries). In the same belt, China has built the Addis Ababa-Djibouti railway as an essential economic project. However, China does not call it a military base, but a base for providing material and technical support needed by the Chinese navy.

<sup>4</sup> <https://www.doctorswithoutborders.org>

accession of 19 African countries to NEPAD (New Partnership for Africa Development) aimed at halting African marginalization in relation to globalization. China employed a mutual relationship with the African countries on a state-to-state basis, i.e. citizen-citizen. This principle meant ‘Deng Xiaoping model’ or crossing the river by feeling the stones, i.e. integrating the common interests and their application in practice. The main trump card of China’s public diplomacy in Africa was the slow but steady economic development as not to provoke corruption, ethnic and confessional civil wars.

Initial investments were modest and parallel to the cultural development of the population so as not to create a vacuum in the education and technological development of their economies. To that end and speaking in geographical terms China begun to eradicate hunger in phases by stimulating the population to a basic education of self-sufficiency and creating conditions for normal living. Next step was a clean water project that led to several civil wars in some African countries.<sup>5</sup> This was followed by winning over the population and its ‘cultivation’ in China, to return and be engaged in the process of developing the African countries.

The best soft power project used as a tool was the *medical diplomacy*, which meant direct help to the population. China delegated its first medical team back in 1964 upon a request of the Algerian government. Since then, China has sent about 15,000 doctors to 47 African countries and has treated about 180 million African patients. In 2003, China sent 860 medical personnel and 35 teams of doctors to 34 African countries (Xinhua, December 16, 2004).<sup>6</sup>

At the same time, China was not rushing to exploit the natural resources of these countries, thus creating mutual trust. Mutual interest did not have the status of colonization or any other type of exploitation, but economic collaborative cooperation. For example, China has invested in 900 economically strong companies in Africa, while the total investment in the economy, without the part pertaining to the infrastructure, is \$ 39.7 billion.<sup>7</sup> China has also provided significant economic assistance to governments, at very low interest rates, completely free technical and technological development for African companies, subsidizing African start-ups, social health, education and free infrastructure (roads, bridges, electrification and gasification). China’s interest has been in concluding long-term economic agreements to use oil with Nigeria, Sudan and Angola. It has also made a series of agreements with countries that do not have oil, but have an infinitely large amount of specific minerals necessary for technological development for the industry and energy.

China’s approach to Africa resulted in a successful joint system of “development resources” by creating multilateral relations with African countries.<sup>8</sup>

---

<sup>5</sup> <https://pulitzercenter.org/projects/africa/water-wars-ethiopia-and-kenya>

<sup>6</sup> Thompson Drew. China soft power in Africa: from the “Beijing Consensus” to health diplomacy. s.n.2005

<sup>7</sup> Thompson Drew. Op.cit., 1-5

<sup>8</sup> Daniel Johanson, Jie Li, New Perspective on China’s Relations with the World, Chapter 10,

## **Chinese economic diplomacy to “conquer the world”**

China’s public diplomacy has a time frame which firstly includes economic conquest of the domestic political scene, then the Southeast Asian region, and finally the world. It based its soft power on foreign aid to other countries, economic ties with states, and cultural transmission. To this end, by creating economic competition with others, it successfully used the code of success at the domestic political scene in a time when people did not care about the democratization of society, because it was an economically successful society in times of financial crisis. This was followed by the economic conquest of the Southeast Asian region, which in combination with economic diplomacy enabled the creation of a regional economic bloc, tourism development, business investment and many development initiatives.<sup>9</sup> It has also created free trade zones, economic alliances, trade agreements and long-term economic agreements with countries in the region. The next step in the soft power was exporting of Chinese private companies around the world, especially in countries that have clashed with the traditional West.

## **European (non) solidarity during health crises**

The COVID 19 virus pandemic, which began in Wuhan, China and later spread to neighbouring Asian countries and Europe, become a nightmare for the European countries. European governments have faced a hitherto unknown enemy, a virus that has virtually halted all social processes in the country. The ignorance concerning the characteristics and the strength of the virus, as well as the lack of an effective drug and undisciplined behaviour of citizens in almost all European countries have increased the number of infected, and consequently the number of deaths. Fear of the uncontrolled spread of the virus was further stimulated by its ineffective handling by the national governments, as well as the numerous WHO paradoxical statements.<sup>10</sup> At the same time, some world leaders openly expressed doubts about the credibility of the organization’s leaders in tackling the pandemic as well as taking measures and actions to combat it. In particular, the US President, who withdrew almost all financial programs intended for the WHO. This provoked a backlash from China, which sees it as a hasty decision directly reducing the organization’s efficiency at a time when it is facing one of the world’s biggest challenges in the 21st century. Rhetoric sparked verbal attacks by the

---

Ilaria Carrozza, China’s Multilateral Diplomacy in Africa: Constructing the Security-Development Nexus, E-International Relations Publishing, p. 145-150.

<sup>9</sup> Nadege Rolland, China’s vision for a new world order, The National Bureau of Asian Research (1414 NE 42nd Street, Suite 300 Seattle, Washington 98105).

<sup>10</sup> WHO - World Health Organization is part of the UN, established in 1948 in Geneva, and is directly responsible for developing special programs for early warning and dealing with epidemics and pandemics.

<https://www.aspistrategist.org.au/the-who-has-failed-the-world-in-its-pandemic-response/>

US diplomacy on China, accusing it of hiding crucial information about the pandemic at a time when its spread could still be controlled. Even the US president went a step further by calling the virus Chinese.<sup>11</sup> In addition, he accused China of being responsible for the suffering of the whole world, which further aggravated the overall situation in conditions when there was a need for unity and consolidation of the great powers to deal with the crisis.

During this time, the virus began to spread in Europe, and some European countries were severely affected, especially Italy and Spain. The number of infected and deceased was rapidly increasing and reminded the world of catastrophic scenarios that occurred in the 1920s during the Spanish flu<sup>12</sup>. News reports from Italy spoke of several thousand deaths every 24 hours, while medical workers desperately sought medical help from the country's government. The Italian government asked for help from the EU, recalling the solidarity of EU members.<sup>13</sup> But instead of helping, each member of the Union closed the borders and banned the export of medical supplies and equipment (ventilators), leaving the affected members Italy and later Spain to deal with the virus on their own. Medical staff was also exhausted in their efforts to accommodate and assist the diseased. Entire social systems collapsed under the onslaught of the virus. Armed forces were deployed to move and transport the bodies of the victims of the virus. All capacities of the state were put in function to deal with the increasingly probable catastrophic scenario threatening the state. The Italian "dam" began to crack under the pressure of the virus. The Italian government requested help from all members of the Union, which have closed their borders and had forgotten about European solidarity, mutual support and the need to help Italian citizens. Later on, the European Commission has apologized to Italy for the lack of solidarity from the EU.<sup>14</sup>

### **Chinese humanity as a tool for exercising influence amid the pandemic**

Just when it seemed most difficult and it looked like Italy was suffocating in its own social anomalies (dysfunctional critical infrastructure, poor epidemiological care for the population in the past, weak inter-ministerial cooperation), China's aid came to fore, like in a movie scenario.<sup>15</sup> Several Chinese planes landed at the Rome airport,

<sup>11</sup> Washington Post, Allyson Chlu, EDT 7, March 20, Edition III, Online, 2020 (<https://www.washingtonpost.com/politics/2020/06/22/mcenany-sloppy-misleading-effort-defend-trumps-indefensible-use-kung-flu/>).

<sup>12</sup> Spanish fever or Spanish flu is one of the deadliest pandemics in human history. It appeared at the end of World War I and lasted for three years, killing about 50 million people. Five times as many people died from the disease as from the war.

<sup>13</sup> [www.politico.eu/article/coronavirus-italy-needs-europe-help](http://www.politico.eu/article/coronavirus-italy-needs-europe-help)

<sup>14</sup> <https://www.bbc.com/news/world-europe-52311263>

<sup>15</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_600](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_600)

<https://www.euractiv.com/section/coronavirus/news/eu-allocates-chinese-aid-to-italy-to-fight-against-the-pandemic/>



carrying thousands of tons of medical supplies and equipment, rapid virus detection tests, automated robots for scanning infected people with symptoms of the virus, and certainly the most important human potential i.e. doctors and epidemiologists with experience of combating the Wuhan virus.<sup>16</sup> The urgent need for protection, ventilators, disinfectants, and medical staff highlighted the reasons for signing the numerous bilateral agreements which were later reached between the Chinese and Italian governments. Chinese aid did not stop there. It was offered to any other government that sought help and requested medical supplies, funds and medical staff (the last category was only approved for countries of strategic importance to China).<sup>17</sup>

Certainly, all this meant the beginning of the need to redefine the Union as we know it. Many members have been left to fend for themselves with the virus, instead of implementing the current strategy of supporting each other to deal with threats. This meant that each national government had to build its own strategy to deal with each type of threat at its own national level, and not to rely on pieces of paper - agreements, principles and obligations on which the Union rests. At the same time, it meant building new bilateral alliances and co-operating with non-EU countries. Such is the case with China. China seeks to form formal and informal alliances with European countries over its Silk Road project<sup>18</sup>.

With its humanitarian diplomacy, China has won the hearts and minds of EU citizens, especially those of the periphery of the Union's political map. Medical care has proven vital in dealing with the virus. The way China, a communist-dominated state with a capitalist economic apparatus has done this, seems to be ideal for winning sympathy around the world. Undoubtedly, the Union's financial assistance to its members, as well as to the Western Balkan countries, is much higher than that of China, but still China has valorised it much more. There are several reasons for this. First, China acted immediately, unlike the slow bureaucratic apparatus of the Union. Then, China sent medical personnel with hands on experience from Wuhan to Italy. This enabled rapid training and organization of Italian medical staff to efficiently fight the virus. China has also inadvertently provided assistance to anyone in need, even symbolically and diplomatically to the United States. All of this has given the world the impression that China is trying to create a new world, more human than the previous world in which money reigns, especially in countries where primary health care is unattainable for the average citizen.

---

<sup>16</sup> [www.dw.com/en/covid-19-china-steps-in-to-help-italy-battle-the-virus/a-52901560](http://www.dw.com/en/covid-19-china-steps-in-to-help-italy-battle-the-virus/a-52901560)

<sup>17</sup> The New York Times, Steven Lee Myers and Alissa J. Rubin, March,20, ED,2020 ([www.nytimes.com/2020/03/18/world/asia/coronavirus-china-aid.html](http://www.nytimes.com/2020/03/18/world/asia/coronavirus-china-aid.html))

<sup>18</sup> It is an ambitious project for China to establish infrastructure projects from China through Europe to the Middle East and Africa. For many countries, this will mean a lot for the economy, especially for foreign trade and foreign markets.

## **Social media as a tool of soft power for creating opinion of the audience (general world public)**

Part of the soft power was realized through the Internet. It should be borne in mind that the role of non-state actors on the Internet during health crises can be really big. Actors who stimulate processes through the Internet do so in a deductive way in order to identify the steps for achieving the ultimate goal. Considering that this is the digital age, the beginning of achieving influence and purpose is the cyberspace. Hence, in the part of self-promotion, numerous projects have been made and have been dis-seminated through social networks. The impact of social networks in crisis situations has a decisive factor in creating public opinion.

To this end, actors who use soft power through social networks during the pandemic do so in three stages. The first stage is to get acquainted with the type of source of threat.<sup>19</sup> At this stage, the data are generally completely true to ensure the credibility of the source of the information. In the second phase, the problem is exaggerated by its strength, intensity and threat. At this stage, some of the semi-true and untrue information is inserted to identify the cause of the threat. According to the US media, China contributed to the spread of the virus as it censored the initial information about the virus. On the other hand, Chinese media report about the zero-patient with corona virus as an American Marine, participant of a military exercise in Wuhan.

The third stage is the stage when social networks are used as a space for assimilation, expanding their influence, spreading their own values, twisting the truth, but also (de)mystifying the altruistic processes of certain countries during the crisis. At the same time, the Internet was used to stimulate fake news from various state and non-state actors as part of the cyber war of the great powers.

### **Fake news**

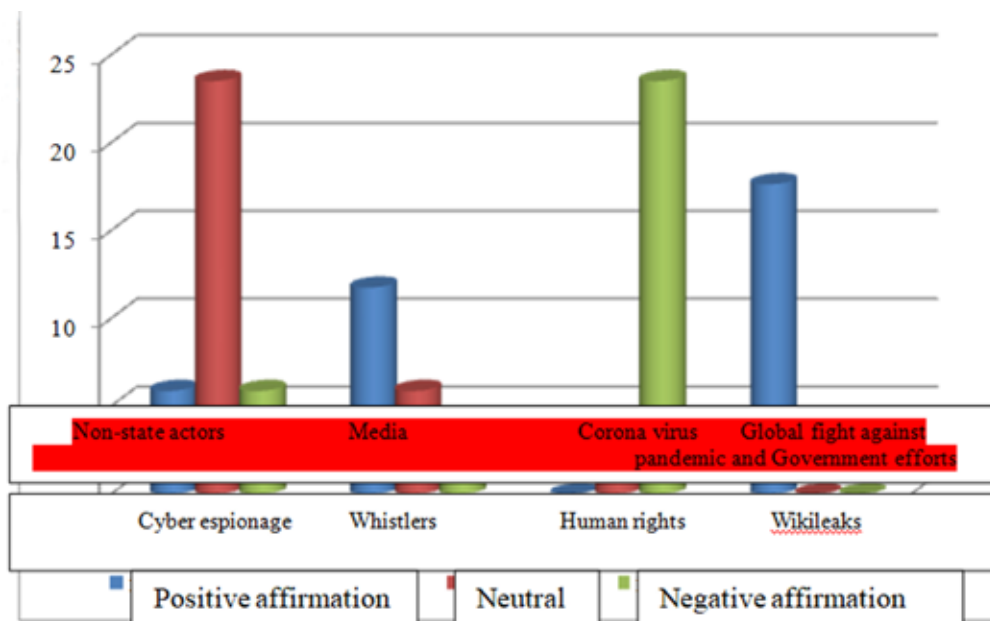
Fake news has become a daily occurrence of the Internet and has had a major impact on creating public opinion during the pandemic. The most common fake news was the impact of the 5G network over the effects of the virus, mass vaccination of the world's population and chipping (putting an electronic chip on each individual). This was the most exposed news on social media covering the topic of the virus. For this purpose, as authors of the text, we conducted a small survey on the social network Facebook in three Facebook groups with over 20,000 members where news about the virus was shared, in the period from April 1 to April 16. We compared the shared news related to three categories. The first category is the concept of putting an electronic chip on each individual to control the mind. The second category is mass vaccination for the purpose of making a large financial profit. The third category is the impact of the 5G network on the effect of the virus.

---

<sup>19</sup> A source of threat can be a military actor, natural disasters, virus or other threat that has the potential to threaten the individual and collective security.

A Facebook group was the unit of content analysis. Then, the results are mutually analyzed, semantically linked, and compared by using Semantic Text Analysis Software.

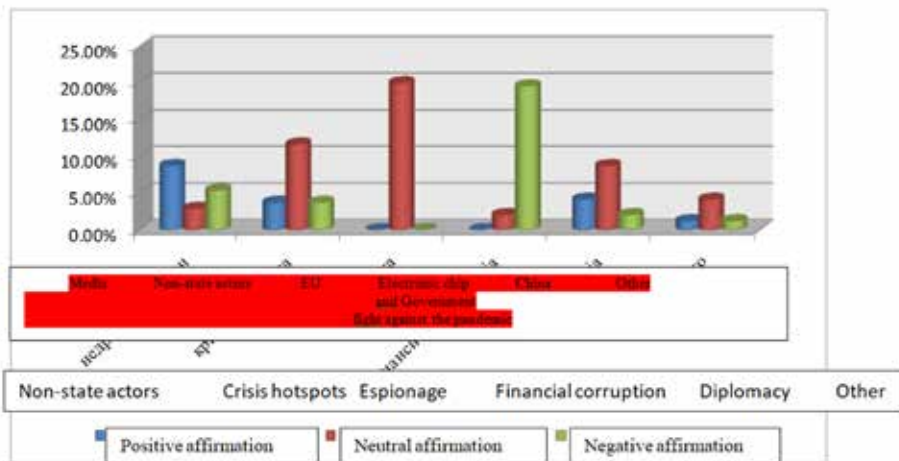
Figure 1. **Support for national governments before the announcement of the possibility of mass chipping of the world's population.**



The data were obtained by using the analytical software *Tropes*. Semantic analysis of certain words in texts that gravitate to the phrase *global war on pandemic* was made. Thus, when we analyze the term non-state actors and their role in the global war against the pandemic, in the content of the published texts on this topic, as far as the early warning of possibility about spreading the epidemic, lack of accurate data on mortality and virulence of the virus, involvement of civil protection in the fight against the pandemic, use of existing drugs for SARS, it turns out they had a neutral affirmation. To be more specific, out of a total of 25 texts, 21 or 84% of the texts are neutral affirmations while 2 texts or 8% had neutral and equally negative affirmations. This is due to the fact that some non-state actors were not given a greater role by the media as epidemiologists warned about major uncertainties of the virus. Each claim should be taken with great reservations, especially if it originates from public figures that are not part of the medical profession. In addition, the media as a key variable in the fight against the virus have had a positive affirmation because the public perceived them as heroes exposed to danger in the field (out of 20 texts, 12 texts or 60% had a positive affirmation, 6 texts or 30% had a neutral affirmation, and 2 texts or 10% had a

negative affirmation). By analyzing the content of the text, the term corona virus had an extremely negative affirmation (out of a total of 25 texts, 23 texts or 92% had a negative affirmation, and only 2 texts or 8% had a neutral affirmation). Support of national governments refers to the ways of dealing with the pandemic and its transparency in publishing data on the current situation with the virus (out of a total of 20 analyzed texts, 18 texts or 90% had a positive affirmation, and only 1 text or 5% had a neutral affirmation and just as much negative affirmation). Also, out of a total of 90 analyzed texts, the subcategory global fight against the pandemic has the highest percentage of positive affirmation, while the subcategory of non-state actors has the highest percentage of neutral affirmation. Finally, the subcategory of corona virus has the highest percentage of negative affirmation.

Figure 2. **Support for national governments after the publication of news about mass chipping of the world's population.**



The chart shows that most of the texts, i.e. the internet posts referring to the category of placing an electronic chip to each individual to control the brain have a negative affirmation. Primarily it is due to the fact that the authors of the texts in the group are people who have already been members of similar social groups that deal with the topic of world conspiracies even before the period of the pandemic. Their texts always talk about globalization and its negative side effects. In addition, in the period between the end of February and the first half of April about 14,000 new members joined these groups. The topic of the posts strongly influenced the opinion of the people. Hence, it diminished the support to the national governments, thus they are considered to be an instrument, i.e. part of the conspiracy theory.

The term media has a positive affirmation again because it is the only source

of news about what is happening in the external world due to the imposed quarantine (out of a total of 17 texts, 9 texts or 52.9% had an affirmative character, 3 texts or 17.6% had a neutral affirmation and 5 text or 29.4% had a negative affirmation). The term EU has the highest neutral affirmation and this is due to the lack of sufficient information about the role of the Union for such and similar crises (out of a total of 22 texts, 19 texts or 86.3% had a neutral affirmation, and only 1 text or 7% had positive or negative affirmation). The terms electronic chip and government pandemic control have had the highest value of negative affirmation (out of 25 texts, 19 texts or 76% had negative affirmation, 4 texts or 16% had neutral affirmation and 2 texts or 8% had positive affirmation). Finally, the term China as a variable for humanitarian aid in material means and human resources without taking sides for mandatory vaccination had the highest neutral affirmation (out of a total of 14 texts, 8 texts or 57% had a neutral affirmation, 4 texts or 28.5% had a positive affirmation and 2 text or 14.2% had a negative affirmation).

Table 1. **Affirmation of mass vaccination category**

Subcategory	total	+	0 (neutral)	-
Total	24 (100%)	4 (16.66%)	3 (12.5%)	17 (70.83%)
Celebrities	7 (29.16%)	2 (8.33%)	1 (4.16%)	4 (16.66%)
Non-state actors	7 (29.16%)	1 (4.16%)	1 (4.16%)	5 (20.83%)
World Bank	3 (12.5%)	0	0	3 (12.5%)
NGO	4 (16.66%)	1 (4.16%)	1 (4.16%)	2 (8.33%)
WHO	3 (12.5%)	0	0	3 (12.5%)

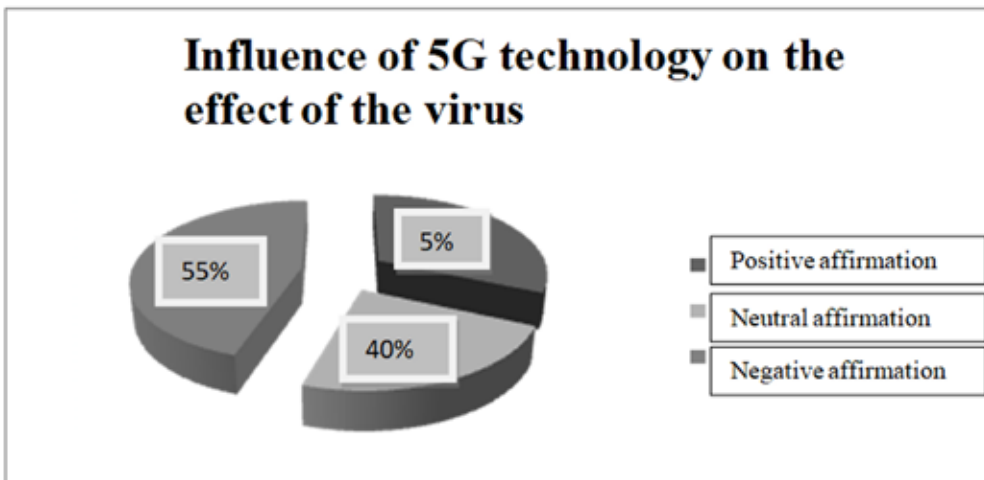
The category of mass vaccination was covered in texts relating to the power of the large pharmaceutical companies that provide support by national media and other actors that disseminate false information about the danger of the virus. The table lists subcategories that influenced the creation of public opinion. However, in the texts published on Facebook, the groups were interpreted with some affirmation, thus creating public opinion among group members (unless a post becomes viral in another group about which the authors of the survey do not have data availability).

Analogous to the above-stated, it can be concluded that in the category of mass vaccination, there is a higher percentage of negative affirmation with a tendency to increase due to the possibility of increasing restrictions given by the WHO to national governments for preventing further spread of the virus (out of a total of 24 texts or posts in the groups, only 4 or 16.66% had a positive affirmative character which would create a positive image in the audience. 3 texts or 12.5% had a neutral affirmation, and 17 texts or 70, 83% had a negative affirmation), which clearly shows that the public does not trust mass vaccination.

Table 2. Affirmation of the category influence of the 5G technology

Subcategory	total	+	0 (neutral)	-
Total	20 (100%)	1 (5%)	8 (40%)	11 (55%)
Death of bees	8 (40%)	0	2 (10%)	6 (30%)
Mind control	2 (10%)	0	2 (10%)	0
Influence of the 5G over climate changes	10 (50%)	1 (5%)	4 (20%)	5 (25%)

Figure 4. Affirmation of the category of influence of 5G technology on the effect of the virus



representation in order to more easily compare the numerous statistical elements.

5G is one of the most frequently mentioned categories in the texts that are analyzed within the Facebook group “5G”. As a category, it was most often mentioned in the first week of April, when one of the biggest scandals in the history of wireless telecommunications, which referred to the mysterious death of bees, was announced. An overview of its subcategories shows that 5G is most often mentioned in texts dedicated to the physical and mental health of people, but also the environment in general. According to the above-mentioned, we can conclude that in the beginning of April, the percentage of neutral texts on 5G was higher, while in the second half of the same month there was a dominance of the number of texts with negative affirmation. This indicates that citizens do not agree with placing 5G antennas near them. The negative attitude towards the alleged impact of 5G on the spread of the virus, as well as the ban on some Western European countries in the world to introduce 5G in their countries, was also very pronounced.

Creating such an opinion for these three categories (especially for the category

of the influence of 5G technology on the effect of the virus) resulted in mass protests in several cities across Europe. Some of the protests were peaceful, while some ended with arson at mobile operators' base stations.

### **Conclusion**

Humanitarian diplomacy with the help of (non) state actors, creates and deigns various political and socio-economic or security situations.

Non-state actors have a great influence in all fields and can be a tool of humanitarian diplomacy. The role of the soft power as an instrument of humanitarian diplomacy is in the power to initiate or catalyze essential political processes that (will) have an overall impact on the overall situation. Viewed through the social prism, humanitarian diplomacy will aim for a long time to create a model of international solidarity and redefine the needs of certain world goods as well as homogenize economic ideology and create universal religious, philosophical and civic values.

Citizens have demanded accountability from their governments and international condemnation of European non-solidarity, which has sparked a new political tsunami on the European political scene. In a situation of a humane or solidarity vacuum, China's soft power has won the sympathy of countries most affected by the virus, especially those who choose their governments. China has been using soft power to define the European Union's already embroiled crisis, and has imposed the need to redefine the fundamental individual and collective values on which the Union has so far rested. Also, the emergence of fake news in a crisis situation has initiated civic activism to be transferred from the Internet to the streets. Hence, thanks to social networks, the ability of small actors to influence a large audience will increase in the future. Consequently, big actors will have reduced power to create public opinion.

### **REFERENCES:**

- Archer Clive. *International Organizations*. 3 rd ed. London, 2001.
- Ambrosius Llyod E. *Woodrow Wilson and the American Diplomatic Tradition: The Treaty Fight in Perspective*. Cambridge University Press, 1990.
- Drew Thompson. *China soft power in Africa: from the "Beijing Consensus" to health diplomacy*. s.n.2005
- Elliot Harris, *The "Un-American" weapon: Psychological warfare* (New York: M.W. Lads Publishing, 1967).
- Gagea Andreea. *Diplomacy in the Games of Power. Diplomacy of Power – Power of Diplomacy*. Bucharest Academy of Economic Studies. 2011.
- Gallarotti, Giulio M., "Soft Power: What it is, Why it's Important, and the Conditions Under Which it Can Be Effectively Used" (2011). Division II Faculty Publications. Paper 57.
- Glen Fisher. *Public Diplomacy and the Behavioral Sciences* (Bloomington, IN: Indiana University Press, 1972).
- Glen Fisher. *American communication in a global society*. Ablex Publishing Corporation, 1987.

- Halliday F. "The Romance of Non-State Actors," In: D. Josselin and Wallace, Eds., *Non State Actors in World Politics*, Palgrave, London, 2000.
- Ham van Peter. *European Integration and the Postmodern Condition: Governance, Democracy, Identity*. Routledge, Milton Park Oxon, 2001.
- Hun Yun Seong. "Toward Public Relations Theory-Based Study of Public Diplomacy: Testing the Applicability of the Excellence Study," *Journal of Public Relations Research* 18, no. 4, (2006).
- J. A. Scholte, "Globalisation and Collective Identities," In: J. Krause and N. Renwick, Eds., *Identities in International Relations*, St. Martin's Press, New York, 1996.
- James Dewar A. "The Information Age and the Printing Press: Looking Backward to See Ahead," *RAND Paper No. 8014*, 1998.
- James P. Muldoon. *Multilateral Diplomacy and the United Nations Today*. West view Press 2en. ed. 2005.
- Joe Johnson, "How Does Public Diplomacy Measure Up?" *Foreign Service Journal* 83, no. 10, 2006.
- Katzenstein Peter J. and Robert O. Keohane, "Anti-Americanisms," *Policy Review* (October/November 2006),
- Kennedy Paul, *The Rise and Fall of the Great Powers* (New York: Random House), 1987.
- Kissinger Henry. *Diplomacy*. Simon & Schuster, 2011.
- Mustonen J. *Case Study: Hard Power or Soft Power? Searching for China use of Soft Power in the pursuit of the economic cooperation framework agreement with Taiwan*, 2010.
- Nye Joseph, *Soft Power: The Means to Success in World Politics*, 1st ed. (New York: Public Affairs, 2004).
- Nye Joseph., *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990); and J. Nye, *Soft Power: The Means to Success in World Politics* (New York: Perseus, 2004).
- Po-chi Chen. *Cyber Public Diplomacy as China's Smart Power Strategy in an Information Age: Case Study of Anti-Carrefour Incident in 2008*.
- Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs*, January/February, 2011.
- Vuving Alexander L. *How Soft Power works? A American Political Science Association annual meeting*, Toronto, September 3, 2009.
- Zengotita de Thomas. *How The Media Shapes Your World And The Way You Live In It*. Bloomsbury, 2005.



## CODE OF ETHICS

**CONTEMPORARY MACEDONIAN DEFENCE** is an international scientific journal published by the Ministry of Defence of the Republic of North Macedonia. The journal publishes scientific and professional articles by domestic and foreign authors that address topics in the field of defence, security and peace.

The Editorial Board of the journal is guided by the highest professional and ethical standards, which means that plagiarism and other unacceptable forms of work in the academic community and in publishing are not tolerated.

All scientific articles published in the international scientific journal “Contemporary Macedonian Defence” are reviewed by relevant reviewers in the appropriate field of scientific research and are classified by the reviewers in several categories (original scientific article, scientific article and professional paper). Manuscripts are submitted to the reviewers in an anonymous form.

This Code of Ethics requires the authors of articles to use the sources correctly in the published articles, which means that they will fully list the sources and authors they have cited in their article. Ethics in the publishing of the articles implies that attention will be paid to hate speech and advocacy of discriminatory attitudes of any kind and on any basis, as well as to declaring any conflicts of interest.

All articles in which the authors do not adhere to this Code of Ethics will not be considered for publication in our scientific journal, which is decided at a meeting of the Editorial Board of the journal.

The authors are responsible for complying with the ethical and professional standards and must obtain approval from the authors for the transmission of portions of their texts or authorized video or other material if the author or the publisher so requests.

The International Scientific Journal “Contemporary Macedonian Defence” does not receive or publish articles that have already been published in another journal, or those in which there is a high degree of resemblance to an already published article of the particular author.

The citation in the articles must be consistent and in accordance with the rules set out in the Guidelines for Authors. At the end of the article there must be a section with reference literature in alphabetical order, listing the complete references.

The author should give due recognition to all those who contributed to the research. Those who have competently contributed to the research should be listed as co-authors. The first author, by submitting the manuscript, guarantees that all co-authors agree with the final version of the article and its final publication.

If the article is a research conducted on people (surveys, interviews, etc.), the

author is obliged to provide information that the entire research process is conducted with consistent compliance with ethical standards to protect the safety, integrity and dignity of the research participants.

The reviewers are required to treat the manuscript in a confidential manner. The manuscript should not be disclosed or its contents discussed with anyone other than the editor or persons authorized by the editor. The reviewer is required to provide a brief explanation to the Editorial Board of his/her final decision regarding the manuscript, especially if the print decision is negative.

The reviewer is obliged to approach the review objectively. The feedback to the author (s) should be given as professionally as possible, without any personal attacks. The reviewer may not use for his / her own research any part of any data submitted to him / her in articles that are still not published. The reviewer is obliged to immediately inform the editor of any similarities between the manuscript under review and another paper, whether it has been published or is being reviewed by another journal. The reviewer must immediately notify the editor of a manuscript that contains plagiarism, falsified data, or views that constitute hate speech or reflect bias. In addition, the reviewer is obliged to make an objective assessment of whether he/she has sufficient competencies to review the submitted manuscript. If the assessment is negative, he/she returns the manuscript to the editor / Editorial Board in the shortest possible term.

The editor should ensure that the submitted manuscripts are anonymous and should not disclose the names and other details of the reviewers to third parties without their permission.

The editor has the right to make the final decision on the acceptance or rejection of the manuscript, regarding the originality and clarity of the manuscript and its relevance to the journal. Under no circumstances should the editor engage in obliging the authors to cite the particular journal as a condition for accepting the manuscripts for publication.

The editor is responsible for timely review and should take reasonable steps if the author files a complaint with respect to the work of the reviewers.



**„SOVREMENA MAKEDONSKA ODBRANA“  
INTERNATIONAL SCIENTIFIC JOURNAL**

**INSTRUCTIONS FOR AUTHORS**

**International scientific journal "CONTEMPORARY MACEDONIAN DEFENCE"** is a theoretical journal published by the Ministry of Defence of the Republic of North Macedonia. The magazine comes out regularly twice a year and once a year there is a special issue on a particular topic. The magazine publishes original scientific papers, reviews of books in the field of defence, security and peace, on a national, regional and global level.

**The magazine publishes only reviewed and specialized papers: original research papers, accompanying research papers and professional papers and book displays.**

If the Magazine accepts the paper the authors are not allowed to publish it in other journals.

Papers must not have more than one co-author.

The manuscript should be submitted in electronic form. The pages and appendices should be numbered.

Papers should be written in English, where the paper should have a title, abstract and keywords.

The paper which are not to be printed are returned to the authors with an explanation.

**TECHNICAL SPECIFICATIONS OF THE PAPER**

**The paper should include:** title, author, institution, abstract, keywords, introduction, main part, conclusion and reference. The full paper should not exceed 5000 words in English.

**Title of the paper** - 14 points, Times New Roman, centered. Title of the paper should be short, but give a true reflection of the content and preferably contain as many keywords from the subject matter covered as possible.

One blank line.

**Authors** name and surname, lower case (Bold), 11 points, Times New Roman, centered.

Two empty rows.

**Institution** – cursive (Italic), 11 points, Times New Roman, centered.

Two empty rows.

**Abstract** - 11 points, Times New Roman, single-spaced. The content of the abstract should be an essential and independent entity.

One blank line.

**Keywords** - maximum 5 words, 11 points, Times New Roman, single spaced.

**Introduction** - 11 points, Times New Roman, single-spaced. One blank line.

**Main Part** -11 points, Times New Roman, single-spaced.

One blank line.

**Conclusion** - 11 points, Times New Roman, single-spaced. The conclusion should be a brief summary of the paper, and to include research results that occurred.

One blank line.

**Reference** - 11 points, Times New Roman, cited according to the Harvard style of citation. The cited reference should be given in a separate chapter in the order in which they appear as footnotes in the text. Cite only the bibliographical data used in the text. Cite all types of sources of information - books, specialized magazines, websites, computer software, printed or e-mail correspondence, and even verbal conversation.

Papers that use tables, pictures, drawings, photographs, illustrations, graphs and schemes, should be numbered with Arabic numerals, and the title of the picture should be written underneath. Each image or group of images should be planned in a well structured manner. The images should be sent as separate a JPG file with a minimum resolution of 300 dpi. Colour images are printed as black and white.

Format: A4-format, delivered in an electronic form.

Margins

TOP	5 cm	TOP	1.89”
BOTTOM	5 cm or Page Setup	BOTTOM	1.89”
LEFT	4 cm (inch)	LEFT	1.58”
RIGHT	4 cm	RIGHT	1.58”
		GUTTER	0”

The Editorial Board is obliged to submit the papers to the competent reviewers. The reviewers and authors remain anonymous. The reviewed papers, together with any observations and opinions of the Editorial Board will be submitted to the authors. They are obliged, within 15 days, to make the necessary corrections.

The time of publishing the paper, among other things, depends on following this guideline.

Deadlines for submission of papers - 30.03. and 31.10. in the current year

ADDRESS:

1. Prof.Dr. Marina Mitrevska –Editor in Chief  
e-mail: marinamitrevska@yahoo.com

or

2. Ass.Prof. Zhanet Ristoska  
e-mail: zanet.ristovska @ morm.gov.mk  
zanet.ristoska@yahoo.com

or

sovremena@morm.gov.mk

*Skopje, 12.04.2018*

***MAGAZINE EDITORIAL BOARD***  
***"Contemporary Macedonian Defence"***



The magazine is published twice a year

[www.morm.gov.mk/contemporary-macedonian-defence/](http://www.morm.gov.mk/contemporary-macedonian-defence/)

СОВРЕМЕНА КОНТЕМПОРАРИ  
МАКЕДОНСКА МАЦЕДОНΙΑН  
ОДБРАНА ДЕФЕНС  
39

CHRISTOPHE CHICLET  
TONI MILESKI, EIKE ALBRECHT  
ARMIN KRŽALIĆ  
IVAN JOVETIC  
IGOR GJORESKI  
KARLO PALJUG, ROBERT MIKAC  
GJORGJI VELJOVSKI  
BOJAN MIKLOSH, LAZAR DJUROV  
LIDIJA KOS-STANIŠIĆ, ANTE ŠUNJIĆ  
NATAŠA MILETIĆ  
IGOR GELEV, BILJANA POPOVSKA

СОВРЕМЕНА МАКЕДОНСКА ОДБРАНА