Is the Ethiopian Federalism in Trouble?

Takele Bayu BEKELE[1]

Ethiopia is a country of a cultural and linguistic mosaic. Paradoxically, the political and bureaucratic system of the country has failed to accommodate the ethno-linguistic and religious diversity of the society. The Ethiopian monarchical system and the military dictatorial government have had pursued a policy of national unity and territorial integrity of the state often at the expense of ethno-linguistic and religious diversity. In effect, the different ethnic and religious groups had suffered from domination and injustice. This has led to the birth of ethno-nationalist movements taking arms against the strong central government demanding self-administration. In 1991 the ethno-nationalist forces led by the Tigray People's Liberation Front (TPLF) have won the battle against the military government which led to the establishment of the Federal Democratic Republic of Ethiopia. However, since its inception, there has been a widespread disagreement among Ethiopian political groups, scholars and even the public at large about the origin, structure and function of the federal system and its constitution. This particular paper aims at critically analysing the risks associated with the Ethiopian federal system in light of Ronald Watts's six principles of federalism: disposition to democratic procedures; non-centralization as a principle; checks and balances to limit the concentration of political power; open political bargaining for making collective decisions; genuine group power-sharing within central institutions, often consociational and respect for constitutionalism and the rule of law while using literature and document analysis as data collection procedure and research methodology. In effect, secondary data sources have been reviewed including various types of relevant books, journal articles, government and non-governmental reports, government implementation plans and progress reports and lastly they have been carefully scrutinized and analysed to secure their reliability, suitability and adequacy. Finally, even though the aforementioned principles are embedded in the Constitution, the paper has found out that the government has practically failed to implement them. Consequently, the federal system in Ethiopia is mainly regulated by the policies of the ruling party rather than by the merits of the Constitution. In effect, the country is facing a multifaceted crisis and the federal system and its constitution are under imminent threats. In the end, the paper recommends that under the present scenario, the situation necessitates the government to carry out a deep structural and system reform focusing on the political and economic imbalances that are observable in the coalition ruling party and among the different ethnic groups in the country. Furthermore, since there is a widespread

[1] Ph.D. student, National University of Public Service, Faculty of Science of Public Governance and Administration; e-mail: takeb21983@gmail.com

disagreement about the origin and development of the federal system and its constitution among different groups in and outside the country, holding a national reconciliation and political referendum on the federal system and its constitution is fundamental to fix ethnic driven conflicts and political instability in the country.

Keywords: *consociation, democracy, political bargaining, constitutionalism, non-centralization*

Introduction

Ethiopia is a diverse nation with more than 80 ethnic groups. No single ethnic community in Ethiopia constitutes more than 50% of the country's population. However, the Oromo, Amhara, Somali and Tigre are the major ethnic groups with significant proportions, according to the 2007 census 34.5%, 26.9%, 6.2% and 6.1% respectively. [1] There are also diverse religions coexisting in the country including Orthodox Christianity, Islam, Protestant and Catholic denominations and other indigenous religions. That is why, in 1928, the famous Italian scholar, Carlo Conti Rossini, described the Ethiopian Empire in his book *Historia di Ethiopia* as "un museo di popoli" or a "museum of peoples", signifying the linguistic and religious diversity of the country. [2]

Paradoxically, the then political and administrational system of the country had been arranged against the existence of such diversity. Modern Ethiopia which had emerged in the second half of the 19th century with the coming into power of Emperor Tewodros II (1855–1868) and finalized by Emperor Menelik II (1889–1913) and further strengthened by Emperor Haile Selassie's (1930–1974) had failed to accommodate its ethnic, linguistic and cultural diversity in its socio-economic and political system of administration. [3] Menelik II, embarked on an aggressive, at times brutal, westward and southward expansion, subjugating and incorporating Oromo, Sidama, Gurage, Wolayta and other groups. [4] In the name of the Emperor, *Neftegna* (Amharic for riflemen) settled the lands (in Amharic *gebbar*) and levied tribute from farmers in the newly conquered territories. They tried to impose Amharic and the Christian Orthodoxy they considered superior to local non-Christian and pagan traditions. [4] Indeed, spearheaded by Menelik II, the Ethiopian state accomplished the momentous achievement of doubling its size by expanding into what is now the southern part of Ethiopia. During the imperial era, the belief of "one language, one religion, history, custom, administration (centrist), flag" have led to the loss of the cultural identity of the nation, nationalities and people of Ethiopia. Similarly, during the military socialist government (*Derg* regime), there was not any substantial change on the policy. Continuing with the imperial era policy of "denying ethnic (cultural) identity", it butchered those who raised ethnic and identity related demands. [3]

The administration system prior to 1991 had not given due recognition to the existential problem of the country, the multi ethnic and linguistic nature of the nation. [5] The consequence of ignoring or suppressing ethnicity in the country led to the birth of militant ethnic nationalism, such as the Tigray People's Liberation Front (TPLF), the Eritrean People's Liberation Front (EPLF), the Ogaden National Liberation Front (ONLF) and the Oromo Liberation Front (OLF) just to mention the dominant ones, with the doctrine of the right to self-determination to promote their respective ethno-regional demands. [6] [7] At the centre of their struggle

there is a claim for the recognition of their language and culture and an attempt to redefine the identity of the state. [8] This aggravated the conflict between the central government (military regime) and ethno-nationalist movements and led the country to an all-out civil war. The war continued for almost two decades and led to the victory of the national liberation movements led by the TPLF dominated Ethiopian People's Revolutionary Democratic Front (EPRDF) over the military regime in 1991.

Hence, the crucial task of the new government was to design an institution that better recognizes and accommodates the country's ethno-linguistic and cultural diversity. This led to the establishment of a transitional government and the development of a new constitution in 1994–1995. The constitution redefined the country along ethnic lines with the creation of nine ethnic-based regional states and two federally administered city-states and named the country *Federal Democratic Republic of Ethiopia.* [9] In this regard, the intent of the 1995 Constitution was to create a more prosperous, just and representative state for its entire population. Relative to the past administration, the system was able to score success in the political, economic and socio-cultural area. The economic growth achieved by the government is particularly remarkable even by international standards. Ethiopia showed a track record of sustained rapid growth and poverty reduction and labelled among the top ten fastest growing economies in the world as revealed in international reports. [10] [11]

Yet, despite continued economic growth and promised democratization, many observers claimed that there was a growing discontent with the EPRDF's ethnically defined state and rigid grip on power and fears of continued interethnic conflict. At the government level, the document released after the National Security Council meeting, held on 10 October 2017 reveals that Ethiopia is currently confronting an alarming level of multi-front crisis which has led the government to admit that the federal system and its constitution is under imminent threats. [12] Freedom in the World 2017 reported that Ethiopia was wracked by protests throughout much of 2016 and 2017, a result of widespread and growing discontent with ethnic and political marginalization and repressive rule by the EPRDF. Had the ethnic driven conflict and the political instability continued, it would have put at risk the entire nation. The country started to feel the effects of instability in the form of revenue reduction from the tourism sector, reduction in the flow of foreign direct investment, lawlessness, lack of peace and security and the depletion of the foreign currency reserve. [12] In general, the political, economic and socio-cultural situation of the state and its people is currently at grave risk and above all, the future looks worst unless properly managed.

Therefore, addressing the roots of this crisis requires an objective assessment of the systemic risk that involves the political economic imbalance and injustice through an investigative approach to the system. This enables the system to design and implement a sound mitigation policy response to properly manage the risks and crisis associated with the wrong implementation of the federal system and its constitution. In this regard, the mere adoption of federal or similar arrangements does not signify an effective accommodation of ethnic diversity and the creation of an inclusive society. The success of subnational autonomy arrangements in addressing ethnic divisions is not guaranteed. Success depends, among other things, on the genuine nature of the federal design and its proper implementation in the Ethiopian context.

The Fault Line of the Ethiopian Federalism

After ousting Mengistu Haile Mariam's dictatorship in 1991, the EPRDF led by Prime Minister Meles Zenawi, embarked on a project to radically transform the country's political system. The regime not only restructured the state into the current Federal Democratic Republic of Ethiopia, but also vigorously redefined citizenship, politics and identity on ethnic grounds. [13] But here the question is why has the country adopted ethnic federalism? What if the government adopts a devolutionary structure rather than ethnic federalism? Why other sound mechanisms and institutional arrangements had not been chosen to better accommodate ethnic diversity? The lesson from the African experience, including the then political administration in Ethiopia, is that when a state fails to readily acknowledge and accommodate its ethnic diversity, federalism or other such arrangements lead to increased tensions among ethnic groups. In this regard, Osaghae argues that federalism is necessary for Africa to manage the problems emanating from diversity such as inequitable social and political relations, and unequal development of groups. [14] Erato Kozakou-Marcoullper argues that federalism, by allowing power to be at once divided and coordinated, enables respect for different identities, accommodation, multicultural co-existence, tolerance and cooperation to take place and acts in a positive way for keeping a country together rather than divided. [15] Federal arrangements can accommodate ethnic communities' aspirations by preserving their culture, language and religion, through an autonomous administration of a territorial space. [15] Hence, the fundamental reason behind the adoption of federalism in Ethiopia after 1991 lies in its potential for accommodating ethnic diversity and fostering the values embedded in ethnic community. [16] [17] [7]

Keeping this in view, the 1994–1995 Constitution was designed to contain the existential problem of the country, accommodating the ethno-linguistic diversity of the nation which was for long ignored. Ethnic federalism as an institutional design not only devolves power but at the heart recognizes, respects, defends and promotes the very nature of human existence with its unique identity/character which is, I strongly believe, a necessary condition for a state in a multi-cultural environment to survive from designation. Indeed, in Ethiopia, the remake over the past two decades has been accompanied by tremendous hopes for a more prosperous and peaceful future, after decades of poverty, hunger and oppression. It is true that the federal system and its constitution have established peace and security which for long has been lost in the country. Nations, nationalities and people are able to administer themselves and able to promote their own unique socio-cultural values which they never imagined it could happen in the previous administration.

However, despite rapid economic growth and poverty reduction as well as celebration of diversity, many observers claimed that post 1991 was characterized by major and minor ethnic conflicts in many parts of the country including the capital, Addis Ababa which was dominantly due to political, economic and border problems.

The World Bank report on violent conflicts in Sub-Saharan Africa 1991–2008, which was prepared by Benjamin Petrini revealed that numerous non-state conflicts between various ethnic groups in different times claimed the life of many civilians, this includes Afar and Issa in 2002 which led to the deaths of 75 people, Anuak and Dinka in 2002 where 35 deaths were reported, Dizi and Surma in 2002 in which 35 were dead, Ogaden and Sheikhal in 2002 which claimed 435 lives, Afar and Kereyou in the year 2002–2003 claiming 69 lives, and the Anuak

and Nuer (Ethiopia) in 2002–2003 left 89 people dead. [18] Amnesty International further reported instances of ethnic violence including ethnic clashes in Gambella in 2003 which led to the death of 65 people, 61 Anuak people and four members of highland ethnic groups and 75 wounded, in addition to this, nearly 500 houses were burned down and plundered. [19] In June 2006 conflicts between Guji and Borena communities in the wake of changes to administrative boundaries in Oromiya and Somali regional states claimed at least 100 lives and displaced at least 35,000 people. [19] Numerous reports also indicated the presence of waves of conflict between the government and protesters in which the government and its agents committed arbitrary and unlawful killings. Trudeau, citing International NGO, Amnesty International claimed that more than 800 persons were killed starting from November 2015. [20] In August 2016, BBC News reported that "Nearly 100 killed" in Oromia and Amhara regional states. [21] Hence, in spite of the rationality of the federal administration in managing the complex ethno-linguistic diversity of the country and reducing conflicts, ethnic competition and conflicts are still critical challenges in the country. [22]

Therefore, for the last two decades, EPRDF has failed to end both the ethnic identity driven conflict and the armed struggle of ethnic based nationalist movements. [23] [5] Hagmann and Abbink argue that political polarization and ethnic competition have been prevalent for the last two decades, in the period of ethnic federalism. [24] Adegehe further adds that ethnic federalism failed to solve ethnic conflicts, still common in regional border areas, resettlement sites and universities, composed of different ethnic groups. [25] Above all, ethnic federalism failed to resolve the "national question". [13] The EPRDF's ethnic policy empowered some groups but it did not lead to dialogue and reconciliation. For Amhara national elites, ethnic federalism impedes a strong, unitary nation state, furthermore for ethno-national rebel groups like the Ogaden National Liberation Front (ONLF; Somalis in the Ogaden) and Oromo Liberation Front (OLF), ethnic federalism remains artificial. [13]

The fundamental concern and issue here is how to address those conflicts which are arising in the society for different reasons in a sustainable manner. Indeed, conflict among groups and in effect political instability is common in every society, particularly in countries like Ethiopia where people are different considering their ethnic, cultural and religious background. This requires genuine institutional arrangement, political leadership and commitment and above all community participation. Hence, the fundamental question here is why the EPRDF government's dream of managing ethnic identity driven conflicts and political instability and the creation of an inclusive society is fading and challenged by unprecedented factors? How federalism along ethno-nationalist lines in countries like Spain, Switzerland and Belgium are relatively successful? Thus, it is of paramount importance to critically analyse the fault line of the Ethiopian ethnic federal arrangement and the failure of the system to deliver much of what is expected of it.

Therefore, this particular paper critically analyses the issue of federalism, particularly pertaining to the question—is the Ethiopian ethnic federalism in trouble?—while scrutinizing the whole process of state–government structuring, adoption and implementation of the democratic federalism project and its constitutional values, norms and principles in light of the framework developed by Ronald Watts. Watts presented a list of the significant political processes and practices on which the effectiveness of different federations depended: [26]

- disposition to democratic procedures;
- non-centralization as a principle;

- checks and balances to limit the concentration of political power;
- open political bargaining for making collective decisions;
- genuine group power-sharing within central institutions, often consociational;
- respect for constitutionalism and the rule of law.

Disposition to Democratic Procedures

In fact, the manner in which the current Ethiopian constitution was crafted and consequently the federal structure was established raises many more prominent governance questions; among others the question of disposition to democratic procedures is fundamental. [27] [13] [6] Though the government defends that the process has been democratic and open to the public and political parties of the time, many have criticized the procedure and development of the federal structure and its constitution. Many observers have claimed that since the TPLF has held the upper hand over other ethnic based nationalist parties, it has rigged and dominated the development process of the federal system and its constitution. For instance, the National Conference on Peace and Reconciliation, which was organized in July 1991—as the foundation for a transitional period after the regime change, excluded many of the political groups from participation. [28] The conference largely included selected individuals and over 20 political organizations handpicked by TPLF/EPRDF. [27] [29] Further, multinational organizations or other ethnic-based organizations that might pose a threat to the new status quo were systematically excluded from the process. In civic and political terms, the remnants of the student movement, the Ethiopian Revolutionary Democratic Party (EPRP) and the All Ethiopian Socialist Movement (Meison) were not invited to attend the conference. [2]

The International Crisis Group also stated that the military superiority of the TPLF and the control that they imposed during the transitional period made the opposition unable, both physically and politically, to reject the so-called federal bargain. [13] Consequently, the EPRDF quickly institutionalized the TPLF's policy of people's rights to self-determination and self-rule. [13] Hence, the introduction of self-determination for the nationalities was done without a genuine consultation of the wider sections of the Ethiopian people, and there was little of a "federal bargain", which according to the federal theory is an essential part of a sustainable federal system. [13] Further, the group argued that although the transitional conference that was held just after the EPRDF came to power in 1991 included a wide spectrum of political parties, their views were hardly taken into consideration and the EPRDF's agenda for the transitional period was adopted largely unmodified. [13] In effect, from the outset, the TPLF through the EPRDF coalition was not able to demonstrate a genuine will to share power with other political forces in a democratic manner. [13] It is possible to infer from this that the TPLF was the creator of the coalition (EPRDF) and the architect of the ethnic federal model and its constitution.

Even though the constitution was applauded for its commitment to liberal democracy and respect for political freedoms and human rights, practically, the government failed to establish democratic values, norms and principles. According to the International Crisis Group "the government has encroached on social expression and curbed journalists, non-governmental organizations and religious freedoms. The closure of political space has removed

any legitimate means for people and political parties to channel their grievances." [13] This produced tensions between the government and the opposition, and led to communal and inter-ethnic animosities and armed conflict between ethno-national rebels and the government. [13] Hence, "the shrinking nature of the political land scape due to the lack of disposition to democratic procedures is responsible for the revival of armed secessionists", movements such as the Ogaden National Liberation Front and the Oromo Liberation Front. Moreover, with the failure of ethnic federalism in developing a peaceful inclusive political atmosphere, many other new opposition political parties took arms against the government such as the Ginbot 7 Movement for Justice, Freedom and Democracy (G7), the Amhara Democratic Forces Movement (ADFM). [13] [25] In effect, the EPRDF firmly monopolizes political representation, decision-making and public space. [13]

However, in a multi ethnic state like Ethiopia, democracy is not only an instrument of government but most importantly ought to be the way of life of its citizenry, due to the values, norms and principles like tolerance towards diversity, the rule of law, accountability, transparency, etc. which are embedded in the system. Building a resilient state essentially depends on the degree of its exposure to democratic values, norms and principles as well as their actual implementation. Therefore, I firmly believe that the process that leads to the launching of a federal experiment is crucial in the success of a federation. In this regard, from the inception period till now the way how the federal system and its constitution have been crafted and implemented need a deep analysis from the perspectives of its disposition to democratic procedures so as to build a holistic system in which no one assumes alienation. This requires the good will of all parties, legally registered political parties, armed nationalist movement groups, and political parties established abroad, particularly the government in power, and other stakeholders to create an open and democratic dialogue for the good of the nation and its people. To the extreme, the EPRDF Government ought to show its political will to carry out a referendum on the ethnic federal system and its constitution if that is needed to end ethnic identity driven conflict and political instability so as to realize the creation of an inclusive society.

Administrative and Political Non-Centralization

In principle federalism is the method of decentralizing powers so that the federal and regional governments are each, within a sphere, co-ordinate and independent. Ethiopia's decentralization policy, elaborated in the 1991 transitional charter and the 1995 Constitution, was created by the current ruling party (EPRDF) to devolve fiscal, political and administrative power to the ethnically organized regional governments. Unlike previous heavily centralized Ethiopian regimes, the EPRDF introduced an ethnically based decentralized federal arrangement, and officially allowed different political parties to compete and participate at both central and regional government levels. Accordingly, the FDRE Constitution, Article 51 and 52 allocated different power and responsibilities to the federal and regional governments separately, as well as concurrently to avoid political and administrative excessive centralization. [9] Nonetheless, the EPRDF controls all the regional state governments in the Ethiopian federation, either directly through its member parties or indirectly through affiliate parties. The relationship between the central

and regional parties is like a relationship between patron and clients. [30] All important political decisions must be taken at the centre or be in line with central policies. Both supporters and opponents of ethnic federalism recognize that centralized party rule and federal interventions in the regions undermine local self-government. [13] Keller also claims that policies and implementation strategies are highly centralized where regional states replicate policies from the centre. [31] Assefa argues that regional governments are neither autonomous nor accountable to their constituencies and further the centre does not allow them to articulate and address regional interests; rather, they are required to implement central directives. [32] In this regard, the adoption of a top-down decision making process is against the very principle of federalism, shared rule and self-rule.

However, some attribute the lack of genuine decentralization in the country to the government's concern that allowing the regions to become too autonomous would encourage some regions to secede, taking advantage of the constitutional provisions like the Somali and Oromia regions. In effect, advocates of state-centred or regulated or democratically centralized federalism argue that the state-centralized form of federalism alleviates tensions of division because the structures are somewhat democratically interlocked. [33] The government also argues that the source of pursuing centralization is the incapacity of regional governments to make and implement decisions and policies by their own.

Whatever the reasons, failure to devolve political and administrative power undermined the federal arrangement and weakened the decision making capacity of regional governments. To the extreme, the fake implementation of the federal system and its constitution re-enforced ethnic based secessionist movements on the ground that the system promotes disproportionate concentration of power in the hands of the TPLF and fake decentralization. Finally, it is the responsibility of the federal government to capacitate and empower regional governments for better outcomes and thereby to overcome the risks associated with excessive centralization of power.

Checks and Balances to Limit the Concentration of Political Power

The 1994–1995 Constitution, Articles 51, 52, 55, 72 and 79 vividly established the kind of power relationship between and amongst the level and branches of government to ensure strong checks and balances in the system. [9] Further, the Ethiopian Federal Government is parliamentary in that it allows the legislature to exercise oversight and control over the executive. [9] However, in practice the power of the executive branch in the federal government surpasses the power of the legislature and similarly in the regional states the executive power exceeds the power of the state in the House of Peoples' Representatives. Hence, the checks and balances system among different state bodies, as well as the level of government is weak and much power is vested in the hands of executive bodies and in the federal government. [22]

In this regard, Semahagn Gashu attributes the lack of strong checks and balances in the system to the notion of democratic centralism—it is one of the major principles currently used to regulate the government structure and intergovernmental relations—which is responsible for undermining the separation of powers principle, the significance of official

channels of government and the accountability of the system. [6] Though there are legislative, executive and judicial bodies within the Ethiopian constitutional system, the separation of powers principle was undermined due to the party's principle of democratic centralism. [6] In effect, the Prime Minister has more power than what is common in parliamentary systems, the central executive's powers are largely unrestrained by the control of other institutions of the federation, such as the House of Peoples' Representatives and the House of Federation. This creates a good opportunity for the party in power to implement its policies and create legislation without the consultation of the regional governments, other political parties or the electorate at large. [27]

The International Crisis Group, while commenting on the political and economic institutional set up of the country, argued that in Ethiopia the role of ethnic federalism as a way to check and balance power is insignificant. Despite the federal government's multi-ethnic composition, TPLF officers occupy the highest levels of all ministries, the party's dominance is particularly evident in the armed forces and the National Intelligence and Security Office. [13] The organization further accuses the government that Ethiopia's political system and society have grown increasingly unstable largely because the TPLF has become increasingly repressive, while failing to implement the policy of ethnic federalism it devised over twenty years ago to accommodate the land's varied ethnic identities. [13] The result is obvious in that there is a greater political centralization, with concomitant ethnicization of grievances.

Therefore, it is imperative to enhance and empower democratic institutions in the country and promote the internal culture of democracy within the ruling party (EPRDF). Particularly, capacitating the judiciary and legislative branch of the government is fundamental to help them discharge what is good for the public as per the constitution of the country. This paves the way to hold the executive branch of government accountable and live up to its constitutional mandate. It is also of paramount importance to empower the capacity of regional governments to avoid the concentration of political and administrative power in the hands of the federal government and thereby to enhance the culture of checks and balances, as well as to promote the notion of "self and shared rule" between the two levels of government. In this regard, well-functioning and autonomous democratic institutions are required to facilitate checks and balances and accountability across different bodies including the executive bodies and also provide inclusive and contextual decisions that would serve as a venue for diversity management and reduce contradiction and conflict. [22] Above all, unless the government implements ethnic federalism as a way to check and balance political, economic and administrative power, ethnic grievances and political instability is in its next door. This urges the nation to ensure political and economic representation and justice for all, so as to ease the increasing ethnic tension and political crisis in contemporary Ethiopia.

Open Political Bargaining for Making Collective Decisions

The most serious shortcoming of the 1991 conference was its disregard of multinational organizations in general and pan-Ethiopian nationalism in particular. However, a crucial aspect of decentralist and balanced federalist ideologies is that the federal bargain should be based on a covenant, where the various political forces in the country voluntarily agree to

make arrangements for power-sharing and the devolution of power. In light of this principle of federalism, there are two major political forces that need be considered in the Ethiopian context, namely the pan-Ethiopian nationalism versus ethnic nationalism. [6] Disregarding this fundamental reality, the transitional charter was devoted solely to the "right of nationalities" and overlooked the pan-Ethiopian nationalism that had been in the process of crystallization in previous decades. [6] Due to such polarization, it has been challenging and will remain as a challenge to find a political solution to the divergent interests of the various groups and make the process inclusive for all the political groupings. However, open political bargaining paves the way to the need for intense negotiation on the issues and the willingness to make concessions among the stakeholders, so as to reconcile these two extreme political-economic perspectives in order to create a legitimate political system and constitution within such deeply divided societies. In effect, the institutionalization of the politics of accommodation and democratic bargaining would reduce ethnic antagonism and promote trust, dialogue, tolerance and recognition of differences, moderation and cooperation as critical engines of coexistence. [34]

Genuine Group Power-Sharing within Central Institutions, Often Consociational

It was argued that consociational democracy as understood in the way of promoting the political culture of accommodation can be an alternative mechanism to prevent potential sources of conflict such as unequal and arbitrary distribution of political and socio-economic opportunities. [35] Moreover, consociational power sharing is highly appropriate especially in those multi-ethnic regional states where the political decentralization does not coincide with ethnic boundaries. Such political culture of accommodation would improve trust and confidence across members of different ethnic groups and eventually discourage the fear of domination. [34]

In Ethiopia, however, despite the federal government's multi-ethnic composition, TPLF leaders have since the fall of Mengistu in 1991 had the most powerful positions in the country among others the security apparatus, top military positions, the aviation industry and major pillars of the economy. [36] Evidence from Freedom House found that the government tended to favour Tigrayan ethnic interests in economic and political matters and in effect the country's political and administration decision making is actually geared towards TPLF. [37] This presented a structural and system risk to the EPRDF Government and the peace, security and economic progress of the nation in general. Hence, the government should work hard in practice implementing a genuine power-sharing system in federal major institutions as depicted in the constitution. Thus, genuinely promoted and practiced consensus-based structures of political and economic governance could address the factors for diversity-based conflicts. [22]

Respect for Constitutionalism and the Rule of Law

The legitimacy of the origin of federal constitutions is particularly crucial. Indeed, since the formation of a federation is an agreement or contract that is freely and mutually entered into; the origin of federations should always be consensual. A federal system of government is a mutual consent among the various constituent parts or, as Trudeau notes, "federalism is by its very essence a compromise and a pact". [20]

In this regard, the fundamental step in the drafting process of a democratic constitution is that the drafting body must be comprised of all the political groupings that have a stake in the process. In the Ethiopian context, there are at least two competing interests without which any constitution-making process would not be successful. One is the sentiment towards the territorial integrity and unity of the country while many linguistic and cultural groups are concerned with cultural survival and equality. [6] Genuine and a real constitution-making process would not be successful unless these two political groupings are fairly represented in the constitution-making body. [6]

The constitution-making process and its subsequent institutionalization of the federal system in Ethiopia, however, was only designed by taking into account the interest and will of ethno-nationalist groups while ignoring the will and interest of others groups like pan-Ethiopianists. Hence, it is possible to conclude that the constitution-making process was largely dominated by TPLF/EPRDF and other ethno-regional political forces. [6] Consequently, in contemporary Ethiopia, it is common to observe that different political parties (both established in and outside the country), scholars and the public to some extent are indifferent towards the constitution as a governing document. This is particularly evident in the 2005 election top leaders from the Coalition for Unity and Democracy (CUD), a national political opposition party, publicly calling the document a constitution of beasts not of the free people. Indeed, the government itself is not faithful to its own constitution since it is common to observe government officials violating the terms and provisions of the constitution. The assessment made in 2017 by the government and the National Security Council revealed the continuous violation of laws by government officials and armed groups across the country and in effect violent conflict and lawlessness presenting an imminent threat to the rule of law and constitutionalism in the country. [12] These all are indicative of the lack of national consensus on the way the national constitution is made and implemented.

This calls for launching an inclusive constitution-making process which must be sought as the first step necessary to design an enduring constitution in a divided society like Ethiopia. This is because a constitution will be considered legitimate only if the vast majority of the polity's members identify themselves with it and view the document as their own. [38] Furthermore, the involvement of political groups in the constitution-making process not only determines the legitimacy of the process and the contents of the constitution, but it may also be a key factor in determining whether the country will undergo democratic transition and attain long-lasting stability. In addition to this, the involvement of various political groupings in the constitution-making process and its inclusiveness must be manifest through the participation of public and civic society groups. This entails the existence of a deep polarization that urgently needs to be resolved through intense negotiation on the document and the willingness to make concessions among the stakeholders and finally hold political

public referendum. In this regard, consensual legitimacy is necessary for a constitution to have real meaning and for the federal project to have a lasting legacy. [39]

Conclusion and Recommendation

After 1991, Ethiopia has entertained relative peace, security and economic progress under the centralized leadership of the TPLF dominated EPRDF. Despite this, there is still no widespread national consensus amongst the opposition political parties both in and outside the country, elites and at large in the Ethiopian society with regard to the notion and practical implementation of ethnic federalism and its constitution. The document presented at the EPRDF's National Security Council meeting reveals that people have lost confidence in the federal system and its constitution and in effect, the country is facing alarming multi-front crisis and imminent threats. The government accepted that the political leadership would take the prime responsibility for the mismanagement of the public resources and failure to act based on the rule of law. But such declaration should further need to be tested practically. Likewise, many scholars and political observers, both local and abroad, as well as ordinary citizens claim that the Ethiopian federalism is in trouble unless fundamental re-structuring is sought for. Indeed, nation building is not an easy task and cannot be achieved overnight. It requires building a sustainable system and structure which necessitates the democratic collective actions of all members of the state. Since its establishment, the legitimacy of the federal system and its constitution has been a governance issue of wide public interest. This paper revealed that the Ethiopian federal state structure and governance system suffered from systemic risks and in effect, was practically challenged when testing the administration in light of Roland Watts's *six principles* that ought to be the characteristics of any federal system: disposition to democratic procedures, non-centralization as a principle, checks and balances to limit the concentration of political power, open political bargaining for making collective decisions and genuine group power-sharing within central institutions, often consociational and respect for constitutionalism and the rule of law. Though some of these principles are embedded in the constitution, the EPRDF Government has practically failed to deliver them properly. The current waves of conflict and political instability is targeted against the system for its failure to deliver political and socio-economic justice for the common good. The grave situation the country is currently facing requires tangible action that goes beyond the traditional and old ways of addressing ethnic conflict and political instability i.e. through military and security policy. Instead an innovative approach is needed to deal with the problem. Since the problem is political and the risk associated with it is systemic and strategic, it requires a political solution with appropriate and holistic mitigation policy response to maintain peace and security and economic progress across the country. Hence, identification and management of risks associated with the system must be an integral part of a sound management and governance framework.

However, if the government is not willing to develop and implement effective risk management that addresses the root causes of political instability of the nation, while taking into account the above mentioned five principles of federalism—further political and administrative crises, as well as economic downturn will be inevitable. At the bottom

line, this requires the existence of a flexible system with political good will and leadership competence to make the federal operations successful. It is recommended, that all this should start with an open democratic dialogue with all sections of the society in general and opposition political parties both in and outside of the country need urgently to bring about a national consensus on the federal system and its constitution. Even with the existing scenario, the EPRDF Government has to be faithful to its own constitution so as to realize the rule of law in the country and save the system from disintegration. The federal system in Ethiopia is mainly regulated by the policies of the ruling party rather than by the merits of the constitution. Therefore, the sustainability of the nation as a diverse state fundamentally requires the full practical implementation of the federal system and its constitution while critically re-structuring the imbalance that are observed in the political economy system of the nation. Furthermore, it is recommended that, since there is a widespread disagreement about the origin and development of the federal system and its constitution among different groups in and outside the country, holding a national reconciliation and political referendum on the federal system and its constitution is fundamental to fix ethnic driven conflicts and political instability in the country.

References

[1] *Summary and Statistical Report of the 2007 Population and Housing Census.* Addis Ababa: Ethiopian Central Statistics Agency, 2008. http://ecastats.uneca.org/aicmd/Portals/0/Cen2007_firstdraft.pdf (Downloaded: 15.11.2017)

[2] ABEBE, S. G.: *The dilemma of adopting ethnic federal system in Africa in light of the perspectives from Ethiopian experience.* Journal of African Studies and Development Vol. 4(7), 2012, 169–175. https://doi.org/10.5897/JASD12.021

[3] MENGISTU, M. M.: Ethnic Federalism: A Means for Managing or a Triggering Factor for Ethnic Conflicts in Ethiopia. *Journal of Social Sciences,* 4 4 (2015), 94–105. https://doi.org/10.11648/j.ss.20150404.15

[4] DONHAM, D. L., WENDY, J.: *The Southern Marches of Imperial Ethiopia: Essays in History and Social Anthropology.* Cambridge: Cambridge University Press, 2002.

[5] TESHOME, W., ZÁHORÍK, J.: Federalism in Africa: The Case of Ethnic-based Federalism in Ethiopia. *International Journal of Human Sciences,* 5 2 (2008), 2–24.

[6] ABEBE, S. G.: *The Last Post-Cold War Socialist Federation Ethnicity, Ideology and Democracy in Ethiopia.* Connecticut: Ashgate Publishing Company, University of Connecticut, 2014.

[7] FESSHA, Y. T.: *Institutional Recognition and Accommodation of Ethnic Diversity: Federalism in South Africa and Ethiopia.* Western Cape: University of Western Cape, 2008. https://doi.org/10.4324/9781315580456

[8] FESSHA, Y. T.: *Federalism, Territorial Autonomy and the Management of Ethnic Diversity in Africa: Reading the Balance Sheet. L'Europe en Formation Revue d'études sur la construction européenne et le fédéralisme pages 265 à 285.* www.cairn.info/revue-l-europe-en-formation (Downloaded 03.03 2019). https://doi.org/10.3917/eufor.363.0265

[9] *The Proclamation of FDRE Constitution.* Addis Ababa: Berhanina Selam Printing Press, 1995.

[10] TAFIRENYIKA, M.: *Ethiopia's development is mostly people-driven. Africa Renewal* (online), 2015. www.un.org/africarenewal/magazine/august-2015/ethiopia%E2%80%99s-development-mostly-people-driven (Downloaded: 25.11.2017)

[11] *IMF Country Report No. 16/322.*: The Federal Democratic Republic of Ethiopia 2016 Article IV Consultation—Press Release; Staff Report; and Statement by the Executive Director for the Federal Democratic Republic of Ethiopia, 2016.

[12] *Current Ethiopian political environment assessment and analysis.* addisstandard.com, 2017. (Downloaded: 30.11.2017)

[13] *Africa Report No.153. Ethiopia: Ethnic Federalism and Its Discontents.* New York: International Crisis Group, 2009.

[14] OSAGHAE, E. E.: Federalism and the Management of Diversity in Africa. *Identity, Culture and Politics,* 5 1–2 (2004), 162–178.

[15] KOZAKOU-MARCOULLIS, E.: *Understanding Federalism: Federal States in the EU: Challenges and Opportunities.* European Parliament Office in Cyprus, 2015.

[16] ASEFA, F.: Ethiopia's Experiment in Accommodating Diversity: 20 Years' Balance-sheet. *Regional and Federal Studies,* 22 4 (2012), 435–473. https://doi.org/10.1080/13597566.2012.709502

[17] TERAMED, T. et al.: Silencing the Ethiopian Courts: Non-judicial Constitutional Review and Its Impact on Human Rights. *Fordham International Law Journal,* 32 1(2008), 259–297.

[18] PETRINI, B.: *Violent Conflicts in Sub-Saharan Africa, 1991–2008.* Washington, D.C.: World Bank, Social Development Department, 2010.

[19] *Amnesty International Report 2005 – Ethiopia.* London: Amnesty International, 25 May 2005. www.refworld.org/docid/429b27e07.html (Downloaded: 28.11.2017)

[20] TRUDEAU, P. E.: Federalism, Nationalism and Reason. In. KARMIS, D., NORMAN, W. (Eds.): *Theories of Federalism.* New York: Palgrave MacMillan, 2005. 221–226. https://doi.org/10.1007/978-1-137-05549-1_20

[21] *Ethiopia protests: "Nearly 100 killed" in Oromia and Amhara.* BBC (online), 8 August 2016. www.bbc.com/news/world-africa-37015055 (Downloaded: 23.11.2017)

[22] TEMESGEN, S. M.: Weaknesses of Ethnic Federalism in Ethiopia. *International Journal of Humanities and Social Science Invention,* 4 11 (2015), 49–54.

[23] ABBINK, J.: Ethnicity and Conflict Generation in Ethiopia: Some Problems and Prospects of Ethno-Regional Federalism. J*ournal of Contemporary African Studies,* 24 3 (2006), 389–413. https://doi.org/10.1080/02589000600976729

[24] HAGMANN, T., ABBINK, J.: Twenty years of revolutionary democratic Ethiopia, 1991 to 2011. *Journal of Eastern African Studies,* 5 4 (2011), 579–595. https://doi.org/10.1080/17531055.2011.642515

[25] ADEGEHE, A. K.: *Federalism and Ethnic Conflict in Ethiopia: A Comparative Study of the Somali and Benishangul Gumuz Regions.* (Doctoral Thesis) Leiden: Leiden University Department of Political Science, 2009.

[26] WATTS, R.: *Comparing Federal Systems in the 1990s.* Kingston: Queen's University, Institute of Intergovernmental Relations, 1996.

[27] AALEN, L.: *Ethnic Federalism in a Dominant Party State: The Ethiopian Experience 1991–2000.* Bergen: Chr. Michelsea, Institute Development Studies and Human Rights, 2002.

[28] ALEMANTE, S.: Ethiopia: Problems and Prospects for Democracy. *William and Mary Bill of Rights Journal,* 1 2 (1992), 205–26.

[29] LINZ, J. J., STEPAN, A. S.: Toward Consolidated Democracies. *Journal of Democracy,* 7 2 (1996), 14–33. https://doi.org/10.1353/jod.1996.0031

[30] CHANIE, P.: Clientelism and Ethiopia's Post-1991 Decentralisation. *The Journal of Modern African Studies,* 45 3 (2007), 355–384. https://doi.org/10.1017/S0022278X07002662

[31] KELLER, E: Ethnic Federalism and Democratization in Ethiopia. *Horn of Africa,* 21 (2003), 30–43.

[32] FISEHA, A.: Theory versus Practice in the Implementation of Ethiopia's Ethnic Federalism. In. TURTON, D. (Ed.): *Ethnic Federalism: The Ethiopian Experience in Comparative Perspective.* Oxford: James Currey, 2006.

[33] BAKKE, M. K., WIBBELS, E.: Diversity, Disparity, and Civil Conflict in Federal States. *World Politics,* 59 1 (2006), 1–50. https://doi.org/10.1353/wp.2007.0013

[34] JINADU, L. A.: Explaining and Managing Ethnic Conflict in Africa: Towards a Cultural Theory of Democracy. *Claude Ake Memorial Papers,* 1 (2007). Uppsala: Department of Peace and Conflict Research Uppsala University, Nordic Africa Institute Uppsala. 2007. http://nai.diva-portal.org/smash/get/diva2:278846/FULLTEXT01.pdf (Downloaded: 18.11.2017).

[35] SMOOHA, S., HANF, T.: The Diverse Mode of Conflict Regulation Mechanism in Deeply Divided Societies. *International Journal of Comparative Sociology,* 33 (1992), 1–2.

[36] AALEN, L.: Ethnic Federalism and Self-Determination for Nationalities in a Semi-Authoritarian State: The Case of Ethiopia. *International Journal Minority Group Rights,* 13 (2006), 243–261. https://doi.org/10.1163/157181106777909849

[37] *Freedom in the world 2017 – Ethiopian Profile.* Washington, D.C.: Freedom House, 2017.

[38] LERNER, H.: *The People of the Constitution: Constitution-Making, Legitimacy, Identity.* (A Paper presented at the mini-APSA, Department of Political Science.) New York: Columbia University, 2004.

[39] ELAZAR, D. J.: *Exploring Federalism.* Tuscaloosa: University of Alabama Press, 1987.

The Trump Administration and U.S.–Russian Relations[1]

Gábor CSIZMAZIA[2]

President Trump's controversial foreign policy performance, particularly in relation to Russia, raises the question of his administration's stance towards U.S.–Russian relations. While the President has displayed initial intentions of reaching out to Moscow, his administration's overall view of the world sets U.S.–Russian relations in a competition-based framework. This "global arena" perspective is reflected in official national security policy documents and by major foreign policy decision-makers as well. Thus the Trump Administration not only maintains its predecessor's initiatives countering Russia but enhances them by further emphasizing deterrence and containment measures in Europe through an increased European Deterrence Initiative (EDI) budget, addressing Russian violation of the Intermediate-Range Nuclear Forces (INF) Treaty, and arming Ukraine with lethal defensive weapons.

Keywords: *Trump, United States, Russia, great power, competition, Europe, deterrence*

Introduction

The Trump Administration's foreign policy performance has been an issue of debate among scholars of international relations and by the general public alike. The tone and decisions of the 45th President of the United States—especially when compared to that of his predecessor—are controversial, and his stance towards Russia is no different. On the one hand, President Trump is under constant fire of accusations due to the alleged collusion between his election campaign team and the Russian interference in the 2016 U.S. presidential elections. In addition to his suggestions on trying to mend relations with Russia, his remarks on the scope of Russian meddling did not help his situation in mainstream media or Congress. For example, in early 2018 the Editorial Board of *The Washington Post* described the President's behavior in the matter inappropriate and called on the legislative branch to fill the void of absent presidential leadership. [1] In other words, at home President Trump is in a politically weak position to form his own Russia policy. On the other hand, the Trump Administration has preserved several of its predecessor's initiatives in addressing Russia's assertive foreign policy. In fact, it has gone further on this road, enhancing some of

2 Assistant Lecturer, National University of Public Service; e-mail: csizmazia.gabor@uni-nke.hu; ORCID ID: 0000-0002-4907-2414

these measures quantitatively and qualitatively alike. These include the continuing targeted U.S. sanctions against Russian individuals, the authorization of sending lethal weapons to Ukraine, and ordering air strikes against the Kremlin-endorsed Assad regime for allegedly using chemical weapons against civilians in Syria. [2] It is without doubt that U.S.–Russian relations have not improved at all thus far under the Trump presidency. The aim of this article is to examine the driving factors behind the Trump Administration's position on U.S.–Russian relations. The analysis reviews external (inherited) factors and internal actors (administration team), highlighting the policy outputs through concrete examples.

The Outside World as It Is

In order to understand the Trump Administration's stance towards Russia, it is necessary to set it into context and examine Washington's view of the international environment and particularly U.S.–Russian relations. The latter has re-occurred several times on the high end of the post-Cold War American foreign policy agenda with each president at the time having tried (and ultimately failed) to establish lasting good bilateral relations. As a result, the bilateral relationship has displayed fluctuations. This article does not intend to map up the history of the post-Cold War U.S.–Russian relationship in its entirety but to highlight its characteristics that emerged by the time the Trump Administration took office.

President Obama's Turn from Partnership to Deterrence

Washington's most recent serious attempt to cooperate with Moscow was made by the Obama Administration in 2009. The "reset" with Russia was rooted in President Obama's view of the international environment. Barack Obama was regarded by some to have a more realist view of the world than his predecessor. While the realist nature of President Obama's foreign policy is debatable,[3] it is clear that he tried to look at the world as it is. Firstly, his administration recognized that that the "international architecture that was largely forged in the wake of World War II is buckling under the weight of new threats". [4: 40] This went hand in hand with the other realization, namely that while America is in fact the leader of this international order, its power is limited.[4] Secondly, this acknowledgment was primarily true in case of global challenges which the Obama Administration was most concerned with. President Obama's 2010 national security strategy characterized the United States' strategic environment with threats, risks and challenges of a "global age" such as: violent extremism, terrorism and the proliferation of weapons of mass destruction (WMDs) (which it considered to be the gravest danger to America), challenges in space and cyberspace, dependence on fossil fuels and climate change, failing states and global criminal networks, as well as the economic inequalities of globalization. Another attribute of the global landscape was that new and emerging powers (including Russia and China) were gaining

---

[3]   For an overview of President Obama's realist-like instincts but the lack of realist worldview, see Stephen M. Walt's article "Obama Was Not a Realist President" published in *Foreign Policy* in April 2016. [3]

[4]   "In an interconnected world, there are no global problems that can be solved without the United States, and few that can be solved by the United States alone." [5: 3]

influence. [4: 8] These recognitions led the Obama presidency to try to build partnerships addressing these global challenges and at the same time to shape a "just and sustainable international order" that represent "the diffusion of influence in the 21st century."[5] [4: 12] It is important to emphasize, however, that the Obama Administration did not want to dismantle the international system let alone discard America's role of leadership. This is a crucial point, as it reveals the conceptual differences between the respective world views of the White House and the Kremlin. While the Obama Administration pursued a cooperation-oriented multi-partner world that would replace the competition-based multi-polar one,[6] the Medvedev/Putin Administration was hanging on to the latter before[7] and after President Obama's term in office alike. [8] Hence this fundamental divergence in views existed in parallel to all of the accomplishments of the "reset" with Russia.

President Obama's national security team knew about the presence of inter-state competition in the world but thought that other global players would share their analysis of the international environment: specifically, the Obama Administration took the liberal view of international competition being "self-defeating" with defectors being punished by exclusion from the opportunities of cooperation.[8] In other words, Washington assumed that common global challenges will lead to common ground with others who would have no real interest in competition. This was also thought of Russia. Expecting "win–win" situations,[9] President Obama emphasized the incentive of Russia being a responsible great power in the international system and his hope of the "reset" bringing a lasting qualitative change in bilateral relations.[10] At the same time, the Obama White House was not entirely naïve. It was aware of the above mentioned dissent in American and Russian world views, as well

---

[5] "The test of this international order must be the cooperation it facilitates and the results it generates – the ability of nations to come together to confront common challenges like violent extremism, nuclear proliferation, climate change, and a changing global economy." [4: 12]

[6] As U.S. Secretary of State (2009–2013) Hillary R. Clinton noted in July 2009: "In short, we will lead by inducing greater cooperation among a greater number of actors and reducing competition, tilting the balance away from a multi-polar world and toward a multi-partner world." [6]

[7] As Russian Minister of Foreign Affairs Sergei Lavrov wrote in May 2007: "Russia has restored its foreign-policy independence – as a sovereign democratic state. Thus, for the first time in many years, a real competitive environment has emerged on the market of ideas for the future world order that are compatible with the present stage of global development. The establishment of new global centers of influence and growth, a more balanced distribution of resources for development, and control over natural wealth, represent the foundation for a multipolar world order." [7: 13–14]

[8] "Even though many defining trends of the 21st century affect all nations and peoples, too often, the mutual interests of nations and peoples are ignored in favor of suspicion and self-defeating competition. […] And when national interests do collide […] those nations that defy international norms or fail to meet their sovereign responsibilities will be denied of the incentives that come with greater integration and collaboration with the international community." [4: 40]

[9] Speaking in Moscow in March 2011, Vice-President Joseph R. Biden said he believed in "'win–win' situations" […] [and rejected] the tired theory that our values and our interests must compete for influence over our politics." [9]

[10] President Obama said in 2009 in Moscow that global "challenges demand global partnership, and that partnership will be stronger if Russia occupies its rightful place as a great power. Yet unfortunately, there is sometimes a sense that old assumptions must prevail, old ways of thinking; a conception of power that is rooted in the past rather than in the future. […] These assumptions are wrong. In 2009, a great power does not show strength by dominating or demonizing other countries. The days when empires could treat sovereign states as pieces on a chess board are over. […] The pursuit of power is no longer a zero-sum game – progress must be shared. That's why I have called for a 'reset' in relations between the United States and Russia. This must be more than a fresh start between the Kremlin and the White House." [10]

as of Russian tendencies for assertiveness—after all, it took office right after U.S.–Russian relations had cooled down due to the 2008 Russo–Georgian War. It did warn the Kremlin that while the "reset" offers great opportunities for achieving common goals in nuclear arms reduction, economic cooperation, and the fight against terrorism, it is not a trade-off in which Washington would be easy on Moscow's possible violation of international norms and principles. Moreover, the Obama Administration's liberal stance was also felt in its willingness to stand up for political reforms and against human rights violations in Russia.[11] This ultimately led to the deterioration of bilateral relations during Russia's 2011 parliamentary and 2012 presidential elections. The Ukraine crisis obviously worsened the situation. President Obama introduced a set of financial economic sanctions against Russian individuals in accordance with its aforementioned world view that offenders of the international order need to be punished. His 2015 national security strategy continued to value partnerships for addressing global challenges while calling for a U.S.-led international order championed by most countries. At the same time, it acknowledged that "in many cases […] coercive measures are meant not only to uphold international norms, but to deter severe threats to stability and order at the regional level." [5: 23] Thus by the end of the Obama presidency, U.S. efforts to conform eastern European allies have formally turned from the latter group's re-assurance to the deterrence against Russia.[12] The Obama Administration's second national security strategy also declared that "power among states is more dynamic", adding that Russia's aggression will "significantly impact the future of major power relations". [5: 4] This was a moderate statement compared to that of the Trump Administration on this subject but it revealed that Washington's more emphasized view on power struggles began to take shape.

President Trump's Global Arena of Competition

Throughout the 2016 presidential election campaign, Donald J. Trump made a series of outspoken statements on what he believed to be the failures of the American foreign policy after the Cold War. [11] His foreign policy turn within his "America First" campaign was named "principled realism" which gave a heavy weight to the realist themes of power and national interests in President Trump's 2017 national security strategy.[13] The Trump Administration's hitherto adherence to realist concepts is debatable,[14] nevertheless, it clearly

---

[11] In his aforementioned speech, Vice President Biden reminded that addressing Russian domestic issues are "necessary to have a good relationship […] [and that Washington] will continue to object when […] human rights are violated or democracy and the rule of law is undermined [in Russia]." [9]

[12] The Obama Administration's European Reassurance Initiative (ERI) was announced in June 2014. In addition to conforming Eastern European allies, it was also meant to increase deterrence against Russian aggression. The latter aspect received further emphasis by the summer of 2016 while the budget for FY 2017 already mentioned European Deterrence Initiative (EDI).

[13] "This strategy is guided by principled realism. It is realist because it acknowledges the central role of power in international politics, affirms that sovereign states are the best hope for a peaceful world, and clearly defines our national interests. It is principled because it is grounded in the knowledge that advancing American principles spreads peace and prosperity around the globe." [12: 55]

[14] As Stephen M. Walt highlighted, while some of the President's ideas (such as mending relations with Russia, reforming international trade arrangements, and adjusting the transatlantic burden-sharing in defense) do have rational foundation, their execution has been counterproductive. [13]

has a more competition focused mindset than its predecessor. Nadia Schadlow, leading author of the 2017 national security strategy document, for example, indicated in early 2017 that American diplomacy was still not fully aware of the essence of the political competition present in the world.[15] When explaining the concept of "America First", Lt. Gen. Herbert Raymond McMaster, President Trump's National Security Advisor (2017–2018) and Gary David Cohn Director of the National Economic Council (2017–2018) at the time reminded that the administration has "a clear-eyed outlook that the world is not a 'global community' but an arena where nations, nongovernmental actors and businesses engage and compete for advantage". [15] This, they emphasized, does not mean that America is alone, as the Trump Administration also intends to rely on partners and international institutions. However, it is noticeable that these institutions are primarily meant to serve U.S. national interests and although Washington is open to reform them, it also retains the option of a selective approach in such engagements.[16] In fact, the Trump Administration concluded that some of the international institutions have proven to be ineffective in transforming other major powers (such as China and Russia) into cooperative partners.[17] This means that the earlier concept of ultimate democratic peace through inclusive engagement of countries has failed.[18] Instead, the Trump team states that "a central continuity in history is the contest for power" and that "geopolitics is the interplay of these contests [over influence] across the globe", [12: 25–26] leading to the return of great power competition. The 2018 U.S. national defense strategy outright says that with the United States "emerging from a period of strategic atrophy, […] facing increased global disorder, characterized by decline in the long-standing rules-based international order […] inter-state competition, not terrorism, is now the primary concern in U.S. national security". [16: 1]

The 2017 U.S. national security strategy confirms the Obama Administration's view that China and Russia are becoming more assertive, but at the same time it goes further and openly declares that they are revisionist powers "contesting [the United States'] geopolitical advantages and trying to change the international order in their favor". [12: 27] The Obama Administration's 2015 national security strategy came to the same conclusion

---

[15] "The Trump administration has an opportunity to build up what we lack: the capacity to engage these long term political competitions. […] Today, the word 'compete' is rare in State Department strategy documents. The new team has an opportunity to develop approaches to counter adversaries, convince the undecided, and influence the competitions unfolding all over the world." [14]

[16] "The United States must lead and engage in the multinational arrangements that shape many of the rules that affect U.S. interests and values. A competition for influence exists in these institutions. As we participate in them, we must protect American sovereignty and advance American interests and values. […] All institutions are not equal, however. The United States will prioritize its efforts in those organizations that serve American interests, to ensure that they are strengthened and supportive of the United States, our allies, and our partners. […] If the United States is asked to provide a disproportionate level of support for an institution, we will expect a commensurate degree of influence over the direction and efforts of that institution." [12: 40]

[17] "Thee competitions require the United States to rethink the policies of the past two decades – policies based on the assumption that engagement with rivals and their inclusion in international institutions and global commerce would turn them into benign actors and trustworthy partners. For the most part, this premise turned out to be false." [12: 3]

[18] "Since the 1990s, the United States displayed a great degree of strategic complacency. We assumed that our military superiority was guaranteed and that a democratic peace was inevitable. We believed that liberal-democratic enlargement and inclusion would fundamentally alter the nature of international relations and that competition would give way to peaceful cooperation." [12: 27]

but expressed it in a more restrained way.[19] The Trump Administration is more outspoken on the respective rise and aggression of China and Russia who (along with others) have also changed the "character of competition" by "operating below the threshold of open military conflict and at the edges of international law" in order to covertly and gradually reach their goals, and ultimately "over time, a new status quo".[20] [12: 27–28] Thus the competition between the United State and Russia exists on a wide scale ranging from the spheres of military, economy and technology, to politics and public opinion. Accordingly, Russian efforts to counter U.S. (and Western) influence are visible in its military—especially nuclear weapons—development programs, cyber attacks against and subversions within other countries' domestic political affairs. The Trump team shares the Obama Administration's views that Russia is using economic tools—particularly Europe's energy dependence—for increasing its political influence. [5: 5] [12: 38] Moreover, while Russia perceives the U.S. and the EU as threats, [12: 25–26] the competition affects other regions as well, including the Middle East.[21] All of this, however, does not mean that the Trump Administration intends to completely isolate Russia. Similarly to his predecessors, President Trump signaled his intent to find areas of joint cooperation, should Russia change course. [12: 25]

Actors and Decisions

The recent chill in U.S.–Russian relations is felt through various issues including the war in Syria. After President Trump announced coordinated air strikes against the Syrian Government's facilities on the 14th of April 2018 as a punishment for a chemical attack in the country the week before, U.S. Ambassador to the UN Nikki R. Haley indicated the future introduction of a new set of sanctions against Russia for supporting the Syrian regime. Director of the National Economic Council Lawrence A. Kudlow denied this, saying that Ambassador Haley's incorrect statement was due to her "momentary confusion". This caused a minor inter-administration clash with Ambassador Haley remarking: "With all due respect, I don't get confused." Although this public dissent turned out to be a misunderstanding caused by a communication error, [17] it does raise the question how members of the Trump Administration—more specifically within the National Security Council—view the U.S. policy on Russia. Therefore, in order to understand the latter, the respective positions of major U.S. foreign policy decision-making actors, as well as the rationale behind some of the administration's decisions are worthy of review.

---

[19] "As the balance of economic power changes, so do expectations about influence over international affairs. Shifting power dynamics create both opportunities and risks for cooperation, as some states have been more willing than others to assume responsibilities commensurate with their greater economic capacity. In particular, India's potential, China's rise, and Russia's aggression all significantly impact the future of major power relations." [5: 4]

[20] "China and Russia want to shape a world antithetical to U.S. values and interests." [12: 25]

[21] As Nadia Schadlow argues, "the Middle East is in turmoil due not only to the assault of Islamist terrorist organizations, but also due to a regional competition among Iran, Arab states, Turkey, Russia, and the West". [14]

The President's National Security Team

Ever since his election campaign, Donald Trump's views on Russia have been controversial. On the one hand, it was clear already before the election that the Trump team was the overall beneficiary of Russian interferences in the campaign which were directed against Hillary R. Clinton who was considered to be more hawkish with regards to Russia. Reports in mainstream media also emphasized Trump businesses having ties to pro-Kremlin Russian financiers. [18] Eventually, allegations of the Trump team's collusion with foreign (Russian) actors triggered an official investigation by ex-FBI Director Robert S. Mueller as special counsel. While the investigation is pursued in the background, mainstream media—having a mutually sour relationship with President Trump—keeps the issue on high display thus maintaining domestic pressure on the White House. On the other hand, Donald Trump has championed the idea of mending bilateral relations "from a position of strength". [11][22] This is mandated by his policies on "America First" and "peace through strength" but also driven by Congress which has quickly limited the President's space of maneuver by enacting President Obama's executive orders on earlier sanctions against Russian individuals thus making it impossible for President Trump to withdraw them without the legislative branch's support. What makes the President's position on the subject more controversial is his communications: though he adheres to the strong policies against Russia, he often shows reluctance.[23]

The President's mixed views on the relationship with Russia can be counterbalanced by the foreign and security policy decision-making actors surrounding him. Key among them is the National Security Advisor. President Trump's first National Security Advisor Lt. Gen. Michael T. Flynn (2017) was forced out of his job very early precisely due to his proximity to—and background negotiations with—Russian actors. [21] While the President showed mixed views on the issue,[24] his second National Security Advisor Lt. Gen. H. R. McMaster (2017–2018) was clearer and more open about Russia. Already under the Obama Administration, Lt. Gen. McMaster, as Head of the U.S. Army Capabilities Integration Center, proposed a study on Russia's new generation of warfare. In his April 2016 testimony before the Senate Armed Services Committee, he indicated that while the U.S. was tied down in Iraq and Afghanistan, "Russia studied U.S. capabilities and vulnerabilities and embarked on an ambitious and largely successful modernization effort" to which the U.S. Army should adapt, as well. [22] Similarly, as National Security Advisor, he declared that "Russia is engaged in a very sophisticated campaign of subversion to affect our confidence

---

[22]   "Now, again, maybe I'm not going to be able to do a deal with Russia, but at least I will have tried. And if I don't, does anybody really think that Hillary Clinton would be tougher on Russia than Donald Trump? Does anybody in this room really believe that?" [19]

[23]   In case of the enacted sanctions known as the "Countering America's Adversaries Through Sanctions Act", President Trump published a signing statement in which he called the piece of legislation "significantly flawed", as it constrains his power as President. [20]

[24]   Although President Trump did ask for the resignation of Lt. Gen. Flynn, shortly after the latter's secret dealing with other (including Russian) diplomats came to light, he did not disapprove his actions, only the fact that the National Security Advisor did not truthfully inform the Vice-President about the discussions. As the President said: "Mike [Flynn] was doing his job. He was calling countries and his counterparts. So it certainly would have been okay with me if he did it. I would have directed him to do it if I thought he wasn't doing it. I didn't direct him but I would have directed him because that's his job." [19]

in democratic institutions, in democratic processes" and thereby creating divisions within Western societies. [23] However, Russia turned out to be one of the collision issues[25] between the President and the National Security Advisor who left office in March 2018. After his departure from the White House, Lt. Gen. McMaster noted that the United States has "failed to impose sufficient costs" on Russia. [25] President Trump's new National Security Advisor, former U.S. Ambassador to the UN John R. Bolton shares his predecessor's thoughts on Russian intent to divide the American society through its interference in the 2016 U.S. presidential election, as well as the idea that hitherto U.S. reactions should be intensified into "decidedly disproportionate"[26] retaliation. He also argued that due to the mainstream media's pressure on the President and his campaign collusion with Russian actors, "the Trump administration has neither developed nor deployed a coherent Russia policy". [26]

Similarly to President Trump, his first Secretary of State, Rex W. Tillerson (2017–2018) was initially regarded as one with mixed views on Russia. On the one hand, his ties to Russia were clear from the start: as CEO of ExxonMobil, he received the Order of Friendship medal by Russian President Vladimir V. Putin in 2013 for the company's 2011 investment in the Russian territories of the Arctic. While the project suffered from the post-2014 sanctions, Mr. Tillerson was head of ExxonMobil until joining the Trump Administration which made him a target for inquiries on financial and economic interests in Russia. On the other hand, his business career was regarded as a proof of aptitude, as he had rallied a group of ex-diplomats and geopolitical experts for his advisory team at ExxonMobil. [27] Yet as Secretary of State, he struggled with his department which was under the blade of financial and personnel cuts. In fact, the Trump Administration has had a tendency to downgrade diplomacy and thereby the importance of Secretary Tillerson in foreign policy decision-making. In the meantime, he became more and more critical concerning Russia. Already during his congressional hearing for the post, Rex Tillerson called for a "clear-eyed" relationship with a Russia that "poses a danger, but it is not unpredictable in advancing its own interest". Similarly to President Trump, he identified the source of the problem in weak American leadership and urged a "frank dialogue" between the two countries. [28: 6][27] By the end of 2017, his position moved closer to the mainstream U.S. views on Russia, and he reminded that "absent a peaceful resolution of the Ukraine situation [i.e. the restoration of the country's sovereignty and territorial integrity], [...] there cannot be business as usual with Russia. [29]

---

[25] For example, President Trump criticized the National Security Advisor for one of his public remarks on Russian interference in the 2016 U.S. presidential elections, downplaying the Russian involvement's importance regarding the outcome of the election. [24]

[26] As John Bolton noted in an opinion article a couple of months before his appointment of National Security Advisor: "We need to create structures of deterrence in cyberspace, as we did with nuclear weapons [...] One way to do that is to engage in a retaliatory cyber campaign against Russia. This effort should not be proportional to what we have just experienced. it should be decidedly disproportionate." [26]

[27] "Our NATO allies are right to be alarmed at a resurgent Russia. But it was the absence of American leadership that his door was left open and unintended signals were sent. We backtracked on commitments we made to allies. We sent weak or mixed signals with 'red lines' that turned into green lights. We did not recognize that Russia does not think like we do. Words alone do not sweep away an uneven and at times contentious history between our two nations. But we need an open and frank dialogue with Russia regarding its ambitions, so that we know how to chart our own course." [28: 6]

Since Tillerson's final statement as Secretary of State was a condemnation of Russia,[28] his removal from the Trump Administration increased the media's and the opposition's suspicion of President Trump being too soft on the Kremlin. [30] However, President Trump's new appointee, former CIA Director Michael R. Pompeo is considered to be a hardliner when it comes to Russia: already in his congressional hearing for his position at the CIA, Mr. Pompeo argued that: "Russia has reasserted itself aggressively, invading and occupying Ukraine, threatening Europe, and doing nearly nothing to aid in the destruction of ISIS." [31: 4] Similarly, in his opening statement of his congressional hearing for the position of Secretary of State, he emphasized that: "President Trump's national security strategy, rightfully, has identified Russia as a danger to [the United States]." [32: 10] Mr. Pompeo is regarded to have a better personal relationship with the President than his predecessor had, yet it is currently a question whether this would play a decisive role in guiding the President on Russia.

Compared to the aforementioned actors, the Secretary of Defense seems to have a stabile position in President Trump's administration. General James N. Mattis already revealed a fraction of the Trump Administration's assessment of the international environment in an August 2016 article he co-wrote with fellows at the Hoover Institution, arguing that the world has become more dangerous as a result of "20 years of the United States operating unguided by strategy" and that Russia (along with China, Iran and terrorists groups) have assaulted the international order. [33] In his congressional hearing for the top position in the Pentagon, General Mattis said that the most important thing is to "recognize that [Vladimir Putin] is trying to break the North Atlantic Alliance", adding that the actions of Russia—along with that of China and terrorist groups—represent "the biggest attack [on the post-WWII order] since World War II" and thus calling for U.S. deterrence. [34: 41] The U.S. commitment to NATO's cohesion is a significant indicator of former Secretary Mattis' efforts to guide the President in foreign and security policy. In contrast to Donald Trump's harsh statement during the 2016 U.S. presidential election campaign that the transatlantic alliance is "obsolete", General Mattis has regarded NATO as "the most successful military alliance probably in modern world history and maybe ever" [34: 56] and has intended to emphasize this view to the President[29]—in which he ultimately succeeded (based on President Trump's later statements). As for the bilateral relationship with Russia, General Mattis did not reject the re-occurring idea of cooperation with Moscow on specific issues while having disagreements in other areas, however, he also noted that there are fewer opportunities for the former and more cases for the latter given that Russia "has chosen to be a strategic

---

[28] Regarding the assassination attempt against former Russian military intelligence officer Sergei Skripal in the United Kingdom, Secretary Tillerson called Russia "an irresponsible force of instability in the world, acting with open disregard for the sovereignty of other states and the life of their citizens". After President Trump removed Rex Tillerson from office, U.S. House Minority Leader Nancy Pelosi noted that "Secretary Tillerson's firing sets a profoundly disturbing precedent in which standing up for our allies against Russian aggression is grounds for a humiliating dismissal". [30]

[29] "I have had discussions with [Mr. Trump] on this issue. He has shown himself open even to the point of asking more questions, going deeper into the issue about why I feel so strongly. And he understands where I stand, and I will work with the other members of the national security team […] to carry these views forward." [34: 57]

competitor". [34: 45][30] At the same time, Secretary Mattis was considered to be a voice of reason within the Trump team, advocating consistency in U.S. engagements (including military operations) throughout the world and cautioning the President in tense situations with Iran or North Korea.[31] While Gen. Mattis intended to utilize President Trump's increase in the U.S. defense budget to prepare the armed forces for a potential conflict with Russia or China, [35] his caution of confronting the former was clear.[32]

Actions of Deterrence

Throughout its first year the Trump Administration has made several steps directed against Russia in one way or another. These included the maintenance of economic pressure through sanctions against individuals, as well as cutting back diplomatic relations through the expelling of Russian diplomats. However, these were only reactions to specific Russian deeds. Considering the notion that the aforementioned competition with great power rivals manifests in various regions, the U.S stance towards NATO and its eastern flank serves as a more persistent benchmark of how the Trump Administration engages vis-à-vis Russia. In addition to promoting "a strong and free Europe", [12: 47] the Trump Administration is particularly attentive concerning "unfavorable shifts" in "regional balances" between the U.S. and other great powers.[33] Hence it intensified efforts aimed at deterring Russia in Europe, starting with a galvanized position on the issue of burden sharing within NATO. Donald Trump made several statements on U.S. dissatisfaction with the fact that most European members of the alliance are not paying enough on national defense and thus are (almost) free riders of Article 5 primarily assured by the United States. These included unconventional announcements such as having U.S. commitment to collective defense depend on whether the given member states actually spend 2% of their respective GDP on defense, as well as emphasizing the importance of the latter during his first attendance at a NATO summit while neglecting to mention America's commitment to Article 5 at all. Such comments received overall negative reactions, yet there are two things that should be noted on the subject (apart from the fact that Secretary Tillerson, Secretary Mattis and later President Trump himself confirmed America's pledge to preserve NATO's collective defense).

---

[30] "I am all for engagement, but we also have to recognize reality and what Russia is up to. And there is a decreasing number areas where we can engage cooperatively and an increasing number of areas where we are going to have to confront Russia." [34: 45]

[31] Ranking Member of the U.S. House Armed Services Committee Adam Smith recalled saying to Gen. Mattis before his confirmation: "Trump has no idea what he's doing but isn't afraid to do it. You're across the river, and they're across the hall. […] Your job is to make sure these morons don't get up in the morning and advance some lamebrained idea." [35]

[32] In his Senate confirmation hearing, Gen. Mattis was asked whether he would support additional sanctions against Russia, to which he said: "I would like to get with the new national security team, craft a strategy to confront Russia for what it has done." [34: 125]

[33] According to the Trump Administration's 2017 national security strategy, "changes in a regional balance of power can have global consequences and threaten U.S. interests. […] China and Russia aspire to project power worldwide, but they interact most with their neighbors. […] The United States must marshal the will and capabilities to compete and prevent unfavorable shifts in the Indo-Pacific, Europe, and the Middle East." [12: 45]

Firstly, this request from Washington is not new at all. Two of the most notable examples for this under the Obama Administration were the farewell remarks of former Secretary of Defense Robert M. Gates in June 2011, and President Obama's remarks after the NATO summit in July 2016. Secondly, the novelty of the message's style presumably had a purpose, as President Trump's threat of decreasing American commitment to NATO was partially echoed by Secretary Mattis[34] who has kept the alliance in higher regard. The rationale behind this notion was to increase pressure on allies so that they would increase their respective defense budgets they had agreed upon after 2014 at a faster pace, and ultimately to strengthen NATO. This idea was also incorporated in the Trump Administration's 2017 U.S. national security strategy, along with the concrete priority goal of having the allies reach their national defense budgets' threshold of 2% of GDP (with 20% of that focused on military capability development) by 2024 as opposed to the Obama Administration's 2015 national security strategy which emphasized U.S. commitment to Article 5 and cited some of the specific measures Washington had taken to help allies against Russia but did not really address their responsibility in this matter.[35] Thus in short, the Trump Administration's tactic of rhetorically wavering U.S. loyalty to Article 5 has actually been aimed at strengthening the alliance to which Washington's commitment in practical terms has remained.[36] Another example for the latter is the Trump Administration's increasing focus on the European Deterrence Initiative, formerly known as European Reassurance Initiative. Both "versions" have served the purpose of increasing U.S. military presence in Central and Eastern Europe via rotations, joint international exercises, trainings, and the enhanced infrastructure and pre-positioning of military equipment. The Trump Administration continued to boost these efforts: whereas the administration's EDI budget request for 2018 was $4.8 billion (a $1.4 billion increase compared to 2017), the request for 2019 grew further to $6.5 billion. Most of these funds are intended for the U.S. Army's intensified presence in Europe with an episodic and less predictable pattern and an increased number of equipment and vehicles (such as M1A2 Abrams main battle tanks, Patriot missiles, armored multi-purpose vehicles and Bradley fighting vehicles). According to the plans, the Army's pre-positioned equipment in Europe should be fully prepared by 2020 when more dynamic deployments with increased troop numbers can take place. [39]

---

[34] At the February 2017 meeting of NATO's Defense Ministers, Secretary Mattis said: "If your nations do not want to see America moderate its commitment to this alliance, each of your capitals needs to show support for our common defense." [36] Although this quote did leave its mark in international media, the U.S. Secretary also indicated that the hinted scenario was one that he would not speculate more upon: "I'd prefer not to [elaborate more about the word «moderate»] because basically that is the headline I do not anticipate ever seeing. […] And I'm very confident that we will not have to have that. Sometimes you say the things you don't want to have happen so that you head them off." [37]

[35] Furthermore whereas the 2015 document noted that "NATO is stronger and more cohesive than at any point in its history, especially due to contributions of the Nordic countries and newer members like Poland and the Baltic countries", [5: 7] the 2017 strategy emphasizes that NATO "will become stronger when all members assume greater responsibility for and pay their fair share to protect our mutual interests, sovereignty, and values". [12: 48]

[36] In June 2017, President Trump presented the issue the following way: "I have been an advocate for strengthening our NATO Alliance through greater responsibility and burden-sharing among member nations. […] I'm committing the United States to Article 5. And certainly we are there to protect. And that's one of the reasons that I want people to make sure we have a very, very strong force by paying the kind of money necessary to have that force." [38]

Another form of deterrence measures is to be found in U.S. nuclear power. Already during the 2016 U.S. presidential election campaign, Donald Trump said that the Obama and Medvedev Administrations' 2010 bilateral strategic nuclear arms reduction agreement known as the New START Treaty left the United States in a disadvantageous position compared to Russia with the latter increasing its nuclear arsenal.[37] The 2017 U.S. national security strategy declared that "nuclear armed adversaries have expanded their arsenals and range of delivery systems" [12: 30] which was later confirmed by the 2018 Nuclear Posture Review (NPR) specifically naming Russia and China in this regard. [41: 2] Although the latter document does not represent a harsh break from the Obama Administration's 2010 NPR, including the support for the aforementioned New START Treaty, [41: 73] it does have an increased focus on catching up with Russia in certain capabilities. Specifically, the report highlights that Russia achieved an advantage in non-strategic nuclear weapons as well as their delivery capabilities that do not fall under the regulation of the New START Treaty but do violate other agreements, most notably the 1987 Intermediate-Range Nuclear Forces Treaty. [41: 9] Moreover, Russia increased its reliance on these systems and decided to follow an "escalate to de-escalate doctrine" by which it opens the possibility of limited nuclear first use in a conflict assuming that this escalation will not lead to Western retaliation but to "capitulation on terms favorable to Moscow". [41: 30] Accordingly, the document calls for U.S. countermeasures that are compliant with existing arms limitation treaties but balance Russian non-strategic nuclear build-up at the same time, for example by introducing a submarine launched cruise missile along with a low-yield warhead. On the one hand, this move would serve as a deterrent against Russia's utilization of its aforementioned doctrine [42] while on the other, it could also put pressure on Moscow to return to the INF Treaty. In a hearing before the House Armed Services Committee shortly after the publication of the 2018 NPR, Secretary Mattis said that the initiative is intended to set U.S. diplomats "negotiating from a position of strength" with the aforementioned weapon systems functioning as potential bargaining chips.[38] [43] The issue of nuclear weapons and delivery systems has been one of the "hot spots" in U.S.–Russian quarrels throughout the last decade or so. Most recently, Vladimir Putin announced the development of a nuclear armed intercontinental missile that would allegedly penetrate any defense system. Reciting earlier complaints of American missile defense efforts hindering Russian security,[39] President Putin criticized current U.S. nuclear policy, as well. [45] While President Trump was less vocal on the subject, only calling the announcement "irresponsible", [46] the case did not improve his

---

[37] During his debate with presidential candidate Hillary Clinton in October 2016, Donald Trump complained: "Take a look at the 'start up' that [President Obama and President Medvedev] signed. The Russians […] create warheads, and we can't. […] We're in very serious trouble, because we have a country with tremendous numbers of nuclear warheads […] where they expanded and we didn't. […] And [Hillary Clinton is] playing chicken." [40]

[38] Secretary Mattis added: "I want to make certain that our negotiators have something to negotiate with, that we want Russia back into compliance. We do not want to forgo the INF [Treaty], but at the same time we have options if Russia continues to go down this path." [43]

[39] Despite the accomplishments of the Obama Administration "reset" policy, particularly the 2010 New START Treaty, Russia has vowed to counter U.S./NATO missile defense efforts in Central and Eastern Europe by developing its nuclear capabilities, defense and delivery systems in parallel to the advancement of the United States' missile defense program, as announced by former Russian President Dmitry A. Medvedev in November 2011. [44]

stance towards President Putin whose remarks could have been understood as a challenge of the U.S. President's strength. [47]

American efforts of stepping up against Russia are also enhanced through more direct engagement with frontier states as well. The need for containment measures was indicated in 2016 by policy analysts Jakub Grygiel and Wess A. Mitchell, the latter of whom became Assistant Secretary of State at the Bureau of European and Eurasian Affairs in the Trump Administration. The two scholars argued that in the time of intensified competition with revisionist powers, America should refocus its attention on alliances on the frontiers [48: 50] where "well-armed allies […] are a strategic blessing for the United States […] by becoming hardened obstacles [for the expansion efforts of revisionist powers]". [48: 55] In accordance, the Trump Administration has moved forward with arms sales to Poland and Romania, the larger European frontline states,[40] and has indicated that it would ease U.S. international arms sales in general. [49] This departure from the Obama Administration's considerations revealed a major novelty of the Trump Administration's policy on dealing with Russian aggression in December 2017: namely, its blessing for arming Ukraine with lethal weapons. Such a move has been long in the making. The Ukrainian Government had approached the Obama Administration to request lethal weapons, and although this idea was pushed forward by some in Congress and advisors of President Obama, he declined out of fear that providing these weapons to Ukraine would only help to escalate the conflict and would ultimately hurt the Ukrainians (and allied cohesion) more than it would hurt Russia.[41] Administration officials also fought to convince President Trump of the move with James Mattis and Rex Tillerson supporting the initiative that would enhance the already provided nonlethal arms (such as body armor, radars, radios and vehicles) with Javelin anti-tank missiles and sniper rifles. An important part of the Trump Administration's rationale is that although these arms are lethal, they are still defensive in nature, meaning that they are only intended to improve the Ukrainians' position against their adversaries, establishing a balance between them and thus make Russian efforts of further aggression more expensive.[42] [51] This is what Jakub Grygiel and Wess Mitchell have described—in the case of allies—as "deterrence by denial" which in their words "involves the development of capabilities that hinder the enemy's military advance by increasing the costs of territorial expansion and control". [48: 55] Furthermore, the potentially increasing expenses of Russian military

---

[40] It is by no accident that President Trump's first heads of state level meetings within Central and Eastern Europe were with the respective presidents of Poland and Romania in the summer of 2017.

[41] As Anthony J. Blinken, Deputy National Security Advisor (2013–2015) and Deputy Secretary of State (2015–2017) to President Obama noted in October 2017: "Proponents [of lethal aid ban under the Obama administration] argued that any military escalation favored Moscow, for whom the stakes were higher and the ability to quickly pour more lethal weapons into Ukraine much greater. They were concerned Ukraine would be emboldened to act out militarily and overplay its hand. They knew that Moscow sought to divide us from our European partners, most of whom opposed lethal aid. President Barack Obama concluded that we should keep the focus where we had the advantage: on tough sanctions, economic aid to Ukraine, training for its troops, support for its reform efforts—especially combating endemic corruption—and determined diplomacy." [50]

[42] As Ukrainian President Petro O. Poroshenko pointed out in the summer of 2017: "Any defensive weapons would be just to increase the price if Russia makes a decision to attack my troops and my territory." [51]

adventures can also contribute to the advancement of the peace process in Ukraine.[43] The case again reveals the Trump Administration's general view that "peace through strength" offers a more viable path to engaging with Russia.

Conclusion

While President Trump's foreign policy is usually viewed as controversial, it does show consistency in itself and partially with that of President Obama regarding Russia. Differing world views between the United States and Russia have already existed during the Obama Administration with the White House visioning a cooperation-oriented multi-partner world, and the Kremlin believing in a competition-based multi-polar one. By the end of President Obama's term in office it became clear that Russian aggression significantly affected major power relations of the future.

The Trump Administration is even more outspoken and vocal in this regard. Its official national security policy documents are testimonies of a competition-based mindset according to which the world is a global arena where the United States faces great powers as rivals. Accordingly, there's a contest of power with Russia (and China) manifesting in the geopolitics of several regions in the world. In addition to these declarations, the major foreign policy decision-making actors within the Trump Administration advocate a firm stance against Russia, as well. All of this has manifested in not only the maintenance of Obama-era initiatives countering Russian aggression but in their qualitative enhancement in Europe, as well.

The Trump Administration's world view and concept of "peace through strength" suggest that President Trump's personal tendencies of trying to get along with Russia are only examples of the already seen initial U.S. presidential efforts of reaching out to Moscow for the sake of mutually beneficial cooperation, and that they are largely outweighed by his administration's awareness of the realities of great power competition—now openly declared on both sides. Given these conditions, a rapprochement with Russia under the Trump Administration is in fact more unlikely than before.

References

[1]   Editorial Board: What Trump still doesn't get about Russian interference in the election. *The Washington Post,* 16.02.2018. www.washingtonpost.com/opinions/an-indictment-describes-russias-information-warfare-trump-continues-to-miss-the-point/2018/02/16/c2c34254-1359-11e8-9065-e55346f6de81_story.html?utm_term=.407c8ed0b0df (Downloaded: 17.04.2018)

---

[43]   Ambassador Kurt Volker, the Trump Administration's Special Representative for Ukraine Negotiations said in April 2018: "I think the delivery of some of these defensive arms to Ukraine demonstrates […] that the cost of escalating the conflict by Russia will only continue to grow. So […] we hope that […] [it] is clear to Russia that it's just not worth it, that escalating the conflict is not the direction to go in. We should be instead trying to end the conflict and bring about peace. So I think having a stronger Ukrainian defensive capability helps in the process of then negotiating towards a final settlement." [52]

[2] VAJDICH, P. D.: Trump's Russia Policy Is Better Than Obama's Was. *Foreign Policy,* 13.04.2018. http://foreignpolicy.com/2018/04/13/trumps-russia-policy-is-better-than-obamas/ (Downloaded: 17.04.2018)

[3] WALT, M. S.: Obama Was Not a Realist President. *Foreign Policy,* 07.04.2016. http://foreignpolicy.com/2016/04/07/obama-was-not-a-realist-president-jeffrey-goldberg-atlantic-obama-doctrine/ (Downloaded: 17.04.2018)

[4] *National Security Strategy.* Washington, D.C.: The White House, 2010.

[5] *National Security Strategy.* Washington, D.C.: The White House, 2015.

[6] CLINTON, R. H.: *Foreign Policy Address at the Council on Foreign Relations.* (Speech Hillary Rodham Clinton Secretary of State) Washington, D.C.: U.S. Department of State, 15.07.2009. https://2009-2017.state.gov/secretary/20092013clinton/rm/2009a/july/126071.htm (Downloaded: 18.04.2018)

[7] LAVROV, S.: The Present and Future of Global Politics. *Russia in Global Affairs,* 2 5 (2007), 8−21.

[8] CARROLL, O.: US 'devaluing' international law and institutions, says Russia's Sergei Lavrov. *Independent,* 15.01.2018. www.independent.co.uk/news/world/europe/sergei-lavrov-us-russia-foreign-minister-start-year-conference-united-nations-donald-trump-putin-a8160076.html (Downloaded: 18.04.2018)

[9] *Vice President Biden's Remarks at Moscow State University.* Washington, D.C.: Office of the Vice President, 10.03.2011. https://obamawhitehouse.archives.gov/the-press-office/2011/03/10/vice-president-bidens-remarks-moscow-state-university (Downloaded: 18.04.2018)

[10] *Remarks By The President At The New Economic School Graduation.* (President Obama's Address at the New Economic School in Moscow.) Washington, D.C.: Office of the White House Press Secretary, 07.07.2009. https://obamawhitehouse.archives.gov/video/President-Obamas-Address-at-the-New-Economic-School-in-Moscow#transcript (Downloaded: 18.04.2018)

[11] TRUMP, J. D.: Trump on Foreign Policy. *The National Interest,* 27.04.2016. http://nationalinterest.org/feature/trump-foreign-policy-15960 (Downloaded: 19.04.2018)

[12] *National Security Strategy of the United States of America.* Washington, D.C.: The White House, 2017.

[13] WALT, M. S.: What Trump Got Right About Foreign Policy. *Foreign Policy,* 28.08.2017. http://foreignpolicy.com/2017/08/28/what-trump-got-right-about-foreign-policy/ (Downloaded: 17.04.2018)

[14] SCHADLOW, N.: Welcome to the Competition. *War on the Rocks,* 26.01.2017. https://warontherocks.com/2017/01/welcome-to-the-competition/ (Downloaded: 19.04.2018)

[15] McMASTER, R. H., COHN, D. G.: America First Doesn't Mean America Alone. *The Wall Street Journal,* 30.05.2017. www.wsj.com/articles/america-first-doesnt-mean-america-alone-1496187426 (Downloaded: 19.04.2018)

[16] *Summary of the 2018 National Defense Strategy of the United States of America. Sharpening the American Military's Competitive Edge*. Washington, D.C.: U.S. Department of Defense, 2018.

[17] COLVIN, J., LEE, M., MILLER, Z.: 'I Don't Get Confused.' Nikki Haley Fires Back at White House After Russia Sanctions Comment. *Time,* 18.04.2018. http://time.com/5244371/nikki-haley-russia-sanctions-confused/ (Downloaded: 21.04.2018)

[18] NESBIT, J.: Donald Trump's Many, Many, Many, Many Ties to Russia. *Time,* 02.08.2016. http://time.com/4433880/donald-trump-ties-to-russia/ (Downloaded: 22.04.2018)

[19] *Remarks by President Trump in Press Conference.* Washington, D.C.: The White House, 16.02.2017. www.whitehouse.gov/briefings-statements/remarks-president-trump-press-conference/ (Downloaded: 22.04.2018)

[20] *Statement by President Donald J. Trump on the Signing of H.R. 3364.* Washington, D.C.: The White House, 02.08.2017. www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-signing-h-r-3364/ (Downloaded: 22.04.2018)

[21] SHEAR, D. M., GOLDMAN, A.: Michael Flynn Pleads Guilty to Lying to the F.B.I. and Will Cooperate With Russia Inquiry. *The New York Times,* 01.12.2017. www.nytimes.com/2017/12/01/us/politics/michael-flynn-guilty-russia-investigation.html (Downloaded: 23.04.2018)

[22] BENDER, B.: The Secret U.S. Army Study That Targets Moscow. *Politico.com,* 14.04.2016. www.politico.com/magazine/story/2016/04/moscow-pentagon-us-secret-study-213811 (Downloaded: 23.04.2018)

[23] HR McMaster: Russian meddling 'sophisticated subversion'. *BBC,* 19.12.2017. www.bbc.com/news/world-us-canada-42409144 (Downloaded: 23.04.2018)

[24] JOHNSON, E.: Trump's rebuke of McMaster was months in the making. Politico.com, 20.02.2018. www.politico.com/story/2018/02/20/trump-mcmaster-tension-national-security-adviser-417110 (Downloaded: 24.04.2018)

[25] *US National Security Advisor LTG H.R. McMaster: Russian Aggression is Strengthening Our Resolve.* Washington, D.C.: Atlantic Council, 03.04.2018. www.atlanticcouncil.org/news/transcripts/us-national-security-advisor-lt-gen-h-r-mcmaster-russian-aggression-is-strengthening-our-resolve (Downloaded: 24.04.2018)

[26] BOLTON, J.: Russian assault on 'American idea' enables Trump to take tough action. *The Hill*, 19.03.2018. http://thehill.com/opinion/national-security/374489-russian-assault-on-american-idea-enables-trump-to-take-tough-action (Downloaded: 24.04.2018)

[27] MacFARQUHAR, N., KRAMER, E. A.: How Rex Tillerson Changed His Tune on Russia and Came to Court Its Rulers. *The New York Times,* 20.12.2016. www.nytimes.com/2016/12/20/world/europe/russia-rex-tillerson-donald-trump-secretary-of-state.html (Downloaded: 24.04.2018)

[28] *Secretary of State Designate Rex Tillerson Senate Confirmation Hearing Opening Statement January 11, 2017.* Washington, D.C.: United States Senate Committee on Foreign Relations, 2017. www.foreign.senate.gov/imo/media/doc/011117_Tillerson_Opening_Statement.pdf (Downloaded: 24.04.2018)

[29] TILLERSON, R. W.: I Am Proud of Our Diplomacy. *The New York Times,* 27.12.2017. www.nytimes.com/2017/12/27/opinion/rex-tillerson-state-department-diplomacy.html (Downloaded: 24.04.2018)

[30] BLAKE, A.: Did Trump fire Tillerson because he was too anti-Russia? *The Washington Post,* 13.03.2018. www.washingtonpost.com/news/the-fix/wp/2018/03/13/did-trump-fire-tillerson-because-he-was-too-anti-russia/ (Downloaded: 24.04.2018)

[31] POMPEO, R. M.: *Statement for the Record before the Senate Select Committee on Intelligence.* Washington, D.C.: United States Senate Select Committee on Intelligence, 12.01.2017. www.intelligence.senate.gov/sites/default/files/documents/statement-pompeo-011217.pdf (Downloaded: 24.04.2018)

[32] POMPEO, R. M.: *Statement for the Record before the U.S. Senate Committee on Foreign Relations.* Washington, D.C.: United States Senate Committee on Foreign Relations, 12.04.2018. www.foreign.senate.gov/imo/media/doc/041218_Pompeo_Statement.pdf (Downloaded: 24.04.2018)

[33] SHAKE, K., MATTIS, J., ELLIS, J.: A blueprint for American security. *San Francisco Chronicle,* 11.08.2016. www.sfchronicle.com/opinion/article/A-blueprint-for-American-security-9137892.php (Downloaded: 25.04.2018)

[34] *Alderson Court Reporting: Stenographic Transcript Before the Committee on Armed Services, United States Senate to Conduct a Confirmation Hearing on the Expected Nomination of Mr. James N. Mattis to be Secretary of Defense.* Washington, D.C: United States Senate Committee on Armed Services, 12.01.2017. www.armed-services.senate.gov/imo/media/doc/17-03_01-12-17.pdf (Downloaded: 25.04.2018)

[35] JAFFE, G., RYAN, M.: Trump's favorite general: Can Mattis check an impulsive president and still retain his trust? *The Washington Post,* 07.02.2018. www.washingtonpost.com/world/national-security/can-jim-mattis-check-an-impulsive-president-and-still-retain-his-trust/2018/02/07/289297a2-0814-11e8-8777-2a059f168dd2_story.html (Downloaded: 25.04.2018)

[36] COOPER, H.: Defense Secretary Mattis Tells NATO Allies to Spend More, or Else. *The New York Times,* 15.02.2017. www.nytimes.com/2017/02/15/world/europe/jim-mattis-nato-trump.html (Downloaded: 26.04.2018)

[37] *Press Conference by Secretary James Mattis at NATO Headquarters, Brussels, Belgium.* Brussels: U.S. Department of Defense, 16.02.2017. www.defense.gov/News/Transcripts/Transcript-View/Article/1085679/press-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/ (Downloaded: 26.04.2018)

[38] *Remarks by President Trump and President Iohannis of Romania in a Joint Press Conference.* Washinfton, D.C.: The White House, 09.06.2017. www.whitehouse.gov/briefings-statements/remarks-president-trump-president-iohannis-romania-joint-press-conference/ (Downloaded: 26.04.2018)

[39] JUDSON, J.: Funding to deter Russia reaches $6.5B in FY19 defense budget request. *DefenseNews,* 12.02.2018. www.defensenews.com/land/2018/02/12/funding-to-deter-russia-reaches-65b-in-fy19-defense-budget-request/ (Downloaded: 26.04.2018)

[40] BLAKE, A.: The final Trump-Clinton debate transcript, annotated. *The Washington Post,* 19.10.2016. www.washingtonpost.com/news/the-fix/wp/2016/10/19/the-final-trump-clinton-debate-transcript-annotated/?utm_term=.11f6abbf46a4 (Downloaded: 29.04.2018)

[41] *Nuclear Posture Review.* Washington, D.C.: U.S. Department of Defense, 2018.

[42] MEHTA, A.: Nuclear Posture Review puts Russia firmly in crosshairs. *DefenseNews,* 02.02.2018. www.defensenews.com/space/2018/02/02/nuclear-posture-review-puts-russia-firmly-in-crosshairs/ (Downloaded: 29.04.2018)

[43] MEHTA, A.: Will the US trade its new sub-launched cruise missile for Russian arms treaty compliance? *DefenseNews,* 06.02.2018. www.defensenews.com/space/2018/02/06/will-the-us-trade-its-new-sub-launched-cruise-missile-for-russian-arms-treaty-compliance/ (Downloaded: 29.04.2018)

[44] *Statement in connection with the situation concerning the NATO countries' missile defence system in Europe.* (By President of Russia Dmitry Medvedev.) Gorki: President of Russia, 23.11.2011. http://en.kremlin.ru/events/president/news/13637 (Downloaded: 29.04.2018)

[45] SAVRANSKY, R.: Putin: New missile renders defenses useless. *The Hill,* 01.03.2018. http://thehill.com/policy/international/376191-putin-new-missile-renders-defenses-useless (Downloaded: 29.04.2018)

[46] MORIN, R.: Trump, May call Putin's statements on Russia's nuclear arsenal 'irresponsible'. *Politico.com,* 05.03.2018. www.politico.com/story/2018/03/05/trump-theresa-may-russia-putin-nuclear-arms-435840 (Downloaded: 29.04.2018)

[47] LEE, E. C.: Trump tells aides not to talk publicly about Russia policy moves. *NBC,* 29.03.2018. www.nbcnews.com/politics/donald-trump/trump-tells-aides-not-talk-publicly-about-russia-policy-moves-n861256 (Downloaded: 29.04.2018)

[48] GRYGIEL, J., MITCHELL, A. W.: Pressure on the Peripheries. *The American Interest,* Summer (May/June) 2016, 49−55.

[49] BENDER, B., PALMERI, T.: Trump to unleash more global arms sales. *Politico.com,* 29.07.2017. www.politico.com/story/2017/09/29/trump-global-arms-sales-243282 (Downloaded: 26.04.2018)

[50] BLINKEN, J. A.: Time for the Trump Administration to Arm Ukraine. *The New York Times,* 04.10.2017. www.nytimes.com/2017/10/04/opinion/trump-ukraine-russia.html (Downloaded: 26.04.2018)

[51] GORDON, R. M.: Jim Mattis, in Ukraine, Says U.S. Is Thinking of Sending Weapons. *The New York Times,* 24.08.2017. www.nytimes.com/2017/08/24/world/europe/mattis-ukraine-russia.html (Downloaded: 26.04.2018)

[52] *Latest Developments on Ukraine Negotiations.* Washington, D.C.: U.S. Department of State, 13.04.2018. https://fpc.state.gov/280441.htm (Downloaded: 27.04.2018)

The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace

(Part 1)[1]

Dóra DÉVAI[2]

Due to the heightened political sensitivity caused by the recently held U.S. midterm elections and the frenzied media concentration on the 2016 election meddling, hacking and leaks have been in the focus of public discussions ever since. In order to better comprehend the appraisal of the U.S. political leadership back in 2016 and early in 2017, this article contextualizes the events and the response measures in the wider cybersecurity position of the U.S. Tracking down the development of the U.S. political and military approach to cyber threats,[3] we came to the conclusion that the U.S. is lacking a working cybersecurity policy largely because its perception of cyber threats is self-centred and still deeply rooted in the strategic thinking of nuclear or traditional military attacks. Even if the same strategic principles are valid in cyberspace, cyberattacks, single, systemic or part of a broader influence operation, they play out according to a set of completely different dynamics than kinetic attacks. The true strategic lesson of the recent election meddling is that Russia has been, and most probably will be, able to seize the momentum and masterfully exploit those inherent deficiencies. Consequently, cyberspace as a strategic environment necessitates the careful analysis of the strategic thinking of the potential adverse nation.

Keywords: *U.S. cybersecurity policy, strategic culture, influence operations, cyber deterrence*

---

[1]   This is the first part of a series of three articles. The second part gives a strategic insight into the national response policy options to substantial cyberattacks in the U.S. The third part of the series continues the discussion with a concise overview of the Russian strategic context of influence operations.

[2]   Ph.D. student, National University of Public Service, Doctoral School of Military Engineering; Devai.Dora@uni-nke.hu; ORCID ID: 0000-0003-1024-4474

[3]   The article refers back to the regulatory background at its given state back at the time during the 2016 midterm elections.

Introduction

"Barack Obama and Joe Biden will ensure that his administration develops a Cyber Security Strategy that ensures that we have the ability to identify our attackers and a plan for how to respond that will be measured but effective" read the 2008 election site of then candidate Barack Obama. [1] The securitization and strategizing of cyberattacks go back to at least as early as the beginning of the 1990s. Nevertheless, there is a growing evidence that nation states have used cyberspace for intelligence and military purposes since the first versions of computers appeared.[4] In the meantime, the dependence of the nation states on the flawless operation of the internet and information technology in general has skyrocketed. In realization of this fact, cyberspace has been publicly recognized as an *operational domain,* and its strategic utility meaning, *the systematic employment of cyberattacks to pursue national political purposes,* has been gaining ground since at least the attack against Estonia in 2007. Moreover, there is also a competition between states seeking to find ways to gain *strategic advantage* through cyberspace that is to use cyber intrusions and cyberattacks in order to influence the "overall relative power relationship of opponents that enables one nation or group of nations effectively to control the course of a military or political situation". [2: 522] This broadening of the activities of nation states in cyberspace necessitates a novel, more systematic approach beyond military planning, more akin to traditional statecraft and strategic art. Consequently, both in the emerging academic strategic literature and in the evolving politico-strategic thinking of the nation states, the nature of cyberspace and its strategic implications are being widely appraised.

The Evolving Concept of Cyberspace as a Strategic Environment

Cyberspace as a *strategic environment* has distinctive features with still plenty of *known and unknown unknowns.* [3] It is to a large extent a hidden landscape both literally, due to the attribution challenge and the technical complexities, and in terms of strategic thinking, as a result of the fast-paced development of the technology and the nascent strategic thought trailing behind it, but also to the particularly strong secrecy surrounding the cyber activities of the nation states. As national cyber strategies are gradually formulated and simultaneously tested also in real life, these tests and incidents yield pragmatic lessons on the nature and the limitations of distinctive national approaches. The recent events of Russian influence operations during the U.S. presidential elections served as the latest reminder of how distinctive this comprehension can be.[5] One aim of this study series is to examine if the traditions of national strategic thinking.

---

[4]   See, for example: KHALILZAD, Z., WHITE, J. P., MARSHALL, A. W.: *Strategic Appraisal. The Changing Role of Information in Warfare.* Santa Monica: Rand Corporation, 1999. Also: HUNT, E.: U.S. Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34 3 (2012), 4–21. NYE, J. S. Jr.: Nuclear Lessons for Cyber Security? In. *Strategic Studies Quarterly.* Washington, D.C.: Air University Press, 2011.

[5]   As for the identity and purpose of the Democratic National Committee (DNC), hackers and leakers, there still are some dissenting voices. Based on the joint U.S. intelligence community reports published in December 2016 and January 2017, the author of this article adopts these as proven facts.

In addition, scholars can also have more insight into how cyberspace or the information environment is gaining *strategic sense,* and how it affects the way international conflicts and rivalry take place. At the heart of these strategic discussions, one of the questions splitting Western academic strategists is: to what extent generic strategic theory—and its major concepts like deterrence—is applicable in cyberspace. According to, for example, Colin S. Gray a most renowned British classic strategic theorist, the nature of political power and rivalry remains the same, thus the traditional premises of strategic theory are also applicable in cyberspace. [3]

In light of these tendencies, despite its technological superiority, the U.S. susceptibility and inept response to the 2016 Russian influence operations constitutes an excellent case study of how nation states seek to integrate cyberspace into their strategic thought. In other words, how they intend to maximize their chances to exploit the opportunities in cyberspace in order to realize their national interests; how they perceive threats coming through cyberspace and how they try to neutralize or eliminate them; and also how these distinctive approaches play out against each other. This time, Russia did manage to take the most advanced cyber nation off guard and exert some influence over the integrity of its core democratic political institution. The assumption of this article is that the Russian strategists recognized and exploited the opportunity offered by the inherent technical determinants of cyberspace, as well as the strategic, legal and institutional and doctrinal incoherence and imbalances of the U.S. thinking.

Moreover, although the operationalization of (cyber) informational power in Russian strategic thinking is indeed fundamentally different from the Western approach, the recent developments also prove the long-running knowledge in strategic communities that Russian strategists are "good Clausewitzians" to be true also in cyberspace. As James J. Wirtz from the Naval Postgraduate School puts it, they understand that war is a political act, hence "quick to think through the links between technology, military operations, strategy, and ultimately political outcomes, despite their lack of technological dexterity". [4: 32] Meanwhile, the U.S. seems to carry on the same deficiency as in its kinetic strategic thought. According to a U.S. expert's recent comment, "America's primary weakness is not in its lack of economic or military power, but in a failure to formulate strategy and, frankly, poorly informed decision-making, even when faced with a peer nuclear power. Military capability in and of itself will not fix these cardinal weaknesses in judgment, nor make up for a lack of vision and political will to see hard choices through". [5]

Several guidebooks and manuals have been published recently on national cybersecurity strategy models. In these, crisis management and contingency planning, information assurance, and resiliency are central organizing elements. In this article the focus is different. We argue that the election-time influence operation revealed that there should be an urgent shift in national cyber security thinking informed by the logic of general strategic thinking. Through the example of the American response measures, our aim is to ascertain some of the new strategic challenges in cyberspace including a powerful and assertive adverse nation state. To this end, we contextualize the events in terms of the relevant American and Russian strategic documents and policy statements. According to the logic of strategic theory, national capabilities, cyber or other, have a relative value and must be appraised in relational terms. Examining the events through a strategic lens will yield some insight into first, how historically distinctive strategic cultures determine cybersecurity strategy formation, second,

how surfacing strategies materialize in practice, and finally, how the resulting action–reaction cycle plays out in cyberspace.

Accordingly, first we apply the basic concepts of strategic theory to cyberspace and cybersecurity. The objective here is to identify the strategic dilemmas of the U.S. response and more broadly, the strategic planning approach in its national cybersecurity efforts. Then, the study will trace back the roots and the strategic repercussions of the idea of strategic cyberattacks in the U.S. In Part 2, the U.S. cybersecurity thinking is examined in terms of deterrence theory and practice. In the kinetic realm, conventional military and strategic nuclear power are pivotal means of deterrence. As the case study in this article reveals, in cyberspace, though it proves to be a much more daunting task, some experts and practitioners even doubt if this is possible at all. Closely related to deterrence, the Russian hacking case adds some lessons on the strategic importance of attribution, as well. To conclude, we sum up the strategic lessons of this case study and make some recommendations accordingly. An upcoming third part of this article intends to highlight in the same vein the major differences concerning U.S. and Russian threat perception in their respective approaches to the strategic use of cyberspace.

Baseline Definitions

Cyber related concepts are still fluid in national security thinking. Even within one policy area, like the military or homeland security, there is a multitude of strategic documents often with inconsistent terminology, which well reflects the fundamental stumbling block of U.S. strategy development in cyber issues. There is a general effort to centralization and unification within each policy area, as well as at the highest overall national security level. Cyber threats pose security threats of a new character that demand strategic level adaptation, but the nature of national security dynamics, however, have not changed because nation states are pursuing strategic goals in cyberspace, just like in other domains. In this study, we will use working definitions that are closest to strategic theory.

Cyberspace

Cyberspace as a working concept here is understood *as part of the overall strategic environment* in which nation states define their ways, ends, and means. In order to better understand the strategic value of cyberspace, the physical, logical and socio-political components have to be considered as an integrated whole. In the evolving strategic studies of cyberspace, the most common model derives from the fusion of a simplified Open Systems Interconnection (OSI) model that characterizes and standardizes the communication functions of a telecommunication or computing system, and a cognitive layer. In 2007, Martin Libicki divided cyberspace into three layers: physical, syntactic and semantic layer. [7] The fourth cognitive or politico-strategic layer encompasses all the actors and their different motivations interests and strategies—military, civilian, commercial individuals, organizations and nation states—who use cyberspace to achieve their goals.

The notion of cyberspace in the U.S. strategic and national security documents has underwent an unsynchronized evolution. Militarily, initially it only appeared publicly in Information Operations documents and it was limited to the technical that is the physical and the syntactic layers. In addition, cyberspace originally constituted only a subfield of the *information environment* and cyber offensive operations constituted one element of military information support operations. However, it has gradually acquired an independent status as a separate domain of operations alongside land, sea, air and space. The first independent doctrine on cyberspace appeared in 2006 entitled *The National Military Strategy for Cyberspace* that treated cyberspace only in terms of its physical components used by the military to implement military operations

In the wider national security context, cyberspace has also evolved gradually but starting out of a purely infrastructural approach. The first seminal occurrences of the vulnerabilities and threats was the Commission on Critical Infrastructure Protection (PCCIP) in 1997. Ever since then, the national security thinking is centred on the cyber security or the physical safety of the infrastructures.[6]

Cyberattack

As of today, in the U.S. there is no official legal definition of a cyberattack. The evolution of the concept of cyberattack in different U.S. strategic documents will be discussed in detail later on. For the purpose of this study, a generic definition of a cyberattack is used taken from one of the most often cited academic sources, the National Research Council's report entitled *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* According to the report, a cyberattack "refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks". [6: 1] This approach is in line with the official U.S. position that does not recognize unauthorized access to computers, or in other words espionage in itself as an attack.[7]

Cybersecurity Strategy

The strategic implications of cyber conflict reach beyond and across the military, intelligence and economic sectors—extending into the high-policy realm of diplomacy and statecraft. Cyberspace at nation-state level is governed by "economic laws of rival resources" and "laws of sovereign jurisdiction and control". [8: 3] Attacks from the physical and semantic layers impact power at the politico-strategic level, while control at the political layer have effects at the other two. Therefore, cybersecurity strategy must follow the logic of national security strategy: "The art and science of developing and using the political, economic,

---

[6]   For example, in 2009 the *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)* defines cyberspace: "as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." [21]

[7]   The report designates such penetrations as *exploitation.*

social-psychological, and military powers of the state in accordance with policy guidance to create effects that protect or advance national interests relative to other states, actors, or circumstances." [9: 1]

Strategic Planning in Cyberspace

Generic strategic theory is the academic literature on how to *think about* national (security) strategies. Consequently, in this study the strategy formulation model of the U.S. Army War College will be used as an analytical framework to evaluate the evolving U.S. strategic thought and security policy in cyberspace. [9]

In the following section, the most important premises of strategic theory are outlined. Strategic theory applies a holistic and integrative approach. Formulating strategy at the highest levels of the state, that is at grand strategic or the national security level is: "a process that seeks to apply a degree of rationality and linearity to circumstances that may or may not be either. Strategy accomplishes this by expressing its logic in rational, linear terms—*ends, ways, and means.*" [9: 1]

Strategic planning has essential building blocks and an established, coherent procedure. If any of these is missing or not appropriately presented, the national cybersecurity process will stumble:

"From an accurate analysis of the strategic environment, the strategist *determines the threats to and opportunities* for the advancement or protection of these interests. From *policy,* the strategist receives the political leadership's vision, guidance, and priorities of effort in regard to interests. Thus, in constructing a valid strategy, the strategist is bounded by the nature of the strategic environment, the dictates of policy, and the logic of strategy." [9: 73]

Policy dominates strategy by the articulation of the end state and its guidance regarding resources, limitations on actions, or similar considerations. "Strategy cannot be formulated in a policy or intellectual vacuum." [9: 9] Strategy is hierarchical. The political leadership ensures and maintains its control and influence over the instruments of power through the hierarchical nature of state strategy. Clarity and precision are the essentials of a strategy to provide strategic purpose and unity of direction.

"The role of the strategist is to exercise influence over the volatility, manage the uncertainty, simplify the complexity, and resolve the ambiguity, all in terms favourable to the interests of the state and in compliance with policy guidance." [9: 18]

The strategic environment has a predominant role in strategy. In order to best serve purposes of a national strategy at the highest-level *cyberspace* must be considered in its broadest sense. In strategic theory the strategic environment incorporates: "[t]he internal and external context, conditions, relationships, trends, issues, threats, opportunities, interactions, and effects that influence the success of the state in relation to the physical world, *other states and actors, chance,* and the possible futures. […] the role of the strategist is ultimately to advocate actions that will lead to desirable outcomes while avoiding undesirable ones, *the strategist must understand the nature of the environment in order to exert influence within it*". Strategy is subordinate to the nature of the environment. Strategy must identify an appropriate balance among the objectives sought, the methods to pursue the objectives,

and the resources available within the particular strategic environment. Strategy must be consistent with the nature of the strategic environment. [9: 17–18; 66]

"The true purpose of strategy is to create favourable effects in support of policy goals for the advancement or protection of national interests. *Strategic effects* are the impact that the accomplishment of strategic objectives has on the environment. Effect flows from strategic performance—the synergy of the objective(s) achieved, the concept(s) employed, and the resources used." [9: 45]

"In strategy formulation, getting the objectives (ends) right matters most! Objectives are the true focus of strategy formulation and, if not properly selected and articulated, a proposed strategy is fundamentally flawed and cannot be effective." [9: 49]

Strategy rests upon the ends, ways and means structure. "Objectives (ends) explain 'what' is to be accomplished. Strategic concepts (ways) answer the big question of 'how' the objectives are to be accomplished by the employment of the instruments of power. They link resources to the objectives by addressing who does what, where, when, how, and why, with the answers to which explaining 'how' an objective will be achieved. […] Resources (means) in strategy formulation set the boundaries for the types and levels of support modalities that will be made available for pursuing concepts of the strategy. In strategy, resources can be tangible or intangible." [9: 69]

The notion of power is a central idea in political science and international relations, military studies and strategic theory, but it has a distinctive meaning in all three. In political science the concept of power has gone through many transformations since pre-WWII times. In essence, it is about influence and control over resources, or directly or indirectly over another party or more broadly over the circumstances of the given situation. As Lawrence Freedman eloquently determines strategy focuses on interplay and balance between the strategic environment, the desired end state and the choice of the right instruments and elements of power:

"The realm of strategy is one of bargaining and persuasion as well as threats and pressure, psychological as well as physical effects, and words as well as deeds. This is why strategy is the central political art. It is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power." [10: 12]

In U.S. military theory, by contrast, *cyber power* is equivalent to military capabilities and power projection in a given natural domain like air, sea or land, or in case of cyber, the cyber domain. Strategic theory combines the political and military understanding of power: elements (capabilities) and instruments of national power that are employed in order to exercise control over the strategic environment to achieve the desired end state.

"Capabilities refer to the set of resources and assets the state possesses that increase its potential (capacity) to carry out its aims. In conventional warfare terms, capabilities are measured by factors like the country's population, industrial capacity, technological advancement, or the size of its military forces. In cyberspace, capabilities refer to the state's resources and assets that help it achieve its goals in cyberspace such as numbers of hackers, the level of expertise in computer science, and malware sophistication." [11] Power is measured by the actual influence exerted or the outcomes brought about. The strategic purpose of cyber power is to achieve policy objectives.

Strategic theory is related to but different from strategic culture as a discipline. Nevertheless, the theory acknowledges that distinctive national history, culture and worldview all play an

important role in strategy formulation. For example, "Western thinking is permeated with the binary logic inherent to Western scientific thought. Binary logic is rooted in Aristotle's philosophical law that something is either A or 'not A.' It cannot be A and 'not A.' It is either true or false. Thus in Western science, math, logic, and much of culture, we assume a world of blacks and whites that does not change—this is bivalent logic—two-valuedness". [9: 43]

The 2016 U.S. Elections and the Russian Influence Operations

The events during the latest U.S. presidential elections is illustrative of the technical, institutional and strategic cultural aspects that might hinder the development of an effective cybersecurity strategy. Detailed analysis of all the U.S. cybersecurity documents is beyond the scope of this study. Instead, in Table 1 the relevant U.S. public statements, marked in bold italics against shaded background, are enlisted in chronological order along with the timeline of the election meddling events. This format enables a quick overview of both the flow events and how they impact the publication of policy statements that try to strategize response mechanisms to a cyberattack. It also helps to elucidate the fact that cyber security strategic planning is at an early phase of progress, still leaving several major strategic gaps unresolved.

Table 1. *A chronology of key events and U.S. strategic documents and policy statements.*
[Edited by the author.]

May 2011	White House: International Strategy for Cyberspace
July 2011	DoD Strategy for Operating in Cyberspace
September 2012	DoD: International Law in Cyberspace. Harold Hongju Koh, DOS legal adviser's statement
2013	DoD Defense Science Board Study: Resilient Military Systems
2013	White House, Presidential Policy Directive (PPD) 21 entitled Critical Infrastructure Security and Resilience
2013	Cyberspace Operations, Joint Publication 3–12(R)
1 April 2015	White House: Executive Order 1396 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"
April 2015	DoD: The National Military Strategy of the United States of America
15 April 2015	DoD Cyber Strategy
5 June 2015	DoD Cyber Command: The Commander's Vision and Guidance for U.S. Cyber Command: Beyond the Build. Delivering Outcomes through Cyberspace
12 June 2015	Law of War Manual—United States Department of Defense
18 December 2015	White House Report to Congress on Cybersecurity Deterrence
March 2016	Department of State International Cyberspace Policy Strategy
Hacking Incidents Start to Appear in Public	
14 June 2016	The Washington Post revealed that "Russian government hackers" had penetrated the computer network of the Democratic National Committee. Crowdstrike technical report published on DNC hacks.
15 June 2016	Guccifer 2.0 crops up in a BlogSpot.

20 June 2016	Mandiant and Fidelis confirmed Crowdstrike's initial findings that Russian intelligence indeed hacked the DNC.
July 2016	Officials announce that the Illinois state online voter registration system is to be shut down following a hack.
13 July 2016	Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues U.S. Department of State Before the House of Representatives Committee on Oversight and Government Reform Subcommittees on Information Security and National Security Hearing on *Digital Acts of War: Evolving the Cybersecurity Conversation.*
13 July 2016	DNC intruders leaked selected files exclusively to The Hill, a Washington outlet for Congress.
22 July 2016	After Trump was officially nominated and before the Democratic National Convention got under way, WikiLeaks published more than 19,000 DNC emails with more than 8,000 attachments.
26 July 2016	PPD–41 Presidential Policy Directive *United States Cyber Incident Coordination.* The directive called for a renewed National Cyber Incident Response Plan that defines a nationwide approach to significant cyber incidents, including threat level assessment and outlines the roles of both federal and non-federal entities.
29 July 2016	Democratic Congressional Campaign Committee (DCCC) server compromise revealed in press. DCCC organizes campaign finances.
1 August 2016	Shadow Brokers announces they hacked National Security Agency (NSA) and stole cyber weapons which they want to sell at auction.
18 August 2016	FBI issues warning of foreign hackers penetrating voter registration database and state election computer systems in Illinois and Arizona.
4–5 September 2016	At the G20 Summit Obama urged Vladimir Putin not to let cyberspace become the "wild, wild west" and "to cut out" cyber intrusion. Obama called on Russia to "act responsibly and start instituting norms" to avoid a Cold War-style escalation, and issued warning that America had "more capacity than anybody, both offensively and defensively".
30 September 2016	*Draft National Cyber Incident Response Plan* is out for public discussion, still in need of codification.
7 October 2016	*Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* designates Russia, saying hacks of U.S. political groups and individual politicians could only have been done with the authorization of "Russia's most senior" officials and that its intent was to undermine the integrity of the election.
15 October 2016	Joe Biden said in an interview that the U.S. is ready to hit back to Putin. "He'll know it", Mr. Biden added. "And it will be at the time of our choosing. And under the circumstances that have the greatest impact."
30 October 2016	The Shadow Brokers claims that the 306 domains and 352 IP addresses revealed in the dump belong to the Equation Group.
8 November 2016	Presidential elections.
10 November 2016	*International Law and Stability in Cyberspace.* Brian J. Egan, DOS legal adviser statement
9 December 2016	The Washington Post leaked that the Central Intelligence Agency (CIA) had assessed that Russia interfered in the election to tilt the election to Trump. Investigation announced by Obama, POTUS vowed on Friday to "send a clear message to Russia" as both a punishment and a deterrent imposing cost.

16 December 2016	Obama explains at the end-of-year news conference the White House perspective on how to handle the hacks. He says: "And so in early September, when I saw President Putin in China, I felt that the most effective way to ensure that that didn't happen was to talk to him directly and tell him to cut it out, and there were going to be some serious consequences if he didn't. […] But the leaks through WikiLeaks had already occurred. […] We allowed law enforcement and the intelligence community to do its job without political influence. […] With respect to response, my principal goal leading up to the election was making sure that the election itself went off without a hitch, that it was not tarnished, and that it did not feed any sense in the public that somehow tampering had taken place with the actual process of voting."
22 December 2016	Intelligence Committee releases declassified Snowden Report.
29 December 2016	The State Department declared 35 Russian government officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco "persona non grata". Treasury sanctions on individuals for malicious cyber-enabled activities. Joint Department of Homeland Security (DHS), Office of the Director of National Intelligence (ODNI), Federal Bureau of Investigation (FBI) Statement on Russian Malicious Cyber Activity. The Department of Homeland Security and the Federal Bureau of Investigation are releasing a *Joint Analysis Report* (JAR) that contains declassified technical information on Russian civilian and military intelligence services' malicious cyber activity. The President has approved an amendment to Executive Order 13964. National Defense Authorization Act for Fiscal Year 2017 approved.
5 January 2017	Directors Clapper and Rogers testified before Congress about the Russian campaign.
6 January 2017	ODNI Declassified report *Assessing Russian Activities and Intentions in Recent U.S. Elections*. The Analytic Process and Cyber Incident Attribution. The review prepared by CIA, FBI, and National Security Agency officials explicitly stated it couldn't determine the effect of the suspected Russian influence campaign on the election process.
12 January 2017	Shadow Brokers tries to sell the hacked cyber weapons again.

Domestic Strategic Environment: Organizational Hindrances of Strategic Planning in Cyberspace

Due to the large number of diverse stakeholders involved, cybersecurity policy is like a multi-dimensional chess play. The ubiquity and the proprietary nature of the potential targets of a cyberattack causes fuzzy scope of jurisdictional responsibilities and policy priorities for strategic level cyber defence. The White House is responsible for the security and the advancement of vital U.S. interests, thus they should provide political coordination and clearly articulated policy guidance at the top of the strategic hierarchy. However, as of today, the U.S. does not have a single cybersecurity strategy. Cybersecurity strategy formulation is a process overarching several policy areas: national security, homeland security and public order. Strategic planning—currently in the phase of risk assessment, vulnerability and threat assessment, and strategic concept development—evolves in parallel in these different policy areas, as well as at state and local levels in accordance with the inherent legal frameworks and institutional culture of each field. Nevertheless, the Obama Administration has taken several substantial steps to further develop an overarching, coherent and more transparent policy approach built on the preliminary cybersecurity measures going back to the 1980s.

Ends, Ways and Means

In cybersecurity governance the homeland security, law enforcement and national security fields are inseparably intertwined. The domestic security authorities are regulated by a patchwork of *domestic laws* which include the Constitution of the United States, federal statutes, and self-executing treaties. This legal framework obliges both government institutions and private individuals, and regulates the division of labour between departments and agencies. According to the Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government: "responsibility for Federal Government cybersecurity is distributed and shared by all agencies; however, specific agencies have additional roles in supporting this mission and ensuring that the Federal Government has the tools, resources, and guidance necessary to make the risk-based decisions necessary to secure their systems. FISMA[8] states that OMB[9] oversees Federal agency information security policies and practices. The OMB Cyber and National Security Unit (OMB Cyber) was created at the beginning of FY[10] 2015 to strengthen Federal cybersecurity." [12: 6]

These are vying for funding with their own distinctive institutional culture. Moreover, a unified strategy has to be accepted and approved by governmental entities at lower levels too, and also by the private sector. Cybersecurity management to a large extent happens at the state level, and any centralization would mean giving up on some of those local prerogatives. For example, in February 2017, New York was the first and so far the only U.S. state to introduce its own cybersecurity policy with some mandatory regulations. Beyond the inherent vulnerability of information technology devices, these proprietary and legislative features make cyber security strategy a daunting task, and constitute a constant vulnerability. As the Russian influence operation demonstrated, even without any destruction or major disruption, significant confusion can be triggered.

Viewed from a strategic lens, the identification of ends, ways and means are far from being sorted out. *Ends* (what to defend) is one of them. The critical infrastructure protection scheme emerged in the mid-1990s due to the realization of the growing dependency on information infrastructures and the risks thereof. It provides the federal government with overarching regulatory authorities in certain vital industries. Twenty years later, basic concepts of the scheme are still contentious. In 2015, the Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government orders the prioritized identification and protection of high value information and assets. In the second part of 2016, the Presidential Commission on Enhancing National Cybersecurity was convened to develop policy recommendations for the next administration. Accordingly, the commission interrogated critical infrastructure owners on what is vital to keep the national economy functioning during a large-scale cyberattack. During the Obama era, the linchpin of the process was established in 2013 via the Executive Order 13636 entitled *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21 *Critical Infrastructure Security and Resilience* which set out steps to strengthen the security and resilience of the Nation's critical infrastructure.

---

[8]   Federal Information Security Management Act.
[9]   Office of Management and Budget.
[10]   Financial year.

PPD–21 re-aligned and updated the HSPD–7[11] critical infrastructure sectors established in 2003, and reduced the number from 18 to 16.[12] Election and voting systems, though were designated as critical infrastructure only after the election hacks in 2016. In addition, it is for the first time that critical infrastructure dependency risks are examined in practice. A large-scale three-year long research is carried out at the Idaho National Laboratory of the Energy Department to map the likely ripple effects and the physical impacts of hacks. Similar tests have been initiated to examine how energy sector grid hacks might affect military readiness. [13]

Ways (who does what, where, when, how, and why) is especially problematic in the domestic cybersecurity environment. As we will see in the next chapter, legislation and the White House tend to apply deterrence as an umbrella strategy in an attempt to achieve strategic unity. Homeland security—risk management and incident response—and law enforcement tools serves as deterrence by denial, and cost imposition. Once these remits are decided all the way through, the question of *means* (resources) also becomes clearer. During the 2016 elections, the Democratic National Convention's servers are owned by the party, and the ownership and operation of election machines fall under state autonomy. Even when the cyber intrusion was revealed, there was no regulation in place concerning inter-agency cooperation and information sharing. Figure 1 serves as an illustration of the fragmented cybersecurity decision making authorities at the top-end of the executive branch.
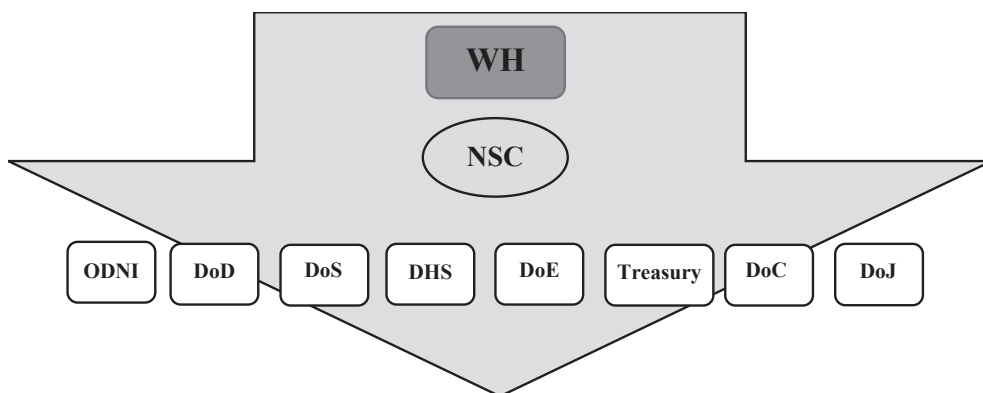
Figure 1. *Politico-strategic cyber security planning at the executive level.*[13]
[Created by the author.]

---

[11] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. See: www.dhs.gov/homeland-security-presidential-directive-7

[12] Presidential Policy Directive 21 (PPD–21) on Critical Infrastructure Security and Resilience identifies 16 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems.

[13] *Legend:* WH = White House; NSC = National Security Council; ODNI = Office of the Director of the National Intelligence; DoD = Department of Defense; DoS = Department of State; DHS = Department of Homeland Security; DoE = Department of Energy; DoC = Department of Commerce; DoJ = Department of Justice.

First, the underlying dilemma starts at the issue of what are the thresholds for government-level response. The methodology for assessing the effect of a cyberattack campaign, and calculating an unacceptable level of "damage" after which the critical cyberattack threshold will be crossed is still evolving. The federal government is primarily responsible for its own governmental networks. Beyond that, it takes first-order responsibility for national security level threats that constitute a *significant cybersecurity incident* in the official parlance. The notion of a major cybersecurity incident was first determined in a memo for the federal agencies by the Office of Management and Budget in 2007. OMB is the largest office within the Executive Office of the President, and it issues the Federal Information Security Management Act guidance, the key point of reference for homeland security planning. The guidance of 2014, based on U.S. CERT National Cyber Incident Scoring System defines *incident* as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." An updated version of 2015 defines a *major incident* as one that:

- Involves information that is classified or "controlled unclassified information", a broader category that includes proprietary information, intellectual property, trade secrets or personally identifiable information.
- Affects at least 10,000 users and is not "recoverable" (for example, sensitive data is exfiltrated from agency systems and publicly posted online. Or, the time to recover is unpredictable or would require additional resources.)
- Causes an agency to lose the ability to provide a critical service to at least some users. A "high-functional" impact, meanwhile, describes an incident in which an agency loses the ability to provide *all* critical services to users.
- Involves the exfiltration, modification, deletion or any other type of unauthorized access of information or system. [14]

There are seven levels of severity based on the impact caused and the recoverability and dependency of the systems affected. The Obama presidency got one step closer to categorizing the national security levels of cyber incidents in the U.S. Cyber Incident Coordination presidential directive issued on 26th July 2016. It also uses the same terminology and scoring system. Under the directive, all major incidents that is those in the top three categories are also considered *"significant cyber incidents,* meaning they are likely to result in *demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties or public health and safety of the American people.* These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors as appropriate." [15] Another factor seems to influence governmental intervention, when the attacker is verifiably a nation state. Obama regularly refers to this as a pivotal part of the calculation. In that case, international law kicks in as the regulatory norm. The next chapter examines international law considerations.

	General Definition		Observed Actions	Intended Consequence[1]
Level 5 Emergency (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.		Effect	Cause physical consequence
Level 4 Severe (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.			Damage computer and networking hardware
Level 3 High (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.		Presence	Corrupt or destroy data
				Deny availability to a key system or service
Level 2 Medium (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.		Engagement	Steal sensitive information
Level 1 Low (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.			Commit a financial crime
Level 0 Baseline (White)	Unsubstantiated or inconsequential event.		Preparation	Nuisance DoS or defacement

Figure 2. *Incident scoring in the PPD–41 Presidential Policy Directive "United States Cyber Incident Coordination".* [20]

According to these measures, the 2016 Russian hacking meets the standard for a significant cyber incident, as there has been demonstrable impact to public confidence and foreign relations.

Secondly, it is blurred to what extent cybersecurity is a civilian or a military responsibility. Currently, cyberattack response is predominantly a civilian law enforcement, counterintelligence and incident response procedure, combined with a (voluntary) regulatory framework serving defence and resilience[14] purposes. In baseline terms, the Department of Homeland Security is responsible for the dot.gov cybersecurity and the public-private partnership with critical infrastructure stakeholders. Meanwhile, the information security technical expertise in the civilian sector is split between the Department of Homeland Security where the US–CERT resides, and the Department of Commerce through the mandate of the National Institute of Technology that is authorized to elaborate voluntary cybersecurity frameworks.

---

[14]   In generic terms resilience is the ability to quickly restore the original shape after an attack. It is an integral part of Information and Communication Technology security incident management and homeland security. Fast recovery limits potential gains and can convince an opponent not to attack.

The U.S. Cyber Incident Coordination presidential directive issued on 26th July 2016 institutionalizes a whole-of-government approach: the directive designates the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, as a lead agency in charge of responding to cyber threats, meaning investigation and prosecution, against the United States agencies or companies. When cyber incidents occur, the Department of Homeland Security provides assistance to potentially impacted entities, analyses the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents. [16]

At the level of industry, during a real-world attack on the grid, the Department of Energy would be responsible for collecting, evaluating, and sharing information on our energy infrastructure, as well as working with Federal, state, and local entities and industry to help facilitate the restoration of damaged energy infrastructure. (DARPA is interested specifically in an early warning of impending attacks, situation awareness, network isolation and threat characterization.)

The Director of National Intelligence (DNI) assists in aggregating analysis of threat trends, and helps "to degrade or mitigate adversary threat capabilities". [16] The Department of State can reach out through diplomatic channels directly to foreign governments where the source of the attack is located. In the aftermath of the Sony attack, on 1 April 2015 Obama issued an executive order entitled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* The Treasury has the authority to levy sanctions against those charged with cyber felony receiving advice from the Department of Commerce and the Office of the U.S. Trade Representative.

Since the 1980s and increasingly from the early 2000s the FBI, endowed both with counterintelligence and law enforcement authorities, has been the lead federal agency for investigating cybersecurity incidents. During the Obama Administration, the cybersecurity remit of the Department of Justice (DoJ) has been extended considerably. John Carlin the head of the DoJ's National Security Division said the coordinated national security investigative and prosecution process and all source intelligence and attribution capability within the DoJ is essential, and these are pieces of a new deterrence strategy. Carlin described the national security investigations procedure—that was established in reaction to 9/11 attacks through the USA PATRIOT Improvement and Reauthorization Act—that it: "seek to harness and coordinate the authorities and capabilities of all members of the national security community, state and local law enforcement, and foreign law enforcement and intelligence partners, and may result in a wide variety of national security activity, including […] arrest and prosecution of perpetrators, imposition of economic sanctions, diplomatic overtures to foreign governments, and actions undertaken by U.S. intelligence services or armed forces overseas." [17]

DoJ is responsible for both national security and cyber economic espionage investigations, attribution and prosecution. Carlin also linked their task to the globally promoted U.S. norms on acceptable behaviour in cyberspace which are enforced by this cross-border law enforcement procedure.

DoD's Role in Cyber Defence

The public debate about the role of the Department of Defense in national cybersecurity has been ongoing for more than a decade. There are signs on the part of the legislative and executive authorities to be inclined to delegate more role to the military. Along with the extended scope of the DoJ and international norms discussed in the next chapter, the military constitutes the other major source of deterrence. When the 2011 DoD Strategy for operation in Cyberspace was issued, the DoD was only responsible for the cybersecurity of the dot.mil domain. As set by domestic law, the military can only provide *assistance* to domestic civilian authorities in special cases related, for example, to counterterrorism, WMD or cybersecurity. DoD has developed and issued key *Defense Support of Civil Authorities,* however, DoD guidance does not clarify the specific roles and responsibilities of key DoD entities that may be demanded to support a cyber incident.

There has been a considerable change in the DoD's role conception after 2012, when in August Saudi Aramco was smashed by a massive cyberattack, and later in September several Wall Street banks were also hit by a series of DDoS attacks for over a week, and the attacks stopped completely only in spring 2013. Since then, a more direct role is articulated for the military in critical infrastructure protection. As of today, the military is also involved in civilian cybersecurity exercises and also in strategic planning, most notably in the yearly Cyber Guard exercises that has shifted from a whole-of-government to a whole-of-nation approach. In the 2015 DoD Cyber Strategy it is one of the five strategic objectives to "be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence". [18: 14] The Strategy also identifies a role for the four groups of mission forces of which the 13 "National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence", thus, they will help defend the nation's critical infrastructure. [18: 6] Unambiguously, the DoD possess the highest level of aggregate cybersecurity expertise both in qualitative and quantitative terms. In the U.S., however, there is a statutory restriction, the so-called Posse Comitatus Act, concerning the employment of the military force on the homeland in peacetime. Rather, it is the National Guards who can operate more freely at local levels, and who will have a major role in cyber defence if it is necessitated. Most national security strategic documents determine this as the last resort.

In December 2015 the White House Strategy on Cyber Deterrence was delivered. It had been commissioned in 2013 by Congress in the *National Defense Authorization Act,* with the purpose of outlining how the United States will respond to cyberattacks. It came out almost two years late, and between April and December 2015 informally the DoD strategy was regarded as a kind of interim national cybersecurity strategy. Another strategic ambition running parallel to national cybersecurity is the full integration of cyber capabilities into military operations and deterrence. Cyber Command have been boosted to more than 6,000 troops and cybersecurity budgets, although precise chapters are indiscernible, have multiplied. In the military strategic context, designated cyber troops are intensively building technical, tactical and C2 operational skills. Rules of Engagement are still in progress, and they are largely classified. In 2016, the DoD launched a task force to explore ways, in which offensive cyber capabilities could provide support to strategic objectives with results to be expected when cyber forces become fully operational. Its mandate is to find ways to

operationalize offensive operations: "[T]he role of full-spectrum cyberspace operations in supporting shaping, deterrence, constrained military objectives, and full-scale conflict is not adequately appreciated or understood. It is the principal objective of this TF to investigate the opportunities for, and limitations of, offensive cyber capabilities in support of overall U.S. strategy and provide actionable recommendations to enhance those capabilities." [19: 32]

The Delicate Balance of Public-Private Partnership

Third, the division of labour between the federal government and private sector actors in cybersecurity is still unsettled. Both parties are still hesitant about the degree of responsibility they are willing and able to take for cybersecurity. The executive branch and private sector relationships are entangled but crucial in any sincere cybersecurity efforts. One of the first and best known exercises examining the issue of strategic information warfare was the 1996 RAND "The Day After" desktop exercise and the following report characterizes the federal government's role as part leadership and part partnership with the domestic sector. Similarly, President Obama and leading DHS cybersecurity officials emphasize that in private sector cybersecurity the government has only an enabling role, providing the private sector with the necessary guidance, early warning and information, incident management assistance and incentives to assist in risk management. In the federal government's discourse, cyberspace is an ecosystem with shared responsibilities. As an initial overture in 2011, the White House submitted a comprehensive cybersecurity proposal to Congress including obligatory cybersecurity standards and voluntary cybersecurity practices that could be required to be adopted by critical infrastructure owners, but it was rejected as a result of the powerful industrial lobby. It was a stark reminder that progress in this area is not just a technical regulatory issue, but rather a tough bargain. Later on, the President submitted several regulatory bills, but there has been little change in the basic stance of the industry's voluntary stance.

In 2016, during the Presidential Commission on Enhancing National Cybersecurity hearings, possible further solutions were gauged along the regulatory versus voluntary approach and the proactive prevention versus mitigation axles. One enabling policy is fostering information sharing between the private sector and public authorities, while ensuring liability protection and incentives. Despite several bills, confidence is still lacking towards federal agencies. The DNC preventing the FBI from having access to party servers is a good example. Extending the DoJ's investigatory and prosecutorial role was welcome by the business community, unlike the White House's Deterrence Strategy which was criticized for ignoring threats below the level of a significant cyber incident. Following in the footsteps of the 2013 NSA leak, the 2016 NSA hack and leak revealed exploit kits used by NSA to penetrate major IT vendors' products like Cisco or Fortinet, was another blow to the confidence of the private sector towards the government.

The Russian meddling and the increasing number of attacks prove to be a double-edged tactic. The distance between public and private actor views and interests seem to diminish. In this regard, there has been an important shift in the position of the government on the private actors' right to execute (active) defensive measures, even if not on hack backing back. This is a sign of opening up to the idea that the private sector has a major share in cyber power.

In May 2015, the Assistant Attorney General Leslie Caldwell announced plans for a guidance for industry on cyber defensive actions. Up until now, this has not materialized. The demand to legalize forms of self-help for the private industry is increasing. Business leaders and the U.S. Chamber of Commerce also put growing pressure on the administration to expand deterrence to cyber threats that do not rise to the level of warfare, but still cause considerable losses.

Conclusion

The article provides a snapshot of the regulatory and institutional environment of the U.S. cybersecurity back in 2016. U.S. cybersecurity as a national security issue area emerged gradually since the early 1990s, and later on, it was fully elevated to the highest level of strategic planning by the Obama presidency. In spite of supposedly having the most powerful cyber weapon arsenal, the U.S. strategic advantage in cyberspace is greatly diminished by the lack of a coherent and functioning cybersecurity policy. The U.S. is far not alone with this deficiency, however, this calls into serious doubt the ability and willingness of the state supposedly with the most powerful cyber capabilities.

Among the most serious problems, governance remains disjoint and weak all along the statutory, regulatory and enforcement levels. Efficiency would require a shift towards centralization and enforcement of regulations at the federal level, but the presidential orders and legislative acts do not go beyond the voluntary regulation for the private sector. Cyber defence of the federal departments and agencies is also still weak as the Office of Personal Management hack shows. On the other hand, there is some progress in the national incident response management plan and in the whole-of-the nation cyber exercises. Although there is some development towards a bigger role for the military, response mechanism short of war remains largely civilian.

References

[1]   Promises about Homeland Security on "The Obameter". *Politifact.com* (online), www.politifact.com/truth-o-meter/promises/obameter/subjects/homeland-security/ (Downloaded: 03.02.2016)

[2]   *Joint Publication 1–02. Dictionary of Military and Associated Terms.* Washington, D.C.: Department of Defense, 2007. https://marineparents.com/downloads/dod-terms.pdf (Downloaded: 03.02.2016)

[3]   GRAY, C. S.: *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle, Pennsylvania: Army War College Carlisle Barracks, Strategic Studies Institute, 2007.

[4]   WIRTZ, J. J.: Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In. GEERS, K. (Ed.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn: NATO CCD COE Publications, 2015.

[5]   KOFMAN, M.: The ABCs of Russian Military Power: A Primer for the New Administration. *The National Interest* (online), 2 February 2017. http://nationalinterest.org/feature/the-abcs-russian-military-power-primer-the-new-19299?page=5) (Downloaded: 03.02.2016)

[6]   OWENS, W. A., KENNETH, W. D., LIN, H. S.: *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: National Research Council of the National Academies. The National Academies Press, 2009.

[7]   LIBICKI, M. C.: *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007. https://doi.org/10.7249/CB407

[8]   NYE, J. S. Jr.: *Cyber power.* Cambridge, Massachusetts: Belfer Center for Science and International Affairs. Harvard Kennedy School, 2010.

[9]   YARGIN, H. R.: Strategic *Theory for the 21st Century: The Little Book on Big Strategy. U.S. Army War College Strategic Theory.* Carlisle: Army War College Carlisle Barracks, Strategic Studies Institute, 2006.

[10] FREEDMAN, L.: *Strategy: A History.* New York: Oxford University Press, 2013.

[11] CRAIG, T., VALERIANO B.: *How to Think about a State's Cyber Capabilities.* New York: Council on Foreign Relations, 2016. www.cfr.org/blog/how-think-about-states-cyber-capabilities (Downloaded: 20.12.2016)

[12] *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government.* Executive Office of the President, 2015. NIST Computer Security Resource Center (online). https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CSIP (Downloaded: 20.12.2016)

[13] STERNSTEIN, A.: If hackers cause a blackout, what happens next? *Christian Science Monitor* (online), 2016. www.csmonitor.com/World/Passcode/2016/1116/If-hackers-cause-a-blackout-what-happens-next (Downloaded: 20.12.2016)

[14] *US-CERT National Cyber Incident Scoring System.* www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System (Downloaded: 20.12.2016)

[15] *US-CERT Federal notification guidelines.* www.us-cert.gov/incident-notification-guidelines#impact-and-severity-assessment (Downloaded: 20.12.2016)

[16] *Cyber Incident Response.* Washington, D.C.: Department of Homeland Security, s.d. www.dhs.gov/cyber-incident-response (Downloaded: 20.12.2016)

[17] CARLIN, J. P. (2016): Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. *Harvard National Security Journal,* 7 (2016), 392–436.

[18] *Cyber Strategy.* Washington, D.C.: Department of Defense, 2015. www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Downloaded: 20.12.2016)

[19] *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.* Washington, D.C.: DoD Defense Science Board, 2013.

[20] *Presidential Policy Directive – United States Cyber Incident Coordination.* Washington, D.C.: The White House, Office of the Press Secretary, 2016.

[21] *Cybersecurity Office, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, D.C.: White House, 2009.

The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace

(Part 2)[1]

Dóra DÉVAI[2]

Given the technical, societal and international nature of cyberspace, national cybersecurity strategy formation demands a hybrid approach of homeland security and the more traditional national security processes. Moreover, as the series of the latest publicly known cyber incidents against the U.S.—the 2014 OMB espionage, the 2015 attack against Sony Pictures, the 2016 DNY attack or the Russian election hack and leaks—show, the dilemma of a proportionate response is a thorny technical, political and strategic task, while the need for a strategic level response is ever growing. Based on the analytical framework elaborated in the first part of this study series, the second part gives a strategic insight into the major determinants of the national response policy options to substantial cyberattacks against the U.S. The article also discusses wider strategic features pertaining to cyberspace, including strategic value of cyber weapons, threat perception, and national strategy cultures, which fundamentally impact cybersecurity and strategy formation.

Keywords: *U.S. cybersecurity policy, strategic culture, influence operations, cyber deterrence*

Major Technical, Operational and Strategic Considerations

In the U.S., responding to cyberattacks of substantial effects more actively and in a sustainable manner have been called for since the mid-2000s. Both policy and private sector communities have been demanding a national security level response instead of a cyber "Maginot-Line" style cyber defence comprising conventional software patches, intrusion detection and fire walls, or pure reactive cyber defence following incident management approach. The DoD introduced the idea of *active defence* in its 2011 strategy. Up till now,

however, active defence is still a very fluid concept running from situational awareness through deception to power projection and offensive cyber operations in cyberspace.

For quite a while, at the level of state-to-state relations, naming and shaming, a low-key instrument used to be the only explicit official reprisal applied by the administration. It was only after the Sony incident in late 2014 that a firm bipartisan consensus evolved that similar attacks cannot remain unanswered. In 2016, the White House's official reaction was criticized as too little and too late, but it did manifest a shift in official response. The next section will discuss those aspects that come into play when a response is considered thoughtfully.

Deterrence in Cyberspace

The need for a more strategic approach to cybersecurity first arose mainly in the academic and military expert circles. As opposed to the case-by-case, ad hoc crisis management, strategic thinking is anticipatory and pro-active, and synthetizes national interests and objectives. By 2008, as the opening citation in this article shows, President Obama's national security team realized the demand for a new policy and intended to meet it, though its attempts were often frustrated by Republican lawmakers and powerful commercial lobby interests in Congress. For the moment, the U.S. Government's official stance is that each response to a significant cyberattack will be examined on a case-by-case basis and it will combine the most suitable elements of national power. In Obama's words, we will respond at a "time and manner of our choosing". Still, the intention is broader than just neutralizing a given attack, and aims to contribute to deterring future attacks, as well. In generic terms, a cybersecurity strategy first and foremost seeks to avert substantial cyberattacks—or strategic effects caused by a cyberattack—by threat actors in a manner that is synergic with the overarching national security or grand strategy framework. The question of "how" *(ways)* is still an unsettled task. Deterrence is just one of several possible strategic concepts, along with alliances, reassurance, diplomacy and norm promotion, dissuasion, economic rewards and punishments.

Deterrence dominated Western strategic thought in the kinetic realm during the Cold War. Strategic nuclear and conventional military deterrence was considered a major tool to prevent large-scale kinetic attacks and maintain international peace and stability. Nevertheless, theoreticians have been arguing for long that this view focusing only on military threats and means to counter them is too restrictive. The feasibility of cyber deterrence is still contentious in many aspects. Cyber intrusions are extremely difficult to detect, and any computer system is inherently vulnerable. The attribution of the attack and the brandishing cyber offensive capabilities are problematic. Hence, the Cold War era model of deterrence was soon discarded as infeasible in cyberspace. [1]

Deterrence theory persists as the departure for cyber deterrence discussions. It consists of some basic principles: "…in order for deterrence to succeed, a deterrer should have sufficient capability, its threat should be credible. It is the adversary's perception and decision making that has to be affected: the cost-benefit calculations inherent in instrumental rationality are assumed to be present in decision situations involving deterrence. Deterrence is achieved if and when a potential attacker, fearing unacceptable punishment or denial of victory, decides to forgo a planned offensive. […] Most specialists have recognized at least two distinct

paths to deterrence: punishment or cost-imposition, and denial. The threat to impose costs in retaliation for a transgression obviously involves a negative incentive. But deterrence by denial also rests upon a form of negative incentive. The ability to resist and ultimately frustrate another actor's efforts can deny it any benefit while still leaving it with the costs of its efforts, again leading to a net negative outcome for the other side. A pure defense posture also does not aim to influence the other's decision; it accepts that an attack may occur and aims only to ensure the attack will not succeed." [2: 2, 38]

There is a tendency among the political elite, the Congress and the executive branch to treat deterrence in cyberspace as an umbrella term for all kinds of cybersecurity strategic ways. Conversely, it is still a question what role deterrence can play in cybersecurity, and what kind of deterrence strategy is the most feasible. In any case, one baseline step has crystalized that cyber deterrence needs to be broad or comprehensive. If deterrence is regarded as a strategic end in itself, then offence, defence and resilience are the ways to achieve it, through whole-of-government means (military, diplomacy, law-enforcement, resiliency, etc.). Deterrence by denial is gradually gaining more acceptance in cybersecurity strategies. It encompasses all forms of IT security measures, as well as any methods to improve resilience. Resilience is an elusive concept, but in general terms it means that once systems were knocked out, there are either redundant devices, and/or procedures in place to have them bounce back as quickly as possible. Cyber defence is no less elusive, as attack capabilities are developing at a neck-braking pace and it is almost impossible to keep up with. Cost-benefit calculations are always crucial in strategic planning, and given that deterrence by denial is extremely costly, this constitutes a huge obstacle in its wide and efficient application.

With the volume of damage growing, the need for alternative means of deterrence has remained in the focus of cybersecurity efforts. The military also started to reconsider viable options to deter cyberattacks. The prevailing argument in military circles was that offence is the best defence in cyberspace, as deterrence and defence are both infeasible. The officially published politico-strategic doctrines though—for example the 2011 Department of Defense (DoD) Strategy for Cyberspace or the 2011 DoD Report to Congress—were much more cautious and hardly mentioned offensive capabilities or intent.

Another problem with cyber deterrence is the very wide range of cyberattacks, as opposed to, for example, the range of nuclear attacks. Accordingly, the refinement of the unified Cold War deterrence approach is observable in cybersecurity strategy formulations. This is analogous with the methodology that Freedman determined as narrow deterrence. It is a form of deterrence narrowed down to retaliation against specific actors and certain weapons, and focuses on the protection of certain systems. For example, in 2013 the DoD's Defense Science Board (DSB) issued its study on Resilient Military Systems recommending deterrence as a necessary element of a cybersecurity strategy, but only as one complementary element of three other constituents, defence, resilience and offence. It recommended narrow strategic deterrence reserved only against the most menacing nation state cyber threats. [3]

Later, in April 2015 the DoD Cyber Strategy, still defensive in posture, pivoted on deterrence, mainly by denial, but the strategy also speaks about the use of offensive cyber operations much more explicitly then any time earlier, if the protection of the U.S. homeland and U.S. vital interests require. There is a new element, only mentioned in a half-sentence, which is the potential use of cyberattacks as a deterrent against threats from other domains. One set of strategic issues is whether cyberattacks can be used as a legitimate coercive means

not just in response to cyberattacks that is in-kind retaliation, but applied more broadly as a means of "cybered" deterrence.[3] The major argument for using cyberattacks as coercion is that it is bloodless and thus less damaging than a military attack.

The DSB also launched a specific cyber deterrence task force in October 2014 that concluded its report in March 2017 incorporating the experiences of the election meddling. It contains several ideas long having been circulated in academic circles, but occurring in public official reports for the first time. Hence, these parts represent a shift in official strategic thinking rather than real novelty in strategic studies. It furthers the idea of narrow deterrence. Most significantly, it acknowledges that: "a more proactive and systematic approach to U.S. cyber deterrence is urgently needed." [4] The report advocates offensive cyber and non-cyber responses with an unprecedented openness. Instead of a generalized deterrence strategy, the report recommends that deterrence be *tailored* to different adversary groups or specific adversaries (great powers: China, Russia; regional powers: Iran, North Korea; and non-state actors: terrorist groups). In deterrence literature tailored deterrence means: "designed and applied with a specific target's motivations, risk acceptance, worldview, and capabilities in mind." [2: 267] The report also endorses "a wider range of military cyber options, and a clear policy and legal framework for their employment", especially vis-à-vis Russia and China. [4: 9] The United States must systematically develop a portfolio of scalable, military and non-military response options to a wide range of potential cyberattacks and costly cyber intrusions "to be able to rapidly provide the President with a range of cyber and non-cyber response options in situations where deterrence fails. In order to support timely decision-making, the 'plays' in this playbook must be in the context of a clear policy and legal framework for their employment (including policy and legal vetting and evaluation via interagency war gaming and discussion)". [4: 14]

A separate section is devoted in the report to strategic and crisis stability. Given the relatively low level of risk in using first strike against an adversary's military capabilities increases the risk of escalation. Therefore, new rungs have to be inserted into the escalation ladder identified through war gaming experience and bilateral strategic stability talks. The report asserts that "[a] critical element in strengthening the U.S. cyber deterrence posture is the clarification of norms regarding the implantation and employment of offensive cyber weapons." [4: 23]

The 2017 National Defense Authorization Act approved by Congress at the end of 2016, delegates the role directly to the DoD and then to the new President to examine and elaborate more effective military and non-military ways of deterrence and the "descriptions of relevant authorities, rules of engagement, command and control structures, and response plans relating to such options". Within 180 days of receiving the DoD report, the legislation requires the President to report to Congress on cyberattacks that warrant a military response. That report should include a "discussion of the types of actions carried out in cyberspace that may warrant a military response or operation; A description of the role of the military in responding to acts of aggression in cyberspace against the United States; A description of the circumstances required for a military response to a cyberattack against the United States;

---

[3]   Gaycken and Martinelli differentiate "cybered deterrence", as deterrence by cyber means, and "cyber deterrence", as deterrence of cyberattacks. [25]

[and] A plan for articulating a declaratory policy on the use of cyber weapons by the United States." [5]

In late 2013, as part of the 2014 National Defense Authorization Act, Congress called for a declaratory deterrence policy by the President. The White House's Deterrence Strategy, as discussed in the previous section, focuses on hardening and increasing the resilience of the most vital critical infrastructure systems as deterrence by denial. Meanwhile, prioritizes the law-enforcement (investigative and prosecutorial) paradigm, partly modelled on counterterrorism, and economic sanctions as cost imposition. Offensive cyber operations are reserved for the most severe cases.

Retaliation, Attribution and Self-Restraint in Cyberspace

In the cyber context, retaliatory deterrence still has a low political feasibility. Retaliation can be in-kind, meaning a counter cyberattack or cross-domain. For several reasons, the U.S. is inclined to exert self-restraint in using cyber offensively. The fundamental feature that distinguishes cyberspace as a strategic environment from the other domains is the difficulty of attributing the perpetrators, which undermines any quick response options. No comprehensive discussion of attribution studies is possible here. What is important to note here is that attribution capability has become a strategic asset for every state. Technical attribution works by tracing back the computer or its geolocation, it can never be unquestionably exact, thus a good result is rather a matter of degree. Digital forensic investigation has to be supplemented with intelligence and information analysis to provide information about the person and the full profile of the culprit(s), and ultimately their links with states or other entities. The more intelligent sources are involved, the higher level of certainty can be achieved. Good attribution requires an immense amount of resources, both technical, human and political, therefore cost is a highly restrictive condition.

Consequently, attribution is not just technical but also a (geo-)political process, and thus requires a very high level of evidence that stands up to scrutiny. In order to initiate a legal procedure or to justify retaliation in self-defence necessitate both solid evidence that meets some legal standards, and the political clout to convince the international community. It is called the burden of proof in legal parlance, and in absence of legally fully verifiable evidence, attribution is only political. If the cyberattack amounts to a violation of international law, but stays below the level of an armed attack, the victim state still has the right to react by a *countermeasure,* which would otherwise itself violate international law, to induce the other state to stop the acts causing disruption. Countermeasures cannot be forcible and must be proportionate, an in-kind response as close to the original violation as possible. In strategic terms, this would parallel compellence.

In the security studies, the most thorough paper on cybersecurity attribution was written by Thomas Rid and Ben Buchanan. Alluding to the many uncertainties surrounding attribution, they say that attribution is what states make of it. "On a *strategic level,* attribution is a function of what is at stake politically. The political stakes are determined by a range of factors, most importantly by the incurred damage. That damage can be financial, physical, or reputational"—they write. [6: 3] Appraising the effects and thus the appropriate response to a cyberattack, in cases like the election influence operations, when the attack builds up slowly

and incrementally, is even more challenging. In addition, international law actually does not determine the standard of proof for States to undertake countermeasures or other means of self-help.

In the U.S., just like in the election hacking case, the private IT security firms play a significant role in detection, incident management and attribution. Those major threat intelligence companies are in the vanguard of IT security worldwide that gives them credential. Consequently, private sector threat intelligence might be a potential point of reference for nation states, too. However, one must not conflate U.S. public attribution with threat intelligence. It rarely happens publicly, but rather through the specialized and confidential information sharing channels between the government and the private sector. The decision whether to communicate the results or not, and how to do it is part of the strategic decision. Public attribution might result in the offenders' termination of an operation, changing tactics, or reacting publicly to allegations. There is another part of the strategic equation, publicizing attribution is also a sensitive issue as it might compromise intelligence sources and procedures, as well as vulnerabilities of the victim. Attribution capability and public attribution constitute a very important element that supports strategic deterrence, and it has been emphasized since 2011, in every official cyber deterrence study and doctrine. An additional message of the identification and indictment of specific persons, or as in 2016 also their links to the Russian Government is that the U.S. is in the possession of very sophisticated attribution capabilities, even if the method of retaliation is not yet refined.

U.S. deterrence strategy, meaning the political and military posture adopted by decision-makers is aimed at averting military or cyber confrontations at the level of inception in the adversary's mind. Patrick Morgan distinguishes this kind of deterrence as *influence strategy*. Meanwhile, the Russian or Chinese strategic thought, in contrast, uses *control strategy*, aiming to take away the other side's ability to launch an attack. [2: 37–38]

As one of the most digitized nations and with its cyber defence at a nascent phase, the U.S. is highly susceptible to cyberattacks. As James Clapper Director of National Intelligence (DNI) said during a Congressional hearing, you do not throw stones when you live in a glasshouse. Therefore, the U.S. advocates strategic and crisis stability in cyberspace as well, just like in the kinetic domains, focusing on political and diplomatic crisis prevention measures. Besides its vulnerability to cyberattacks, the U.S. benefits a lot from long-term stability in the interconnected commercial and military environment. In the White House's *International Strategy for Cyberspace,* or the Department of State's *International Cyberspace Policy Strategy* and in the Department of State legal adviser's statement entitled *International Law and Stability in Cyberspace,* international stability is a central concept. The U.S. sees itself as a standard bearer in cyber issues as well, and pursues international strategy accordingly. Consequently, the U.S. strives not to set a bad precedent in using cyber operations widely and recklessly.

Once military or cyber confrontation did start, escalation dominance is a primary goal. Cyberattacks are especially problematic in terms of escalation, as the second and third order effects are not sufficiently mapped out; nevertheless, it is widely acknowledged that cyberattacks are prone to swiftly escalate into physical space. It is extremely difficult to plan and implement targeted cyberattacks in order to achieve specific strategic effects, thus nation states tend to use it sparingly. In spite of the laborious efforts of international law experts, the legal background and the rules engagement of offensive cyber operations is still unclear.

Another hindrance in the usage of offensive operations comes from the nature of cyber weapons. As soon as a malware is detected, the defenders can patch the particular vulnerabilities, thus it cannot be used again. In addition, it is only a matter of time and expertise that its patterns are reverse engineered, and rivals can improve themselves and learn new techniques, thus cyber weapons might as well be turned against the attacker. [7]

Retaliatory threat also has to be credible. Nevertheless, due to the above-mentioned reason, nation states try hard to conceal their actual cyber capabilities. As a result, the reluctance to brandish one's cyber force to prove how powerful it is renders deterrence ineffective. Instead, the U.S. announces loudly how it extends the volume and technical skills of its cyber troops, as well as its commitment to use them when called upon. However, the higher-level strategies coming from the DoD and the White House emphasize that a retaliator cyberattack is the last resort.

Finally, the most important fact is, that in-kind retaliation or more broadly an active-defence military response is not guaranteed to be able to efficiently neutralize the threat of an ongoing cyberattack, especially in peacetime. That is, the compellence value of cyberattacks is controversial. Martin Libicki analysed this aspect in depth in his 2009 study on Cyber deterrence: eliminate hackers. Nevertheless, the U.S. military does allot great deterrence value to cyber power when it is preparing to reach its full offensive and defensive cyber operational potential that is superior to any other nation state. [8] [9] The idea is similar to the strategic strike value of the air force, [10] that even if the sources of the threat cannot be neutralized directly, the will of the attacking party can be broken by disrupting military supply chains or decapitating supporting economic facilities, or by imposing unacceptable costs on the attacker's hinterland.

Although the White House's presidential directives, the *Cyber Deterrence Strategy* issued in December 2015, as well as the DoD's *Cyber Strategy* which come to the closest of policy guidance and declaratory strategy, order only a last resort role for the military. This judgement, however, is in flux both at the strategic and the operational level. Military cyber power is developed in parallel as a means of deterrence, along with an incremental overall strategic shift in the intention to use it.

Using the military in retaliation is regarded as a last resort. Obama was well-known for his non-confrontational, cautious but pragmatic attitude. According to officials near him, this outlook dominated major U.S. decisions on how to employ cyberattacks, for example against Libya in 2011 or in response to Iranian DDoS attacks in 2012–2013. Based on Obama's personal statements, this approach prevailed in the Russian case, too in 2016. Self-restraint is also integrated into strategy. In June 2013, the top-secret *Presidential Policy Directive* issued in 2012 was leaked. It establishes cyber operations policy for a number of offensive and defensive cyber operations. Two kinds of operations are enlisted that correspond to power projection or active defence in cyberspace: "Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities—other than network defence or cyber collection—conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace. […] Offensive Cyber Effects Operations (OCEO): Operations and related programs or activities—other than network defense, cyber collection, or DCEO—conducted

by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks." [11: 3]

Cognizant of the challenges due to legal complexities and targeting precision, most of the cyberattacks can only be authorized by the President of the Defense Secretary. In order to avoid collateral damage, including upsetting the stability and security of the Internet, and unintended foreign policy consequences, decisions to attack have to be weighted carefully and measured against all other options. Prospects of an offensive cyberattack against the U.S. private infrastructure have to be considered, too. All in all, the assiduously compiled document arranges for alternatives that minimize the use of OCEO.

Proportionate Response, Legal Considerations and Declaratory Policy

Returning to the issue of proportionate response, the threshold for a retaliatory response is obscure legally and politically as well. The definition of a *major cyber incident* is an approximation of the impacts of cyberattacks on vital U.S. values and interests, and shows how the U.S. thinks about cyberattacks within its jurisdiction. The U.S. is a vocal advocate of the norm that when the attack is safely attributed to a foreign nation state, international law constitutes the main point of reference on how to respond to it. Unfortunately, when it comes to cyberspace, the interpretation of international law is extremely contentious. The U.S. authorities do not automatically recognize the Tallin Manual, where influence operations are mentioned as an act not deemed equivalent to the use of force: "[a]s an example, non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force." [12: S1, R11, par. 3]

In fact, the U.S. official statements hardly go into any specific details about how international law is applicable in cyberspace. In addition to a few particular policy statements of U.S. Department of State officials, the Law of War Manual is regarded as the most important expression of the U.S. views on the law of war, and it is also the most detailed, publicly available record of U.S. legal guidance on cyber operations since a legal assessment published by the DoD Office of General Counsel in 1999. [13] What the Obama Administration defines as calculated ambiguity, is most visible in the omissions or the vagueness of the Manual. It is inarticulate on what kind of cyber operations the use of force is needed, and also on the standards of attribution. What constitutes a lawful target in cyberspace is not discussed in detail either. At one place, the Manual notes that cyber operations which merely involve information gathering may not implicate rules applicable to attacks. What amounts to an attack is not discussed in detail, it is only mentioned in the context of cyber operations. In accordance with an apparent majority of international lawyers, the Manual reserves the application of the *ius in bello* rules on targeting to operations that amount to an attack. The Manual refers to a cyber operation "that would destroy enemy computer systems" as prohibited if directed against civilian infrastructure. The Manual notes that rules that apply to attacks do not apply to operations below the attack threshold and such operations may therefore be directed, consistent with the law of war, against civilians or civilian objects subject to the requirement of military necessity. The Manual mentions briefly that cyber operations resulting only in reversible or temporary effects may not amount to an attack. Such operations can be webpage

defacement, disruption of Internet services and dissemination of propaganda. Proportionality in *ius in bello* prohibits attacks expected to produce "loss of life or injury to civilians, and damage to civilian objects incidental to the attack" that would be "excessive in relation to the concrete and direct military advantage expected to be gained". The Manual dismisses from proportionality calculations, "mere inconveniences or temporary losses" including "brief disruption of internet services to civilians" as well as "economic harms in the belligerent state resulting from such disruptions". [13]

Thresholds have to be effective in a strategic sense too, and thus need wider international recognition. According to a RAND study a threshold is: "…a negotiated, declared, or tacitly understood delimiter between measures short of war and high-order conflict such as full-scale conventional or nuclear war." [14]

Clearly articulated policy is indispensable in strategic planning to give unified and unambiguous guidance to lower-level strategies. Explicit or declaratory policy is very often demanded from the President by the domestic military, legislative and expert community. In the international context, clarity is key in governing alliance policies and in signalling to rival nations. If there is no common interpretation of signalling acts, then the whole effort is useless, or might become even escalatory.

The declaratory policy based on the nuclear analogy (Nuclear Posture Review) states, in general terms, why a nation obtains certain kinds of weapons and how those weapons will be used. Offensive cyber operations and intelligence gathering are not new, but in contrast to earlier time periods when they were developed and used in complete secrecy, now their use for national security purposes is gradually gaining some legitimacy and thus require mutually acknowledged international rules. The U.S., however, is highly secretive about its cyber weapons policy. In comparison, Russia and China speak much more openly about how they want to employ their cyber capabilities. Secrecy is inherent in U.S. cyber policy. The White House during the George W. Bush Administration started to partly unveil its strategic intentions in cyberspace. The Obama national security administration realized the need and was much more open, but still refused to set precisely what the U.S. regards an armed attack in cyberspace, and advocated *calculated strategic ambiguity* instead to maintain some freedom to manoeuvre. The 2015 White House report to Congress articulates the need for "a nuanced and graduated declaratory policy and strategic communications" tactic that emphasizes the U.S. Government's commitment to using its capabilities to defend against cyberattacks, but one that is "ambiguous on thresholds for response and consequences to discourage pre-emption or malicious cyber activities just below the threshold for response. […] The administration will consider whether to speak more openly about whether and how the United States might respond to malicious cyber activities, although such public discussion will require carefully balancing such transparency against intelligence and military equities…" the report states. [15: 3]

A DNI officials responsible for cybersecurity commented on the White House official policy: "You don't want to invite people to do anything they want below that red line thinking they'll be able to do it with impunity, and secondly, you don't want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense. […] There's an interest in ambiguity from a strategic sense that also leads to a strategic uncertainty. So it's two sides of the same coin […] If you

don't have specific red lines, you don't have specific necessarily action plans in certain scenarios." [16]

Moreover, there is a consensus that a response also has a publicly undisclosed element, presumably cyber in nature. In 2014, North Korea's Internet network was also knocked out for almost hours. Russia was subject to several cyberattacks between October and December 2016, but there is no evidence they had any link to the skirmish between Washington and Moscow. [17] This reasoning aligns with what Libicki described as *implicit deterrence*, and as the best possible strategic option for the same reason as the U.S. Government stated.

In cyberspace, uncertainty is ubiquitous, and thus calculated ambiguity is difficult. Traditionally, strategic ambiguity means that nation states intentionally leave certain parts of their strategic choices unveiled, when they want to avoid having to choose between opposing options and thus forgo having to "pay an opportunity cost" of lost choice or bear the negative consequences of their strategic choice. The doubt so created also liberates other states who can pretend not to know and thus not having to react publicly to the undisclosed facts, but still being aware they can take those facts into account when planning their own actions. Given the substantial amount of uncertainty in cyberspace, and the volume and scope of cyberattacks against U.S. infrastructure, this strategy rather encourages others who may think they can get away with attacks, or the costs stay below the gains. As a result, U.S. strategic ambiguity seems to be more of a genuine nature than calculated.

Consequently, it is no surprise that President Obama even in possession of good enough attribution tends to first discuss the issue behind closed doors, only at the highest level with the attacking state, as he did so with China and also with Putin at the G20 summit in October 2016. Simultaneously, signalling might also be conducted through public or non-public channels. However, similarly exploiting plausible deniability, the U.S. is still supposed to carry out the most of its cyber activities in secret.

As a matter of fact, the majority of cyberattacks in a calculated manner stay below the level that could possibly reach the damage caused by an armed attack. So did the 2016 Russian operations. Michael Schmitt, a leading legal expert on cyberattacks said: "That lack of clarity is an invitation for Russia and other aggressors to launch similar operations. If states don't, frankly, move forward with a little more dispatch and a little more focus, our opponents are going to play in this gray area." [18]

At the heart of the legal matter is, whether the Russian interference amounted to a violation of the international law. First, it would qualify as such, if it is regarded as a coercive intervention into the internal affairs of another state that is force the target state to do something it otherwise would not do. In the Russian case this coercive element is the most contentious. The intervention could be considered coercive if there was unambiguous evidence that Russia's intent was to alter the result of the elections in favour of one of the candidates. Whereas, the Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence (ODNI) on Election Security states that Russia's intent was to undermine the integrity of the election. Later, the ODNI declassified report entitled *Assessing Russian Activities and Intentions in Recent US Elections* "explicitly stated it couldn't determine the effect of the suspected Russian influence campaign on the election process." [19]

Second option is the violation of U.S. sovereignty. Sovereignty guarantees that states have the exclusive right to control their territory. Unauthorized intrusion into the computer

system of another country might amount to the breach of sovereignty, but this runs counter to the consensual view of turning a blind eye over espionage which in this case was also accompanied by the leak of information. Still that doubtfully amounts to the violation of sovereignty.

If the atrocity does not violate international law, the target state still has the right to "retorsions" under international law. These are actions that states can adopt as self-help without violating their international law obligations. Actually, U.S. response measures fall into this category, and U.S. charges do not explicitly mention that Russia committed a violation of international law. As legal experts point out, retorsions, unlike self-help measures do not even have to be proportionate and thus they can be applied with much more freedom.

Elections as the Target of Cyber-Enabled Influence Operations

National elections are always politically sensitive time periods and the widely spread digitized platforms open up new access points to manipulation. The technical vulnerabilities of voting systems have been a subject of worries since earlier times. In 2008, large amount of information was stolen from the computers of the Obama and McCain campaign teams. Experts have called attention to the vulnerability of the electronic voting systems; still little precautions had been made to introduce more trustworthy systems. [19] There is no consensus on to what extent direct manipulation of election systems can influence final election results. There is no unified national voting system in the United States. Voting systems vary by state and local entities. The biggest concerns are vulnerabilities in voter registration databases, where voters and tabulation systems can be disenfranchised, which happened in a 2014 Ukrainian election, and attackers infiltrated some voting machines and registries in the U.S., as well. In close contests, experts say, it is enough to manipulate the number of legitimate voters in battleground states.

Releasing sensitive information or the spread of fake news to manipulate public opinion are also tactics seen before. The real tactical novelty was the wide spread systematic social media manipulation, as well as the willingness of the perpetrators to reveal their presence, although not their true identity. [20]

Early in January 2017, the U.S. Congress verified and acknowledged the result of the 2016 elections as valid, and the intelligence community fell short of claiming that the Russian influence operations did manage to alter the final election results. Therefore, from a legal perspective it would be difficult to prove that Russia breached U.S. sovereignty and achieved decisive strategic victory over. Hence, in a strategic sense, the purpose of the meddling has to be sought elsewhere.

Due to the attribution caveat, the dubious legitimacy of counteractions, and the low cost-high gain ratio of elections meddling render elections even more geopolitically worthwhile soft targets. In this case, doubt and suspicions about the integrity of the election was dispensed. IT security and intelligence experts claimed that the perpetrators did want to be noticed, or even advertised their theft. Consequently, the operation can also demonstrate that the attacker has sophisticated cyber capabilities on a par with the U.S., and is not afraid to use it to exert influence. Accordingly, validating its own major power status that merit a strategic partnership role. Holding national elections integrity in danger can also serve

as a deterrent. As diplomatic relations between the U.S. and Russia has been deteriorating since at least 2011, and they reached a low point in 2016. In the Russian view, Russia is in a constant state of war with the West. Even at the time of lower level tensions, Russia has been alleged to use DDoS or defacement attacks in coercion or to express its resentment. In his seminal work entitled *Strategy of Conflict,* Schelling argues that strategy in the nuclear age was less about the application of force and more about the "exploitation of potential force". Competitors sought to coerce each other through threats. The power to make threats was not reducible to capabilities or clear commitments alone. Rather, one could also gain leverage through deception and bluffing. That is, you could manipulate the other party and gain a concession. The art of strategy involved constraining an adversary's attacks by manipulating their expectations of costs and risks.

But like, for example, in the attack against Georgia in 2008, the political turmoil might serve as a prelude to a military attack, preparing the battlefield for a larger campaign. Election meddling or similar cyber enabled influence operations have a high strategic value. The long-term strategic question is, therefore, if such operations are to be tolerated tacitly as a useful form of coercion, less damaging than military confrontation.

International Strategy

In line with the main aim of this study, the U.S. election hacking is contextualized in a comprehensive strategic context. Hence, since the beginning of 2000, U.S. has sought to reach out to its allies and international partners employing diplomatic means in its cyberspace policy. The Obama Administration has been especially active in its efforts to elevate cyberattacks into the realm of strategic-politico thinking and shape the global strategic environment through the promotion of international law and norms of behaviour in cyberspace. The U.S. advocates a set of non-binding voluntary norms articulated in the 2011 White House International Strategy and in several official statements of the DoS. These norms and confidence building measures—initially focusing on common vocabulary, and lately on international stability—are often also interpreted as means of deterrence, or as measures supporting deterrence. In addition, the U.S. is very active in bilateral talks and agreements on contingency cooperation, targeting, information sharing, or international policy coordination, with other countries including China and Russia, or regional organizations like the EU.

The U.S. identifies itself as standard-bearer and global leader whose narrative seeks to reflect universal values and interests. It pictures cyberspace as a wild-wild west, ungoverned territory, where establishing norms of acceptable behaviour is in everybody's interest and those who misbehave can be punished. Accordingly, cyberspace is a globally interconnected and interdependent area—global commons, where the free flow of information and stability is a common good, and disruption is detrimental to all. However, this idea is misplaced or even directly antagonistic with the interests of other states. For example, Russia, China, Iran or North Korea follow a different strategic path that aims to construct self-sustaining IT infrastructures and networks in order to reduce their dependence to a minimum, and to boost their state control over "sovereign" cyberspace to the maximum. Given the Russian great

power identity and adversary relations with the West, any operation that diminishes the moral standing and credibility of the U.S. as a global leader is a strategic gain for Russia.

The prohibition of attacks on critical infrastructure is one of these norms, but before 2016 election systems were not part of it. Furthermore, the U.S. seems somewhat flexible when interpreting these norms. It is indicative, for example, when State Department Deputy Coordinator for Cyber Issues Michele Markoff said that the supposedly Russian attacks on Ukrainian critical infrastructure do not violate these norms because they only apply in peacetime. The U.S. also seeks to ensure its own interests through these norms, but it may well have blowback effects. For example, leniency with cyber espionage or cyber exploitation for national security purposes has actually limited U.S. freedom to sanction and deter substantial but non-disruptive cyber intrusions. In 2015, James Clapper ironically expressed envy over the Office of Personal Management hack's success. Moreover, cyber intrusion techniques used for espionage or exploitation can very easily be turned into disruptive attack mode, thus inhibiting defensive efforts.

Part Conclusion

In light of these strategic, legal and political considerations, the Obama Administration's caution seems to be warranted. In December and January 2016, the Government and the President published several official statements attributing the attacks to the highest levels of the Russian Government and the intelligence services. Technical and non-technical evidence was cited by ODNI, Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the Department of Homeland Security (DHS). 35 diplomats were expelled because of a series of unacceptable Russian activities upsetting diplomatic norms of behaviour going back to several years.

The agencies of the widest and highest level, showing unity of effort and consent, provided attribution. The DHS–FBI Joint Analysis Report and the accompanying list of IP addresses manifested for the first time that the U.S. Government acknowledged that the Russian cyber gang names and methods exist (not necessarily all involved in the election hacking) with the aim to raise awareness about Russian malicious cyber activity and thus enable potential targets to better defend themselves. Earlier it was only in the Sony case that a nation state and not just certain individuals were identified as perpetrators in any official statements. The executive order entitled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* dates back to 2015. The scope of the original Executive Order is very telling of the U.S. narrowly focused threat perception, concerning activities that:

- harm or significantly compromise the provision of services by entities in a critical infrastructure sector;
- significantly disrupt the availability of a computer or network of computers (for example, through a distributed denial-of-service attack);
- cause a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain (for example, by stealing large quantities of credit card information, trade secrets, or sensitive information).

After the Russian meddling, the order was amended to authorize sanctions on those who:

- tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. [21]

Using this new authority, the President has sanctioned two Russian intelligence services, The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) and The Federal Security Service of the Russian Federation (FSB), four individual officers of the GRU, and three companies that provided material support to the GRU's cyber operations.

This combined response signified a very important normative message on what is unacceptable behaviour in cyberspace, and what can be expected as proper attribution and proportionate response. In terms of deterrence, the pattern set back in 2015 continued applying a comprehensive cross-domain, whole-of-the nation approach also including some undisclosed most likely cyber response, without escalating the attack.

To sum up, cybersecurity strategy demands a comprehensive strategic approach which involves deterrence only as one of the ways. Currently a non-military posture dominates the U.S. approach, pure cyber defence is combined with deterrence by denial and cost imposition, as well as by wide ranging diplomatic tools. Meanwhile the U.S. cybersecurity efforts, despite several centralizing measures, are still disjoint and reactive, but once an incident is deemed serious enough, response is deliberated carefully and on an overall strategic basis considering effects to wider foreign policy and national interests. Reducing uncertainty deriving from the strategic environment should be a central principle in a security strategy, and in particular in cyberspace. Accordingly, the lack of clear declaratory policy, or the so called calculated strategic ambiguity at the highest level of strategic hierarchy results in disorientation at lower the strategic levels too. Moreover, it impairs overall deterrence. The U.S. socio-political and strategic culture is inherently decentralized, therefore, allocating responsibility for cybersecurity at lower state and local (commercial) levels is a trend to be expected in future policies.

Digitally enabled national elections present a particularly attractive target for politically motivated influence operations, and the integrity of elections is vital for political order. Therefore, elections security or more broadly political security[4] need to be integrated into national security concepts. As cyber-enabled influence operation is likely to remain a strategic threat, besides the technical verification solutions, the United States should outline a clear declaratory policy on electoral interference that entails cost imposition.

Strategic Cultural Context

National security strategic planning pivots on the accurate assessment of the strategic environment, and thus on the catalogue of *real* threats coming from it. Threat perception and the choice of how a nation state aims to address those threats at a strategic level are influenced by the distinctive historical experiences, domestic political environment and

---

[4] In securitization theory, political security is about the organizational stability of social order. The heart of the political security is made up of non-military threats to sovereignty. [26: 141]

technical determinants. In 2016, although there were plenty of indications that Russia had been making attempts to influence U.S. elections, the actual incidents caught the U.S. national security and political elites off guard, therefore rendering response completely reactive. As a recent precedent, in 2014 Russia had targeted public opinion and rigged elections in Ukraine. Moreover, U.S. intelligence had been tracking specific Russian attempts to access U.S. voting systems, although it is not publicly known how much of that was reported to the parties concerned. [19]

Besides the disjoint domestic cybersecurity governance and the calculated strategic ambiguity, the U.S. was taken by strategic surprise due to a narrow strategic focus on threats coming from cyberspace. This limited focus might be ascribed to long-running Western biases towards the strategic cyberattack concept and cyber power concepts, as well as to the rigid binary view of war or peace state of affairs. A detailed comparison of Western and non-Western strategic approach to cybersecurity is beyond the scope of this study. Instead, we provide a brief outline of some major differences in the American and Russian cybersecurity orientation that might explain heightened U.S. susceptibility to Russian political influence operations.

The Evolution of U.S. Threat Perception in Cyberspace

In the U.S., cyberspace had been securitized gradually over the past decades, and its roots go back to times before the Internet, to at least as early as the 1970s. In the U.S. cybersecurity approach, hard power assets like military and economic security have been traditionally strategized as vital U.S. interests. As a result, by the second part of the 1990s, the idea of strategic information warfare (SIW) became widespread. Computer scientists repeatedly warned of the vulnerabilities of the growing number of networked computer systems, for example, one landmark study was the National Research Council report in 1991 *Computers at Risk: Safe Computing in the Information Age.* By the mid-1990s, simultaneously with the accumulation of sophisticated cyberattacks against high-end U.S. governmental or military computer systems, the technical information security risks were increasingly linked with the societal and political impacts. In the military strategic planning, the concepts of the Revolution in Military Affairs and information operations gained ground. The intelligence community has been sending alarms about extensive foreign power cyber espionage. Both in the academic and military strategic community the notion of information warfare has been widely explored. George Rattray points out, though, that information warfare was (is) a broad construct, and it can be interpreted in many different ways. [10] However, by the mid-1990s the national security community became preoccupied by the idea of a strategic level information warfare. In terms of strategic studies, the idea was that the enemy can bring a whole country to its knees without an all-out war by targeting its centre of gravity, in this case, the homeland critical infrastructure and/or the military C2 supply and logistic chains. The spectre of a "digital Pearl Harbor", the idea of a sudden, unexpected devastation by comprehensive cyberattacks on critical infrastructure, or the idea of cyberattacks used as "weapons of mass disruption" soon proliferated in national security discourse.

The other area where the U.S. is particularly sensitive to cyber intrusions is the economy. Maintaining U.S. predominance in the global economic production is conditioned to a large extent on its edge in technology and innovation, and its protection is a vital national interest. Consequently, in the U.S. economic security is closely related to intellectual property protection and economic competition is prone to be securitized in terms of national security threat. Before long, in the U.S., narrative large-scale state sponsored economic cyber espionage became labelled as geopolitical competition waged through strategic information warfare. It is regarded strategically significant, and often referred to as "death by thousand cuts" because of the potential effect on large number of people and the ability of states to conduct their economic and military activities globally. [10]

This fear of state-sponsored economic espionage and illicit technology transfer has been detectable in the U.S. since the 1970s, and it has become especially prevalent after 2000. [10: 26] For example, the United States–China Economic and Security Review Commission was created by Congress in October 2000 with the mandate to monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the U.S. and China. Each year the Commission submits a detailed report on Chinese economic espionage. In 2011, the Office of the National Counterintelligence Executive in a special report to Congress singled-out Chinese and Russian hackers as the world's most rampant perpetrators on cyber espionage. Economic security is designated as a priority in all the national cybersecurity strategic documents. Such approach conflates the traditional economic warfare concept with cyberespionage, cybercrime, cyber-sabotage and even cyberterrorism. [22] As Paul Cornish, British strategic expert points out, the question is "whether the economy might be the way, and cyberspace the means with which to attack the organization and coherence of a modern developed state; not for financial or criminal gain, and not in order to achieve a terrorist 'spectacular', but for maximal political or strategic ends?" As opposed to "a cyber Armageddon", supposes that "it could be in the economic interests of the predator to preserve and exploit, rather than attack and destroy the target economy and its cyber infrastructure"—says Cornish. [23: 9–10]

Strategic cyberwar concept is modelled upon kinetic strategic warfare conducted with nuclear or the air power, and its impact is clearly felt in U.S. cyber threat perception. Focusing on SIW sets a very high bar to a strategic-level defence or response to cyberattacks, whereas the likelihood of such a high-end attack is rather low, and even non-disruptive attacks, like the election meddling can have significant strategic effects. In all of the publicly available strategic documents or expert opinions up till 2017, this narrow strategic approach prevails. The scope of threats is also narrowed down to the military and economic sectors of security, and political security does not feature as a high priority security threat. For instance, the 2015 WH report on deterrence says: "Although cyberattacks can have a range of direct and indirect effects that vary in their severity, U.S. deterrence efforts are particularly focused on those attacks that could result in loss of life, harm to U.S. critical infrastructure, significant damage to property, or significant threats to the national security, foreign policy, or economic health or financial stability of the United States or its interests." [15: 6]

Although U.S. strategists consider Russia a peer competitor in cyberspace, their strategic calculus seems to disregard the essence of Russian strategic thought. National security level cyberattacks are interpreted as destructive or disruptive activities, or as egregious espionage. Treating major malicious activities in cyberspace as the use of force or armed

attack is dubious, and the majority of the attacks fall below this level. Consequently, efforts to address these activities will not fit easily into delineations and authorities—for example Title 10, Title 22, Title 50 of U.S. Code—defined on the basis of whether it is time of peace or war. Furthermore, while unauthorized access to the servers of the Democratic National Convention (DNC), the Democratic Congressional Campaign Committee and some state election systems, or to the NSA could have been interpreted as "standard" national security espionage operations, the leaking of carefully selected sensitive information aims at different strategic gains. These activities amount to covert action and incorporate influence operation or active measures well-established in Russian strategic thinking.

It was only after the elections fiasco that there has been a shift towards a more nuanced U.S. strategic approach. The 2017 report of the DSB Task Force on Cyber Deterrence addresses these challenges. It says that cyber deterrence must be able to cope with a range of cyberattacks, and "…it must do so in contexts ranging from peacetime to 'grey zone' conflicts to crisis to war". [4: 9] Accordingly, the report distinguishes two major categories of cyberattack: "*Cyberattack:* For the purposes of this report, a cyberattack is any deliberate action that affects the desired availability and/or integrity of data or information systems integral to operational outcomes of a given organization. Not all cyber intrusions constitute attacks; indeed, the vast majority do not. […] In addition, while there is considerable attention given to cyberattacks focused on data and software-in-operation, supply chain vulnerabilities are of growing concern." [4: 2–3]

"*Costly Cyber Intrusions:* Under our definitions, China's massive cyber theft of U.S. intellectual property and Russia's hack of U.S. political parties to facilitate information operations undermining confidence in U.S. elections represent costly cyber intrusions. The cyber intrusions in these cases did not affect the availability and/or integrity of U.S. data or information systems, and so do not constitute cyberattacks, but these intrusions did facilitate unacceptable actions by China and Russia that imposed respectively economic and political costs on the United States." [4: 3]

The report recommends that the threshold for a response and the scope of deterrence should be broadened: "The United States must clarify, first internally and then to potential adversaries, that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions. Theft of IP and hacking in support of undermining U.S. political institutions are now clearly on the list; there are numerous other contenders. One example is egregious behaviour in conducting cyber espionage. […] Some would view the 2015 cyber heist from the Office of Personnel Management of some 18 million records containing personal information as so egregious as to warrant a strong U.S. response. A second example is the pre-positioning of malicious software in critical systems, for example the HAVEX9 and BlackEnergy10 malware discovered in the U.S. electrical grid. In the view of this Task Force, although egregious cyber espionage and the insertion of malware in critical systems of the U.S. electrical grid may not constitute cyberattacks, the United States must consider how such malign acts might be deterred." [4: 7]

Conclusion

To draw a final conclusion, it can be stated that the strategic appraisal of cyberspace along with the preparation of the institutional and regulatory measures have been an ongoing process for several decades. Nevertheless, there is still a long way to go in order to achieve a coherent policy or genuine strategic planning. As the shortfalls of the response to the Russian meddling show, despite its wide-ranging intelligence capabilities, the U.S. threat perception is rather limited most probably due to its strategic cultural impulses. At the same time, Russia has managed to better align its broader strategic goals with their ways-ends-means triad.

What can be perceived as a granular tendency is a shift towards federal centralization and the general recognition that the government must have a larger role in prevention, information sharing and a much more refined crisis communication. Also, there is a growing willingness to make public attribution and to involve vibrant international cooperation.

References

[1] *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C.: U.S. National Research Council, 2010. https://doi.org/10.17226/12997

[2] PAUL, T. V., MORGAN, P. M., WIRTZ, J. J.: *Complex Deterrence: Strategy in the Global Age.* Chicago: University of Chicago Press, 2009. https://doi.org/10.7208/chicago/9780226650043.001.0001

[3] *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.* Washington, D.C.: DoD Defense Science Board, 2013.

[4] *Task Force Report: Cyber Deterrence.* Washington, D.C.: DoD Defense Science Board, 2017.

[5] WEBER, R.: Defense bill sets strict deadlines for Trump to asses vulnerabilities, deter cyberattacks. *Inside Cybersecurity,* December 28, 2016. https://insidecybersecurity.com/daily-news/defense-bill-sets-strict-deadlines-trump-assess-vulnerabilities-deter-cyber-attacks (Downloaded: 24.02.2017)

[6] RID, T., BUCHANAN, B.: Attributing Cyber Attacks. *The Journal of Strategic Studies,* 38 1–2 (2015), 4–37. dx.doi.org/10.1080/01402390.2014.977382 (Downloaded: 20.12.2016) https://doi.org/10.1080/01402390.2014.977382

[7] DÉVAI, D.: Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions. *Academic and Applied Research in Military and Public Management Science,* 15 1 (2016), 61–75.

[8] KRAMER, F., STUART, H., WENTZ, L.: *Cyberpower and National Security.* Washington, D.C.: NDU Press, 2009. https://doi.org/10.2307/j.ctt1djmhj1

[9] DAVIS, P.: *Cyber Deterrence: An Old Concept in a New Domain.* (Strategy Research Project) Carlsisle, Pennsylvania: U.S. Army War College, 2013.

[10] RATTRAY, G.: *Strategic Warfare in Cyberspace.* Cambridge, Massachusetts: MIT Press, 2001.

[11] *Presidential Policy Directive 20. US Cyber Operations Policy.* 2013. https://fas.org/irp/offdocs/ppd/ppd-20.pdf p.3 (Downloaded: 25.02.2015)

[12] *Tallinn Manual on the International Law Applicable to Cyber Warfare.* (NATO Cooperative Cyber Defence Centre of Excellence) Cambridge: Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139169288

[13] WATTS, W.: Cyber Law Development and the United States Law of War Manual, International Cyber Norms: Legal, Policy & Industry Perspectives. In. OSULA, A-M., RÕIGAS, H. (Eds.): *NATO CCD COE Publications.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016. 49–63.

[14] *RAND Stretching and Exploiting Thresholds for High-Order War.* 2016.

[15] *White House report to Congress on cyber deterrence.* 2015. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/dec2015/cs2015_0133.pdf (Downloaded: 25.02.2015)

[16] MOORE, J. (2015): Here's the Government's New Definition of a Major Cyber-incident. *Nextgov,* November 4, 2015. www.nextgov.com/cybersecurity/2015/11/heres-governments-new-definition-major-cyber-incident/123393/ (Downloaded: 25.02.2016)

[17] LOWE, C., ZINETS, N.: Russia says foreign spies plan cyberattack on banking system. *Reuters*, Dec 2, 2016. https://www.reuters.com/article/us-russia-cyberattack-banks-idUSKBN13R0NG (Downloaded: 25.02.2015)

[18] MARKS, J.: There's Cyberwar and Then There's the Big Legal Gray Area. February 9, 2017. Nextgov. www.nextgov.com/cybersecurity/2017/02/theres-cyberwar-and-then-theres-big-legal-gray-area/135298/. (Downloaded: 25.02.2017)

[19] *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Intelligence Community Assessment, 2017. www.dni.gov/files/documents/ICA_2017_01.pdf (Downloaded: 12.12.2017)

[20] *JAR–16–20296. GRIZZLY STEPPE – Russian Malicious Cyber Activity.* Washington, D.C.: U.S. Department of Homeland Security and Federal Bureau of Investigation, 2016.

[21] *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment.* Washington, D.C.: The White House, Office of the Press Secretary, December 29, 2016 https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and (Downloaded: 14.01.2015)

[22] RAVICH, S. F. (Ed.): *Cyber-Enabled Economic Warfare: An Evolving Challenge.* Washington, D.C.: Hudson Institute, 2015 www.hudson.org/research/11408-cyber-enabled-economic-warfare-an-evolving-challenge (Downloaded: 14.05.2016)

[23] CORNISH, P.: *The Vulnerabilities of Developed States to Economic Cyber Warfare.* London: Chatham House, 2011. www.chathamhouse.org/sites/files/chathamhouse/0611wp_cornish.pdf (Downloaded: 14.01.2015)

[24] GAYCKEN, S., MARTELLINI, M.: Cyber as Deterrent. In. MARTELLINI, M. (Ed.): *Deterrence and IT Protection for Critical Infrastructures.* Heidelberg: Springer, 2013. 1–10. https://doi.org/10.1007/978-3-319-02279-6_1

[25] BUZAN, B., WÆVER, O., WILDE, J. de: *Security. A new framework for analysis.* London: Lynne Rienner Publishers, 1998.

No Peace No War: The Ethiopian–Eritrean Conflict[1]

Sigatu Tadesse KALEAB[2]

The aim of this article is designed to provide an overview of the historical relations between Ethiopia and Eritrea from pre-colonial times up until the break-out, the major causes of the war, as well as its course and to analyze the situation after the cease-fire including the failed UN peacekeeping and later the proxy war in Somalia. The paper is a desk study, mainly based on secondary data analysis of the available secondary information and documentary examinations; news materials, academic literature, books, and online articles were used. By giving insight into the history, the course war and dynamics of conflictual relations and the frozen war between these two states will help to understand the security dynamics of the region.

Keywords: *conventional war, Ethiopia, Eritrea, proxy war*

Introduction

The relationship between Eritrea and Ethiopia is arguably the most important and volatile and continues to serve as the main source of regional instability in the Horn of Africa. [1] The Horn of Africa is composed of Djibouti, Ethiopia, Eritrea, Kenya, Somalia,[3] Sudan, South Sudan, and Uganda. In the 1890s, after the opening of the Suez Canal, the British, Italian and French were interested in the region because of their strategic location. After the end of World War II, the United States and in the 1960s, the Soviet Union were interested in the region, therefore at the time of the Cold War, it became the area of the rivalry of superpowers. [2] In 2015 China established its first overseas naval base in Djibouti adding the number of military bases in Djibouti to seven including France, US, Japan, Italy, Germany, and Spain. This shows that the region is still strategically important in military, economic and political terms despite the lack of natural resources comparing to other African regions. Most importantly, location lies on the crossroads between the indispensable Middle East oil and the economies of the industrialized countries.

Eritrea became an independent sovereign state on 24 May 1993 after a long civil war with Ethiopia. According to the Guardian's Neal Ascherson, "the African Vietnam" [3] which won

a 30-year war of liberation against an Ethiopian army supported by the Americans and then by the Soviet Union. [4] In 1998 Eritrea and Ethiopia went into a full-scale war. And both countries have remained in a state of war since the 1998 border conflict. Eritrea maintains a large standing army (mostly conscripted), with a primary focus on the defence of the border with Ethiopia. [5] However, significant numbers of conscripts choose to flee the country rather than serve. This makes Eritrea one of the world's fastest emptying nations, a country of about 4.5 million, governed by a secretive dictatorship accused of human rights violations that are playing an outsize role in the biggest global migration crisis since World War II. [6] Eritrea[4] is the second largest nation after Syria to resort to seaborne smugglers to cross the Mediterranean to Europe. [7] About 6% of the population has fled the country. [8]

On the other hand, Ethiopia is a key ally of the Western world, especially the US, which considers it an important regional security partner in the global war on terror. [9: 83] According to the Global Fire Power, Ethiopia is currently the strongest Sub-Saharan country in military terms and the third strongest country in Africa after Egypt and Algeria, ranking higher than Nigeria and South Africa. [10] Ethiopia is also the largest UN peacekeeping contributor in the World, [11] sending its troops to Abyei, South Sudan, Darfur and the African Union Mission in Somalia. The relations between these two states will help to understand the security dynamics of the horn of Africa "which is characterized by destabilization and cross border interventions". [12]

Historical Background

Tigrinya-speaking people on both sides of the Mereb River in northern Ethiopia shared the same language, the same religion and the same basic social, cultural and economic institutions and structures. Undoubtedly, the Tigrinya-speakers of Tigray and Eritrea considered themselves at that time to be an integral part of the *Habesha* (northern Ethiopian) cultural, religious and political realm as embodied by the Orthodox Church and the Ethiopian Monarchy. [13: 258]

However, the Islamic areas north of the Mereb, which were spread out in a semi-circle north of the Tigrinya-speaking areas, had never really been completely integrated into the Empire on the other hand the governor of the northern province received the title of Baher Negash (Ruler of the Sea), whereas the governor of the southern province was given the title of Tigre Mekonen (Lord of Tigray), where both holders of office were given authority over the rulers of all other principalities within their province. [13: 258]

By the middle of the 18th century, local rulers north of the Mereb no longer sought approval by the distant Emperors for their assumption to power. However, while independent of imperial control, these petty rulers still considered themselves part of the Ethiopian polity and never declared their political independence from the Empire. However, it was at the time when Yohannes IV became the first Emperor of Ethiopia to place highland Eritrea under direct

---

[4]   Gérard Prunier, the French academic and historian refers to Eritrea as "the African equivalent of North Korea" for its highly centralized, militarized and authoritarian system of government on the African continent. Lectures given at the Association for Study of the Middle East and Africa.

rule. [13: 259] Under King Yohannes IV, in 1879 Alula became the Governor of the northern province under the title of *Ras* and established his headquarters in Asmara.

In 1882, Italy controlled the Red Sea coastal area of Assab then it expanded Massawa in 1885 with the support of the British. [14: 13] Italy used Assab and Massawa as a springboard to move into the interior of Ethiopia. However, they were defeated at the battle of Dogali in January 1887.

Italy manipulated Ethiopia into signing the Treaty of Wuchale in 1889. The treaty granted the Italians the right to full control over Eritrea and a protectorate role over Ethiopia. However, the interpretation of the treaty became controversial, which culminated in the battle of Adwa in 1896 and the subsequent defeat of Italy. Nevertheless, Italy had managed to establish Eritrea as a separate colonial entity in 1890. [15: 62] A number of treaties (1900, 1902, 1906) were concluded to demarcate this boundary, but for most of its length, the boundary agreed upon in the treaties was not demarcated on the ground. [13: 264]

After the Italians were defeated in World War II, they were evicted from their colonies in the Horn of Africa by the British in 1941. During the following decade, Eritrea remained under British administration. In 1950, the United Nations proposed that a federation would provide Eritrea with autonomy under its own constitution and elected government. In 1952 the act of federation was ratified by Emperor Haile Selassie I and British authorities officially give up their control.

In 1960, leaders of a movement, all Muslims, who were entertaining the idea of an independent Eritrean state, then living in exile, announced the formation of the Eritrean Liberation Front (ELF) in Egypt. By the mid-1960s the ELF was able to field a small guerrilla force in the western plain of Eritrea, and thus it began a war that was to last nearly three decades. Ethiopian authorities portrayed the movement as an Arab tool and sought to rally Eritrean Christians to oppose it; however, deteriorating economic and political conditions produced the opposite result. [16] Moreover, in 1962, the Ethiopian Parliament and Eritrean Assembly voted unanimously for the abolition of Eritrea's federal status, making Eritrea a simple province of the Ethiopian empire. Soon afterward, Tigrinya was banned in education; it was replaced by Amharic, which at the time was the official language of Ethiopia. This turned an entire generation of Eritrean Christian students toward nationalism and the Christians began to join the ELF in significant numbers at the end of the 1960s. [16]

As more and more Christians joined the ELF, it attempted to exclude Christian participation which led them to establish their own organization, the Eritrean People's Liberation Front (EPLF), a secular and Marxist organization. ELF and EPLF were fighting each other, as well as the Ethiopian Government. The latter EPLF dominated the war of independence. [14: 161]

Meanwhile, the Tigray Peoples Liberation Front (TPLF) was founded in 1975 by a group of Tigrayan university students most of whom were active participants in the Ethiopian Student Movement, who revolted against Emperor Haile Selassie I's regime in the 1960s. The front fought with the military government, *Derg* which came to power in 1974 after the Ethiopian Revolution and toppled the emperor from power and forged alliance with other

ethnic groups in Ethiopia to create the Ethiopian People's Revolutionary Democratic Front (EPRDF), which came to power in 1991 after the demesne of the *Derg.*[5]

TPLF made cooperation with EPLF while it fought the *Derg* and the collaboration would remain tactical and mostly characterized by non-strategic short-termism. [17: 269] EPLF also entered into alliances with TPLF mainly for opportunistic reasons. Militarily pressed by the Ethiopian government forces, mostly in 1974 and 1975 it saw the emerging movements in Tigray as useful tools to dissipate the military strength of the Ethiopian Government. [13: 269] Most importantly, it was already clear to the leadership of the EPLF before the end of the war that only the consent of the TPLF led the Ethiopian authorities to the independence of Eritrea which would guarantee rapid international recognition of Eritrea's independence. [13: 276] Medhane Tadesse described the relations as follows: "The EPLF and TPLF carried forward their differences and the resultant mutual suspicion even while they worked to maintain a shaky military alliance to overthrow the *Derg.* Historical animosity and mutual suspicions, different, if not opposing, political trajectories, and prevalent economic and border issues might be considered as major factors in the conflict." [17: 277]

Post-1991 Ethio–Eritrean Relations and Causes of the Conflict

The governments of both states maintained seemingly good relations. The Tigray People's Liberation (TPLF) which dominates the Ethiopian Government through the Ethiopian People's Revolutionary Democratic Front (EPRDF) on the one hand, and the People's Front for Democracy and Justice (PFDJ), the former Eritrean People's Liberation Front (EPLF), ruling Eritrea on the other hand, reflect a political marriage of convenience based on temporarily shared political and economic interests rather than a genuine alliance based on mutual acceptance and deep-rooted friendship between their leaders. [13: 257]

After the 1993 referendum, by signing a Treaty of Friendship and Cooperation on 13th July 1993, the two states formalized their relations. It was agreed that Eritreans would continue to use the Ethiopian Birr as their currency, which was to be provided by Ethiopia. Ethiopia would return Eritrean bank deposits that had been transferred to Ethiopian banks in the final period of the *Derg* rule. The Ethiopian Government also assumed responsibility to pay pensions to Eritrean pensioned ex-civil servants. [18]

Assab was turned into a free port for Ethiopia. Under the terms of the agreement, Ethiopia would pay for the use of the harbor facilities but no duties would be levied on goods arriving at Assab in transit to Ethiopia. Ethiopia consented to buy raw petrol to be refined at Assab and to turn over 30% of the refinery's output to the Eritreans as rent payment. As both countries were using the same currency, it was also agreed upon that trade between Eritrea and Ethiopia would be duty-free. They also adopted the policy that Eritreans within Ethiopia would continue to be treated as Ethiopian citizens.

The various agreements between the two countries were very advantageous for the Eritrean side. They allowed Eritrea to import a wide range of goods for *Birr* from Ethiopia,

---

[5]   This front consists of four political parties. The parties are the Oromo Peoples' Democratic Organization (OPDO), the Amhara National Democratic Movement (ANDM), the Southern Ethiopian People's Democratic Movement (SEPDM) and the Tigrayan People's Liberation Front (TPLF).

which Eritrea would otherwise have to pay for in scarce hard currency. The agreement on the Assab refinery not only guaranteed Eritrea a stable supply of most of its fuel needs but also considerably helped the Eritrean authorities to save the hard currency. The agreement about nationality allowed Eritreans living within Ethiopia, as well as inside Eritrea to freely engage in economic activities inside Ethiopia and even to retain positions in the civil service and the state-controlled sector of the Ethiopian economy. [13: 278]

The currency and customs union to maximize Eritrean savings of hard currency openly violated the spirit of the currency union by pursuing its own policy in regard to exchange rates of hard currency within Eritrea. [19: 377] There are also indications that with the tacit approval of the Eritrean Government, Eritrean traders abused the transit rights for Eritrean goods to divert transit goods illegally which were to be sold for a handsome profit on the Ethiopian market. [13: 279]

Eritreans and the Eritrean Government itself was involved in illegal trade, such as the smuggling of coffee, oilseeds and other products of Ethiopia. [20: 38] In effect, Eritrea became a major coffee exporter without producing an ounce of coffee and was actively engaged in the Ethiopian black market, forgery activities and illegal business transactions, which ended up damaging Ethiopia's economy.[6]

The predicament began when Eritrea demanded more money from Ethiopia for using the crude oil refinery at Assab; consequently, Ethiopia started importing refined petroleum. Also, Ethiopia diversified its import routes to Djibouti and Mombasa rather than using only the port of Assab and Massawa.

Most importantly, it was the introduction of an independent Eritrean currency, *Nakfa,* which lead to a bitter antagonism. The Eritrean Government proposed *Nakfa* in 1997 and the Ethiopian *Birr* should have equal value and should be used in both countries. This would have meant that having a huge stock of *Birr* which could continue buying goods from Ethiopia without having to resort to hard currency. [13: 282] However, this proposal was rejected by the Ethiopian Government, which instead insisted on using hard currency as a medium of exchange. [21: 119] According to Trivelli, it is this demand from Eritrea that angered the Ethiopian Government, as well as the Ethiopian public in general. [21] Eritrea introducing the new currency, left the Eritrean central bank with a large quantity of now worthless *Birr* notes on its hands which created a deteriorating relationship between the two states that made war possible. [21: 119–120]

This economic misunderstanding had an adverse effect on both Eritrea and Ethiopia, to varying degrees. Eritrea suffered most, given its dependence on Ethiopia's economy and markets. Eritrea exported more than 65% of its products to Ethiopia, whereas only 9% of Ethiopia's products were destined for Eritrea. Moreover, Eritrea was highly dependent on Ethiopia for its food consumption. [20: 38] Jon Abbink summarizes the overall unresolved reasons for the conflict between the two states as follows: "The underlying causes of their problematic political and economic relationship since 1991 [...] issues concerning trade, communications, trans-border movements of laborers and pastoralists, the outstanding bank debts (especially of Eritrea to Ethiopia's banking system), goods and property in Assab port destined for Ethiopia and confiscated by Eritrea, Ethiopian military hardware given 'on

---

[6]   Taddesse cited in source [20: 38].

loan' to Eritrea well before the war, legal issues relating to ethnic groups in both countries, citizenship, environmental problems, water-sharing and so on." [22: 409]

The 1998–2000 Border Conflict

The late Nobel Peace Prize winner and Israeli politician Shimon Peres said "war is a competition of making the least mistakes when the biggest mistake is to open the war". [23] On 12 May 1998, a mechanized brigade of the Eritrean army attacked and conquered the town of Badme. [24] Observers on the region wrote the war was fought over a "small strip of contested territory, nowhere more than a few miles wide, and lacking any resources of evident value". [21: 120] The Guardian described the war as "Ethiopia and Eritrea are slugging it out with modern tanks, aircraft, and artillery for the sake of a few miles of stony nothingness". [4]

Gérard Prunier analyzed the war in 1998 as follows: "International wars are usually fought to acquire territory, to gain economic advantage, to overthrow a hated or dangerous neighboring regime, for religious or ethnic reasons or in order to improve a country's position on a regional or international geostrategic chessboard. If we discount the disputed 400 sq. km as relevant to the first possible cause, we are left with nothing since none of the others apply: the Ethio–Eritrean conflict cannot benefit either of its protagonists economically, there is no desire by one regime to overthrow the other, there are no religious or ethnic reasons behind the fighting, and both countries have lost out geopolitically, whether we consider the regional situation or their relationship with their powerful common protector, the United States." [25]

The number of soldiers mobilized by both states was estimated more than 200,000. The violence generated considerable casualties and huge costs on both sides. An estimated 70,000 to 100,000 people were killed, 1 million were displaced. [26: 168] Both countries bought weapons from Russia, Ukraine, Italy, China, Bulgaria, and other countries. MiG–29s by Eritrea, and Sukhoi–27s by Ethiopia, both supplied by Russia. [27] Ethiopia bought Mi–24 helicopter gunships, and Mi–8 cargo helicopters in a deal which provided, as with Eritrea, for technical support, as well as training and pilots. [27] Ethiopia also bought arms and ammunition from China, and T–55 tanks from Bulgaria. [28] Eritrea obtained weapons and ammunition from Bulgaria and other east European countries. [27] Both Ethiopia and Eritrea spent a huge amount of money on the war, estimated at up to $1 billion. [20: 45]

The fighting was of the kind associated in Europe with the First World War, with infantry attacks backed artillery on the trenches occupied by the enemy, with a massive loss of life. [21: 123] Since the Eritreans were strategically on the defensive, most of the attacks were carried out by Ethiopians, whose total losses were correspondingly higher.

The initial clashes between 6 and 12 May 1998 left the area around Badme badly damaged. Ethiopia claims that the Eritrean action displaced over 24,000 people and destroyed twelve schools, a veterinary clinic, fertilizers and grain stores and a series of brief but bloody battles along the border between 22 May and 11 June. [27]

On the ground, the fighting centered on three areas: around Sheraro and Badme in the west, around the town of Zalambessa on the road linking the two countries in the center, and in the far south for control of the road to the Eritrean port of Assab. [27]

A series of air raids resulted in a number of civilian casualties. Ethiopian planes attacked the airport in Asmara. The Eritrean air force also hit targets in the Tigrayan regional capital, Mekele, civilian targets, including a school with 47 people killed. Later, the Eritrean President Isayas Afeworki expressed his regret at their deaths and insisted they were not intentional. [27]

On 6th February 1999, after an eight-month lull, Ethiopia made the first of a series of probing attacks on the Badme front, followed by attacks on the Eritrean positions inside Ethiopia at Zalambessa and Bure, on the road to Assab. On the 23rd of February, Ethiopia launched Operation Sunset and finally broke through the Eritrean defenses, driving the Eritreans out of the disputed area, over-running the whole of the Baduma plains and penetrating 25 km into Eritrea. [27]

Gebru Tareke described the war as follows: … The Eritrean forces had entrenched themselves in fortifications and bunkers that led General Samora Yunus, commander of the northern forces, to contemplate: "The Eritreans are good at digging trenches and we are good at converting trenches into graves. They, too, know this. We know each other very well." The general was not bragging, for subsequent events proved him correct, but he may have lost twice as many of his own men as Eritreans he buried in their foxholes." [46: 345]

According to the Human Rights Watch report, the Ethiopian Government is known to have forcibly expelled an estimated 75,000 people of Eritrean origin during the war; likewise, the Eritrean Government forcibly expelled or took part in the voluntary repatriation of an estimated 70,000 Ethiopians. [29]

Attempts were made for a peaceful solution to the conflict that has ranged from the USA to Rwandan efforts as facilitators, to visits by an Organisation of African Unity (OAU) delegation, the Italians, the Egyptians, President Kabila in person, and the Dutch. [30] [31] However, the fighting was brought to an end with the signing of the Algiers Peace Agreement[7] and the establishment of the Ethiopia–Eritrea Border Commission (EEBC)[8] in 2000. However, Ethiopia's refusal to implement the rulings of the EEBC prior to negotiations and Eritrea's insistence on an unconditional and immediate demarcation of the border, have locked the two governments in an intractable stalemate. [1]

The Failed United Nations Mission in Ethiopia and Eritrea (UNMEE)

Following talks in Algiers, a ceasefire came into force on 31 June 2000, under which a United Nations peacekeeping force was set up, when the Security Council, by its resolution 1312 (2000) decided to establish the United Nations Mission in Ethiopia and Eritrea (UNMEE) consisting of up to 100 military observers and the necessary civilian support staff. [32] The UNMEE was deployed along a 25-kilometre wide strip between the two armies which

---

[7] The *Algiers Agreement* was a peace agreement between the two governments signed on 12th December 2000, at Algiers, Algeria to formally end the war.

[8] Establishment by the Algiers Agreement, it was mandated to delimit and demarcate the colonial treaty border based on pertinent colonial treaties (1900, 1902 and 1908) and applicable international law. The Commission was seated in The Hague with the Permanent Court of Arbitration serving as registry and the UN Cartographic Section providing technical support.

is agreed by the Algiers Agreement. [26: 168] Later, the UNMEE expanded to a total of 4,200 military personnel, including 220 military observers, three infantry battalions and the necessary support units, to monitor the ceasefire and border delineation between Ethiopia and Eritrea.

However, on 30th July 2008, the Security Council unanimously adopted resolution 1827 terminating the mandate of the UNMEE. The Council decision came in response to crippling restrictions imposed by Eritrea on the UNMEE, as well as the cutting off of fuel supplies—making it impossible for the operation to continue carrying out its mandated tasks, and putting at risk the safety and security of UN personnel. [32]

Post-War Stalemate and Proxy War

Since 2015 the security situation in Ethiopia has deteriorated and the government declared a state of emergency from October 2016 up to August 2017. However, as this paper is being written, there are still violent protests and targeted killings across the country. A leaked document assessing the security and political situation presented at the National Security Council meeting held on October 2017 revealed that "all anti-people forces are forming a strategic consensus and using the latest support of the Egyptian and Eritrean governments and are trying to destroy the constitutional system by sectarian violence and riots". [33] This is not unexpected because the two states are in quasi-war. For example on 15th April 2011, the Ethiopian Government for the first time openly announced it would use "any means at its disposal" to remove the incumbent regime in Asmara. [34] Ethiopia is assisting the Eritrean Democratic Alliance and other smaller groups, such as the Red Sea Afar Democratic Organization in their fight against the Eritrean regime. [35: 98] In September 2013 the Red Sea Afar Democratic Organization and Saho People's Democratic Movement made an agreement in Ethiopia to carry out military attacks to topple the Eritrean regime. [36]

In line with the saying "the enemy of my enemy is my friend" Eritrea has been arming and training insurgent groups, namely the Ogaden National Liberation Front (ONLF) and the Oromo Liberation Front (OLF), to infiltrate Ethiopia through Somalia and undermine its security. Eritrea's support for Islamist groups in Somalia was also viewed as a security threat by Ethiopia, given their irredentist rhetoric and radicalization agenda.

In fact, since its independence, Eritrea has fought all its neighbors including Yemen and has been linked with military activity as far away as the Democratic Republic of the Congo (DRC) and South Sudan. [5: 491] In December 2009, invoking Eritrea's alleged support for Somali armed opposition groups and its border conflict with Djibouti, the Security Council passed resolution 1907 (2009), which imposed a sanctions regime on Eritrea, including a general and complete arms embargo (on both imports and exports) and prohibited Eritrea to provide support to the armed groups engaged in destabilization activities in Somalia and to undermine the peace and reconciliation efforts as well as regional stability. [37]

The report of the Monitoring Group on Somalia and Eritrea dated in July 2011 describes the Eritrean post-war subversive deeds in the region as follows: "Eritrea's foreign and security policy, including its involvement with various armed groups throughout the region, can only be understood in the context of the 1998–2000 war with Ethiopia. Ethiopia's failure, to date, to implement the ruling of the Eritrea–Ethiopia Boundary Commission on the disputed

border, and the continuing presence of Ethiopian civilian officials and military forces on territory awarded to Eritrea by the ruling, is routinely cited by the Government of Eritrea as justification for its support to Ethiopian armed opposition groups, such as ONLF and OLF, which are named in this report. Eritrea's 'cold peace' with Ethiopia is also reflected in its actions elsewhere in the region, notably Somalia, where Ethiopia and Eritrea have supported various rival factions and administrations since 1998." [38]

After six years, on 2nd November 2017, the Monitoring Group on Somalia and Eritrea in its report states: "Investigated allegations by a neighboring Member State of support provided by Eritrea to Al-Shabaab in Somalia. Despite receiving some corroborating information from another regional Member State and regional administrations in Somalia, the Group has not been able to substantiate the allegations. As such, the Group has, for its fourth consecutive mandate, not found conclusive evidence of support provided by Eritrea to Al-Shabaab. […] Eritrea continued to provide support to armed groups intent on destabilizing Ethiopia and Djibouti, including the Benishangul People's Liberation Movement, the Front for the Restoration of Unity and Democracy (FRUD-Armé), Patriotic Ginbot Sebat (PG7) and the Tigray People's Democratic Movement. While none of these groups poses a critical threat to either Djibouti or Ethiopia, the support of Eritrea for them continues to generate insecurity in the region and undermines the normalization of relations between the regional Member States." [39] Consequently, on 14th November 2017 the UN Security Council extended arms embargoes on Eritrea, by adopting Resolution 2385 (2017).

The very purpose of both governments eventually becomes to destabilize each other with their extended support to respective opposition groups. [35: 98] Meanwhile, there have been episodes of military incursion. In March 2012 Ethiopia attacked an Eritrean military base after the killing of five European tourists it blamed on Asmara. [40] On December 2014 an Ethiopian air force pilot has defected to Eritrea, flying an MI–35 gunship helicopter across the border with his co-pilot and a technician. [41] On 22nd March 2015, the Ethiopian Air Force has bombed the Bisha gold mine in Eritrea, located 150 kilometers west of Asmara, along with the Eritrean military depot at Mai Edaga. [42] On 12th June 2016, Ethiopian forces launched an unprovoked assault over the Eritrean border at the town of Tsorana and Eritrean forces managed to launch a counter-offensive that ended the assault. [43]

Conclusion

The defense expert, Fred Charles Ikle stated "[m]any wars in this century have been started with only the most nebulous expectations regarding the outcome, on the strength of plans that paid little of any attention to the ending. Many begin inadvertently, without any plans at all". [44: 108] *If indeed war should break out, then it would not be in our power to stop it, for such is the logic of war." This is an excerpt from* Khrushchev's letter to John F. Kennedy at the time of the Cuban Missile Crisis. [23] Terminating a conflict under favorable conditions has been one of the most difficult tasks facing any political and military leaders. [45] Today after almost 20 years, both Ethiopia and Eritrea are in the inauspicious situation because of a protracted "foolish war, against the wrong enemy and on a false pretext". [46: 343]

The war was unplanned; when the Eritrean leaders sent their tanks and artilleries across the border, their intention was to intimidate a government they believed would capitulate

to their demand. Isayas Afeweriki, the President of Eritrea underestimated the patriotism, fierceness and willingness of Ethiopians to fight when he ignited a war whose scale and duration he did not plan for and of which he had no exit strategy. [46: 343]

After nearly two decades of a cold war, a resolution requires political courage from both governments. Only negotiation can address the root causes of the war which are historical, economic and political. Hailemariam Desalegn, Ethiopia's Prime Minister said that he is willing to hold talks with Eritrea. "The most important thing for us is to fight poverty […] to have regional integration. If we two do that, it will be much more productive", he also mentioned his predecessor "Meles Zenawi had asked for more than 50 times even to go to Asmara and negotiate with Isaias Afwerki". [40] The leaders of both countries should know that both states are "condemned by geography, economy, and history to have their future inextricably entwined". [46: 343] Otherwise the result will be as B. H. Liddell Hart, the military historian, and military theorist puts it "the downfall of civilized states tends to come not from the direct assaults of foes, but from internal decay combined with the consequences of exhaustion in war". [47: 359]

This article was written at the end of 2017. By the time of the publication in 2019, there is a new political development. After the appointment of a new Prime Minister in Ethiopia, Abiy Ahmed (Ph.D.) in April 2018, and his call for peace, the two countries signed a Joint Declaration on Peace and Friendship in July 9th, 2018 in Eritrean capital, Asmara and an Agreement on Peace, Friendship And Comprehensive Cooperation in September 16th, 2018 in Saudi Arabia. This will be a beginning of a new chapter in the complicated relationship between the two states.

References

[1] GOITOM, G., TRONVOLL, K.: Ethiopia and Eritrea: Brothers at war no more. *Aljazeera* (online), 8 December 2013. www.aljazeera.com/indepth/opinion/2013/12/ethiopia-eritrea-brothers-at-war-no-more-201312111228604587.html (Downloaded: 30.10.2017)

[2] HAILE, S.: Historical Background to the Ethiopia–Eritrea Conflict. In. CLIFFE, L., DAVIDSON, B.: *The Long Struggle of Eritrea for Independence and Constructive Peace.* Nottingham: Spokesman, 1988. 11.

[3] PRUNIER, G.: *Eritrea and its Discontents.* ASMEA, 2011. (video) https://vimeo.com/18716003 (Downloaded: 25.11.2017)

[4] ASCHERSON, N.: When two tribes go to war, only the arms dealers win. *The Guardian* (online), 28 February 1999. www.theguardian.com/world/1999/feb/28/ethiopia.nealascherson (Downloaded: 25.11.2017)

[5] IISS: *The Military Balance 2017.* London: The International Institute for Strategic Studies and Routledge, 2017.

[6] STEVIS, M., PARKINSON, J.: African Dictatorship Fuels Migrant Crisis: Thousands flee isolated Eritrea to escape life of conscription and poverty. *WSJ* (online), 2 February 2016. www.wsj.com/articles/eritreans-flee-conscription-and-poverty-adding-to-the-migrant-crisis-in-europe-1445391364 (Downloaded: 27.11.2017)

[7]   Thousands of civilians fleeing 'rule of fear' in Eritrea, say UN experts, warning of gross rights abuses. *UN News* (online), 24 June 2015. www.un.org/apps/news/story. asp?NewsID=51239#.Whte3UqnFPZ (Downloaded: 27.11.2017)

[8]   Eritrea profile – Timeline. *BBC* (online), 30 October 2017. www.bbc.com/news/world-africa-13349395 (Downloaded: 27.11.2017)

[9]   KLOSOWICZ, R.: The role of Ethiopia in the regional security complex of the Horn of Africa. *Ethiopian Journal of Social Sciences and Language Studies,* 2 2 (2015), 83–97.

[10] African Powers Ranked by Military Strength Ranking. *Global Fire Power* (online), s.d. www.globalfirepower.com/countries-listing-africa.asp (Downloaded: 27.11.2017)

[11] Troop and Police Contributors. *United Nations Peacekeeping* (online), s.d. https://peacekeeping.un.org/en/troop-and-police-contributors (Downloaded: 27.11.2017)

[12] BUZAN, B., WAEVER, O.: *Regions and Powers: The Structure of International Security.* Cambridge: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511491252

[13] TRIVELLI, R. M.: Divided histories, opportunistic alliances: Background notes on the Ethiopian-Eritrean war. *Africa Spectrum,* 33 3 (1998), 257–289.

[14] NEGASH, T.: *Eritrea and Ethiopia: The Federal Experience.* Uppsala: Nordiska Afrikainstitutet, 1997.

[15] HALL, J. G.: *Exploration of Africa the Emerging Nations: Ethiopian in the Modern World.* Philadelphia: Chelsea House Publishers, 2003.

[16] MARKAKIS, J., LAST, G. C.: *Eritrea.* Encyclopaedia Britannica (online), s.d. www.britannica.com/place/Eritrea/History (Downloaded: 01.11.2017)

[17] TADESSE, M.: Tigray People's Liberation Front (TPLF). In. PRUNIER, G., FICQUET, É. (Eds.): *Understanding Contemporary Ethiopia.* London: C. Hurst & Co. (Publishers) Ltd., 2015. 257–282.

[18] FESHAY, B.: *The Economic and Political Integration between Eritrea & Ethiopia: Was it Feasible?* 28 May 2015. http://assenna.com/wp-content/uploads/2015/05/Berhe_Eri-Ethio.pdf (Downloaded: 15.11.2017)

[19] LATA, L.: The Ethiopia–Eritrea War. *Review of African Political Economy,* 30 97 (2003), 369–388. https://doi.org/10.1080/03056244.2003.9659772

[20] MULUGETA, K.: The Ethiopian–Eritrean War of 1998–2000: An Analysis of its Causes, Course, Impacts and Prospects. In. MESFN, B., SHARAMO, R.: *Regional Security in the post-Cold War Horn of Africa.* Monograph 178. Pretoria: Institute for Security Studies, 2011.

[21] CLAPHAM, C.: *The Horn of Africa: State Formation and Decay.* London: Hurst & Company, 2017.

[22] ABBINK, J.: Ethiopia–Eritrea: Proxy Wars and Prospects of Peace in the Horn of Africa. *Journal of Contemporary African Studies,* 21 3 (2003), 407–426.

[23] RAIK, G.: *The Diplomatic Manoeuver.* Cambridge: Belfer Center for Science and International Affairs John F. Kennedy School of Government, 2016. www.belfercenter. org/publication/diplomatic-maneuver#_ftn9 (Downloaded: 01.12.2017) https://doi. org/10.1080/0258900032000142446

[24] JOIREMAN, S. F.: Ethiopia and Eritrea: Border War. In. BENSON, S. G., MATUSZAK, N., O'MEARA, M. A. (Eds.): *History Behind the Headlines: The Origins of Conflicts Worldwide.* Vol. 1. Detroit: Gale Group, 2001. 1–11. http://scholarship.richmond.

edu/cgi/viewcontent.cgi?article=1124&context=polisci-faculty-publications (Downloaded: 12.11.2017)

[25] PRUNIER, G.: The Ethio–Eritrean Conflict: An Essay in Interpretation. *refworld* (online), 1 November 1998. www.refworld.org/docid/3ae6a6b74.html#_ftn1 (Downloaded: 20.11.2017)

[26] LYONS, T.: The Ethiopia–Eritrea Conflict and the Search for Peace in the Horn of Africa. *Review of African Political Economy,* 36 120 (2009), 167–180. https://doi.org/10.1080/03056240903068053

[27] PLAUT, M., GILKES P.: Conflict in the Horn: Why Eritrea and Ethiopia are at War. *Briefing Paper New Series,* No.1, 31 March 1999. https://reliefweb.int/report/eritrea/conflict-horn-why-eritrea-and-ethiopia-are-war, (Downloaded: 25.11.2017)

[28] Ethiopia and Eritrea: War, it is. *The Economist,* 11 February 1999. www.economist.com/node/185946, (Downloaded: 25.11.2017)

[29] Eritrea and Ethiopia. The Horn of Africa War: Mass Expulsions and the Nationality Issue (June 1998–April 2002). *Human Right Watch,* 15 3 (A) (2003), 1–59. www.hrw.org/sites/default/files/reports/ethioerit0103.pdf (Downloaded: 18.11.2017)

[30] Why? The Eritrean–Ethiopian Conflict. *Review of African Political Economy,* 25 77 (1988), 508–26.

[31] ALLEN, C.: Britain's African Policy: Ethical, or Ignorant? *Review of African Political Economy,* 25 77 (1988), 405–407.

[32] UN: *United Nations Mission Ethiopia and Eritrea.* New York: United Nations, 2017. https://unmee.unmissions.org/background (Downloaded: 02.11.2017)

[33] As exclusive Document Presented at the Ethiopia National Security Meeting. *Addis Standard* (online), November 13, 2017. http://addisstandard.com/8852-2/ (Downloaded: 14.11.2017)

[34] WILLIAMS, P. D.: *Horn of Africa Webs of conflict & Pathways to Peace.* Washington, D.C.: Woodrow Wilson International Center for Scholars, 2011. www.academia.edu/1288198/Horn_of_Africa_Webs_of_Conflict_and_Pathways_to_Peace_Oct_2011 (Downloaded: 15.10.2017)

[35] ATINAFU, K. BAYEH, E.: The Ethio–Eritrean Post-War Stalemate: An Assessment on the Causes and Prospects. *Humanities and Social Sciences,* 3 2 (2015), 96–101. https://doi.org/10.11648/j.hss.20150302.15

[36] TEKLE, T-A.: Exiled Eritrean rebel groups plan joint military attack against regime. *Sudan Tribune* (online), 8 September 2013. www.sudantribune.com/spip.php?article47958 (Downloaded: 14.14.2017)

[37] *Resolution 1907 (2009): Adopted by the Security Council at its 6254th meeting, on 23 December 2009.* New York: UN Security Council, 2009. www.un.org/ga/search/view_doc.asp?symbol=S/RES/1907%282009%29 (Downloaded: 25.11.2017)

[38] *Letter dated 18 July 2011 from the Chairman of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council.* New York: UN Security Council, 18 July 2011. www.refworld.org/docid/50362c0b2.html (Downloaded: 25.11.2017)

[39] *Letter dated 2 November 2017 from the Chair of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council.* Monitoring Group on Somalia and

Eritrea, 6 November 2017. /www.un.org/ga/search/view_doc.asp?symbol=S/2017/925, (Downloaded: 28.11.2017)

[40] Ethiopia PM willing to talk to Eritrea. *Aljazeera* (online), 6 December 2012. www.aljazeera. com/news/africa/2012/12/2012125145129652231.html (Downloaded: 28.11.2017)

[41] Ethiopian pilot defects to Eritrea in helicopter: state media. *Reuters* (online), 23 December 2014. www.reuters.com/article/us-ethiopia-eritrea/ethiopian-pilot-defects-to-eritrea-in-helicopter-state-media-idUSKBN0K114U20141223 (Downloaded: 15.11.2017)

[42] TOPF, A.: Ethiopian Jets Attack Canadian Gold Mine in Eritrea. *Wardheer News* (online), March 22, 2015. www.wardheernews.com/ethiopian-jets-attack-canadian-gold-mine-eritrea/ (Downloaded: 15.11.2017)

[43] BRUTON, B.: Africa: *A Frightening Flare-up on the Ethiopia/Eritrea Border, and Another Resounding Silence from Washington.* 15 June 2016. http://allafrica.com/stories/201606150132.html (Downloaded: 15.11.2017)

[44] IKLE, F. C.: *Every War Must End.* New York: Columbia University Press, 1971.

[45] THOMAS, T. M.: *Conflict Termination and Military Strategy. A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.* Newport: Department of Operations, 1994. www.dtic.mil/dtic/tr/fulltext/u2/a283406.pdf (Downloaded: 01.12.2017)

[46] TAREKE, G.: *The Ethiopian Revolution: War in the Horn of Africa.* Addis Ababa: Eclipse Printing Press, 2016.

[47] LIDDELL HART, B. H.: *Strategy.* 2nd Revised Edition. New York: Meridian, 1991.

Public Sector Innovation in Europe[1]

Csaba MAKÓ,[2] Miklós ILLÉSSY,[3] András BORBÉLY[4]

In the recent decades there is a growing interest in how public and private organisations can develop abilities to innovate in order to cope with the challenges created by the changing priorities of the political market, the intensification of global competition and the higher speed of the technological changes. The ability of organisations to mobilize their internal resources into efficient and dynamic routines depends on intangible resources (e.g. creativity) and less on such traditional tangible factors as physical or financial sources. The core aim of the paper is to identify and compare the creative/learning capabilities of the workplaces in the EU–27 countries. The data of the European Working Conditions Surveys (2005, 2010 and 2015) shows that public administration boosts creative workplaces in all countries. The increasing rate of creative jobs may speed up the implementation of the "High-Engagement Civil Services".

Keywords: *innovation, private/public sector, work organisation, creativity, country cluster*

Introduction: The Role of Innovation in the Employment Growth and in the Organisational Performance

There is a growing consent between the practitioners and academics on the importance of non-technological (e.g. workplace development programmes, etc.) innovations in generating sustainable competitiveness of the national economies and in opening a new road for both economic and social development. Systematically collected experiences on the diffusion of various types of innovation indicate that—in the long run—the higher employment rate is one of the visible outcomes. [1] The World Bank's research institute carried out the most comprehensive and methodologically well-founded research on the employment impacts of innovative or non-innovative firms. The survey covered 26,000 firms in 71 countries. According to their results, innovative firms generate significantly greater employment

---

2   Prof. Em., Dr. (DSc), National University of Public Service, Szent István University; e-mail: mako.csaba@tk.mta.hu; ORCID ID: 0000-0002-2597-3103
3   Research Fellow, Hungarian Academy of Sciences, Centre for Social Sciences, Institute for Sociology; e-mail: illessy.miklos@tk.mta.hu; ORCID ID: 0000-0002-0241-0287
4   Ph.D. student, Szent István University, Doctoral School of Management and Business Administration; e-mail: andras.borbely1989@gmail.com; ORCID ID: 0000-0002-9853-577X

growth and this growth is much more inclusive than previously expected. [2] In addition, according to the recent review of some sixty American papers on workplace innovation indicates that the efficiency effects of workplace innovation on performance premiums range between 15% and 30%. [3] Looking at the European experiences, according to the Finnish workplace development programmes (2004–2010) "…active employee and middle management participation in planning and implementation phase of the project, close internal collaboration during the process, competence in project work, methods used by external experts, and external networking were related to simultaneous improvements in productivity and the Quality of Working Life (QWL) at workplaces. […] Direct participation of employees can function as a 'change agent'." [4: 41]

In spite of favourable performance outcomes of the workplace innovation, the mainstream innovation streams are stressing the importance of the technological (i.e. product and process) innovations and are neglecting the roles of such non-technological innovations as new models of work organisations, new working and employment practices, new business models and marketing methods, etc. For example, according to such emblematic figure of the so-called open innovation system as Chesbrough: "There is no inherent value in a technology per se. The value is determined by the business model used to bring it to market. The same technology taken to the market through two different business models will yield different amounts of values. An inferior technology with better business model will often trump a better technology commercialized through inferior business model." [5: 14] However, the European innovation policy landscape is still dominated by a technological focus, despite the undeniable but rather slow transition to a more holistic approach.

The so-called Dortmund/Brussels Position Paper elaborated by the European Network for Workplace Innovation (EUWIN) and other experts of non-technological innovation stress that although social innovation is a pre-condition for the successful implementation of new technologies, it cannot be implemented successfully without the necessary organisational adjustments and innovations, if the share of the organisation investing in workplace innovation is low. Stakeholders and decision-makers often lack the adequate information and knowledge resources, and consequently they are rarely aware of the importance of workplace innovation. Organisational and workplace innovations represent a hidden resource for the whole Europe to become more competitive, especially in South and Eastern Europe. [6] In these countries "…perception of work may be classified as an individual one. This notion has a focus on the quality of a single workplace, its individual skill requirements and individual employment condition protection. The collaborative character and its implications in the 'Nordic debate' which are meant in the notion of 'new forms of work organisation' are badly understood." [7: 412]

Beside the visible inequalities in the share of workplace innovation investment within the country groups of the European Union (i.e. the highest investment in the Nordic countries and the lowest one in the Mediterranean and Central and Eastern European countries), both theoretical experts and practitioners often underestimate the important role of the social (collective) and organisational learning necessary for the successful implementation of the innovations—especially in case of their radical forms.

For example, the potentials of the use of such generic or integrative technologies as the Information and Communication Technology (ICT) are un-exploited or under-utilised due to these shortcomings. In this relation it is worth quoting Lundvall, [8: 2–3] who stressed

that "…firms that introduced ICT without combining it with investments in the training of employees, with change in management and with work organisation got a negative effect on productivity growth that lasted several years. […] What is at stake is the capacity of people, organisations, networks and regions to learn. Learning to cope with the full potential of the new technologies is, in a sense, to transform them from being new to being old." In addition to the Lundvall insistence on the key role of learning absorbing new technologies (i.e. ICT), we have to add the growing importance of the combination of technical and social competencies. There are "…more and more voices suggesting that the digital economies will also require the collaboration of the 'Techies' with humanities majors, the so-called 'Fuzzies' in order to complement their understanding of the social challenges and creativity among other elements." [9: 1] In this relation it is worth noting that "…the better competence of US firms in utilisation of ICTs explains as much as 50 per cent of the differences in growth in productivity between Europe and the US." [10: 39]

The paper is structured as follows. Following the introduction on the importance of the interplay between technological and social innovations, the first section briefly outlines the theoretical and methodological foundations in the public sector innovation research. The second section describes the methods on how to measure the creativity of work. The third section is dealing with the empirical analysis of the various waves of the European Working Conditions Survey (EWCS 2005, 2010 and 2015) aimed to identify types of work shaping innovativeness of the organisations—with special focus on public administration. Finally, the concluding section summarizes the analysis.

Innovation in the Public Sector: Theoretical and Methodological Foundations

After World War II, until the end of the 1970s, the mainstream international innovation surveys have been focusing and collecting data on Research and Development (R&D) activities in the private sector. These analyses were able to describe the innovation potential of mainly manufacturing (and other industrial) firms operating in the private sector, while the innovation activity of the service sector and in particular the organisations of the public administration were omitted. The report of the expert group of the European Commission indicated "…that public sector innovation today mostly happens through uncoordinated initiatives rather than as a result of deliberate, strategic efforts. The quest for more and better public sector innovation is hindered by several barriers, which fall into four major categories: weak enabling factors or unfavourable framework conditions, lack of innovation leadership at all levels, limited knowledge and application of innovation processes and methods, and insufficiently precise and systematic use of measurement and data." [11: 5]

Following a more than a decade-long preparation, the OECD did initiate pilot studies on the innovation—in private and manufacturing sectors—in the Nordic countries. The lessons from these surveys were summarized in the Oslo Manual (1992). This manual served as a theoretical and methodological guideline for the various waves of the Community Innovation Surveys (CIS) which were carried out by the National Statistical Offices (NSO) within the European Union. The first edition of the Oslo Manual essentially aimed to measure or map not only the R&D activities in their strict sense but the diffusion of technological

(product + process) innovation, as well. In this relation it is worth mentioning that the original questionnaire elaborated in the first edition of the manual and used in the following surveys was not able to measure the innovation in the fast growing service sector. The modified version of the questionnaire published in the second edition of the Oslo Manual (1997) is suitable to measure innovation in both the manufacturing and service sector. However, only the third edition of this Manual (2005) covers such types of non-technological innovations as marketing or new business and organisational practices. According to this Manual: "…innovation represents a new or significantly developed product (services) or process, new marketing methods, or the implementation of the new management-organisational methods in the business or workplace practices and in the external relations of the organisation." [12: 494]

There is a rather new research agenda having the ambition to compare and identify the similarities and differences of organisational innovation characterising the private and the public sectors. Following Hollanders et al., [13] Table 1 compares the characteristics of the innovation in the private and the public sectors. The table indicates well both the similarities and differences of innovation activities in the two sectors. For example, similarities are dominating in the fields of process and organisational innovation. However, service innovation instead of product innovation and communication innovation instead of market innovation characterise the public sector in comparison with the private one. In the innovation management literature, the following definition of service innovation is used widely: "Service innovation is a new service or such a renewal of an existing service which is put into practice and which provides benefit to the organisation that has developed it: the benefit usually derives from the added value that the renewal provides the customers. […] A service innovation process is the process through which the renewals described are achieved." [14: 4]

Table 1. *Differences between the private and public sector innovation.* (EPSIS [13])

Private sector	Public sector
Product innovation	Service innovation
Process innovation	Process innovation
Organisational innovation	Organisational innovation
Marketing innovation	Communication innovation

Before presenting the methods used to identify the creative or innovative potentials of the European workplaces, it is necessary to briefly outline the main features of the systematic theoretical framework. We adopted a broad-based innovation policy approach elaborated by Ramstad [15] and called "expanded triple helix as an innovation generating policy model". This model goes beyond the traditional national innovation approach in the following fields. It stresses the importance of the "social innovation", focusing besides public players to other organisations, in addition to inter-organisational relations, the internal development of the organisation has decisive roles in innovations, and finally this approach stresses that changes are not located at one level (e.g. at the top or bottom) but "…changes on different levels are interrelated. Without knowledge about the micro-structures we might get little out of attempts to change institutions and organisations at the meso- and macro-levels." [15: 2]

In a recent study of the European Centre for the Development of Vocational Training (Cedefop) [16] the authors tried to combine the different levels of data. Three aspects of intellectual capital were identified and considered as determinants of a firm's innovative ability: human capital, structural capital and relational capital. Human capital covers individual knowledge, skills and competencies of the members of an organisation. Structural capital is defined as the "organisational and technological structures and processes allowing the sustained operation and innovation of the organisation." [16: 22] Relational capital includes all relations through which an organisation is linked to its environment. It is essentially important in capturing relevant information from stakeholders, customers, suppliers, associations, etc. The authors conceptualized the three fields of intellectual capital in the following way (see Table 2):

Table 2. *Human, structural and relational capital
as determinants of innovative ability.* [16: 23]

Intellectual capital		
Human capital	**Structural capital**	**Relational capital**
Domain related knowledge, skills and competences	Organisational culture	Relations to customers
Practical experience	Cooperation and communication within the organisation	Relations to suppliers
Social skills and competences	Equipment relating to information technology, software and other technological systems	Relations to investors/shareholders
Motivation	Knowledge transfer and storage	External cooperation with educational institutions
Leadership skills	R&D infrastructure for product innovation	External knowledge acquisition
Personal skills and competences	R&D infrastructure for process innovation	Social engagement/Corporate social responsibility
Continuous vocational training	Organisational structure	Image of company/brand
Initial vocational education and training	Organisational processes	Engagements in associations and public relations
Continuing higher education	Use of modern ICT	
School and higher education	Learning-intensive forms of organisation	

Methodology: How Can We Measure Creative and Innovative Capability at the Workplace?

In testing empirically the various types of work, our analysis uses the datasets of the 4th (2005), 5th (2010) and 6th (2015) wave of the European Working Conditions Surveys (EWCS).[5] The methods used are based on the work of Lorenz and Lundvall, [18] who

---

[5] EWCS is a cross-sectional survey taken in every five years since 1990, organised by the European Foundation for the Improvement of Living and Working Conditions (Eurofound, Dublin). The recent waves of this survey cover more than 40,000 workers in the EU member states and in various other European countries. [17]

analysed the fourth wave of the European Working Conditions Survey and distinguished three types of employees according to the dimensions of cognitive demands of work and employees' autonomy. These three groups are "creative workers", "constrained problem solvers" and "Taylorised workers". The methodological background of these groups will be presented later in detail at the end of this section and at the beginning of the next section.

In our study, we focus on salaried employees working in organizations with at least 10 employees in non-agricultural sectors as industry, service and public administration, excluding education; health and social work; household activities; as well as agriculture and fishing.[6] The sample examined consists of 11,661 salaried employees in case of the 4th wave (2005), 14,192 in the 5th wave (2010), and 14,425 in case of the 6th wave (2015). Not only the sampling procedure, but also our method to group the sectors of the statistical nomenclature is consistent with Lorenz and Lundvall's work. [18] (See our groups in Table 3 below.)

Table 3. *Summary table of NACE sectors, codes and the sector groups used in the paper.*
(Own compilation following the work of Lorenz and Lundvall. [18])

Sector-group	Code	Economic activities
Manufacturing, construction, utilities	C	Mining and quarrying
	D	Manufacturing
	E	Electricity, gas and water supply
	F	Construction
Retail and other services	G	Wholesale and retail trade, repair
	H	Hotels and restaurants
	I	Transport, storage and communication
Business and financial services	J	Financial intermediation
	K	Real estate, renting and business activities
Public administration	L	Public administration and defence, compulsory social security
Community, social and personal services*	O	Other community, social and personal service activities
	Q	Extra-territorial organizations and bodies
Excluded sectors	A	Agriculture, hunting and forestry
	B	Fishing
	M	Education
	N	Health and social work
	P	Activities of households

Legend: *We did not indicate the "Community, social and personal services" group in our sector level tables, however, we included it in the aggregate results.

In order to identify the main differences between EU countries, we distinguished five country groups on the basis of their institutional settings (i.e. welfare system, labour market regulation, labour relation issues etc.). Our typology is analogous to country groupings

---

6   EWCS uses the NACE (Nomenclature Statistique des Activités Économiques dans la Communauté Européenne) industry standard classification system (its Hungarian equivalent is the TEÁOR system). In order to achieve data interoperability, we used the NACE 1.1 version.

used in comprehensive institutional studies (e.g. Hall and Soskice's work, [19]) as well as organizational studies using the same database. [20] [21] [22] In this perspective, we distinguished "Scandinavian", "Anglo–Saxon", "Continental", "Mediterranean" and "Central and Eastern European (CEE)" country clusters. (See Table 4.) In order to elaborate unbiased results, all tables presented in this study incorporate cross-national weighted data.

Table 4. *Summary table of countries and country groups used in the paper.*
(Own compilation following several recent studies. [19] [20] [21] [22])

Country group	Country
I. EU–15 (old member states)	
Scandinavian	Denmark, Finland, Sweden
Anglo–Saxon	Ireland, United Kingdom
Continental	Austria, Belgium, France, Germany, Luxembourg, the Netherlands
Mediterranean	Greece, Italy, Portugal, Spain
II. EU–12 (new member states)	
Central and Eastern European	Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia[*]
—–	Cyprus, Malta[**]

Legend: [*]Croatia was excluded from our analysis. [**]Countries of Cyprus and Malta were not assigned to any of the country groups; however, we included them in the EU–27 aggregates.

Not only the sampling procedure but also the choice of variables and methods of analysis for this study is consistent with the approach of Lorenz and Lundvall. [18] In order to characterize the main attributes of a creative workplace, we used the following six binary variables:

1. a variable measuring whether the work requires problem solving [PBSOLV];
2. a variable measuring whether one's able to learn new things from work [LEARN];
3. a variable measuring the presence of complex task in one's work [COMPLX];
4. a variable measuring the use of individual's own ideas at work [IDEAS];[7]
5. a variable indicating the presence of autonomy in choosing the working methods [AUTMET];
6. a variable indicating autonomy in choosing the order of tasks [AUTORD].

The type of the factor method which was carried out on these variables is Multiple Correspondence Analysis (MCA). Further analyses were elaborated on two factors which contributed together to 58% of the inertia in case of EWCS 2005, 60% of the inertia in case of EWCS 2010, and 59% of the inertia in case of EWCS 2015. In order to group the cases, hierarchical clustering (Ward's method) was carried out on the basis of the factor scores on each sample.

---

[7]   A binary variable transformed from a five-level ordinal scale, as follows: "always", "most of the time" ("almost always" and "often" in EWCS 2005) answers were recoded into "yes"; "sometimes", "rarely", and "never" ("sometimes", "rarely", "almost never" in EWCS 2005) were recoded into "no".

This paper, however, uses Lorenz and Lundvall's work [18] only as a theoretical and methodological starting point, and it differs from it in several ways. First, we included data from the fifth and sixth wave of EWCS (2010 and 2015). This allowed us to enlarge the scope of the analysis with the comparison of periods before and after the recent financial (2008) crisis. Second, our paper widens the limits of their study by evaluating the differences between each European country group, and including the public administration sector into the analysis. In the current phase of our research, we intend to introduce several results of descriptive analyses[8] on the basis of the results of the abovementioned more sophisticated statistical tools.

Creative Jobs in the European Union: Sharp Contrast along the North–West and South–East Axis

Before presenting the distribution of different job clusters and later their changes over time, it is worth describing shortly the characteristics of these clusters. As we can see from Table 5 below, variables used to measure both the cognitive and the autonomy dimensions of work show relative stability in the three waives of the European Working Conditions Survey carried out between 2005 and 2015. The creative cluster can be characterised by an overrepresentation in all six variables: they mobilise extensively their cognitive abilities during the employees' work and they enjoy high level of autonomy in doing so. Around half of the European employees belong to this category of workers. The constrained problem solver jobs show high degree of problem-solving and learning activities, their working tasks are rather complex, but—surprisingly enough—they rarely use their own ideas during work. Similarly, the level of autonomy in choosing the methods of work and the order of tasks is far the lowest compared to other employees. They account for nearly one quarter of the employees. The group of Taylorist workers can be characterised by the lowest level of problem solving and learning activities, they execute relatively simple tasks. In contrast, their autonomy is significantly higher than those belonging to the category of constrained problem solvers, although it is far below the average of creative employees: from one fourth to one third of employees belong to this job category.

Table 5. *Distribution of work organisation variables across job clusters, EU–27.*
(Following Lorenz and Lundvall's choice of variables, [18]
own calculations based on EWCS 2005, 2010, 2015.)

Variable	2005				2010				2015			
	CW	CP	TW	AV	CW	CP	TW	AV	CW	CP	TW	AV
PBSOLV	97	87	40	80	97	91	45	81	97	92	44	83
LEARN	91	85	16	70	92	85	14	69	93	87	14	72
COMPLX	84	82	8	64	85	78	7	62	86	77	7	64
IDEAS	76	22	29	51	71	16	25	46	70	16	25	46
AUTMET	94	22	37	62	94	16	38	60	94	18	41	63

---

[8]   For the sake of transparency, the tables and figures presented in this paper incorporate results without decimals (i.e. due to rounding, not all results add up to 100).

Variable	2005				2010				2015			
	CW	CP	TW	AV	CW	CP	TW	AV	CW	CP	TW	AV
AUTORD	91	14	34	58	94	17	37	60	93	19	38	62
Total share	**50**	**24**	**26**	100	**49**	**24**	**27**	100	**52**	**24**	**24**	100

Legend: CW = creative workers; CP = constrained problem solvers; TW = Taylorised workers; AV = average; PBSOLV = solves problems during work; LEARN = learns new things in work; COMPLX = solves complex tasks; IDEAS = able to use own ideas; AUTMET = able to choose work methods; AUTORD = able to choose the order of tasks

Creative jobs are especially prevalent in such sectors as research and development; other computer related activities; electricity, gas, steam and hot water supply; insurance, reinsurance and pension funding; financial intermediation. Constrained problem solvers are typically working in such sectors as land transport and transport via pipelines; manufacture of textiles; manufacture of motor vehicles; manufacture of chemicals and chemical products and manufacture of basic metals. Taylorised workers are most prevalent in sewerage; manufacture of textiles; manufacture of wearing apparel; land transport and transport via pipelines; postal and courier activities.

Creativity and Autonomy of Employees in the European Union: Polarisation of Work Organisation from North-West to South-East

As we can see from the table above, undoubtedly the creative job cluster gives the biggest opportunity for the employees to work autonomously and to deploy their creativity. It is not at all surprising that the Scandinavian countries are those where these kinds of jobs dominate the most. (See Figure 1.) In Denmark 77% of all jobs investigated are creative, whereas the same ratio is 74% in Sweden and 73% in Finland. In addition to these countries, we find above the European average presence of creative workplaces in such Continental countries like Luxembourg (65%), the Netherlands (63%), France (62%), Belgium (59%) and Austria (57%), together with the two Anglo–Saxon countries: the UK (59%) and Ireland (55%). It is interesting to see that while all Mediterranean countries are below the European average (52%), two former socialist countries, namely Estonia (62%) and Slovenia (55%) have a share of creative jobs above the average. The position of Germany is also surprising: creative work organisations are less widespread in Europe's biggest economy than the EU–27 average and exceeds Spain by only two percentage points. Besides Germany we find only Mediterranean and Central and Eastern European countries below the EU–27 average, with Greece, Latvia, Slovakia, Romania and Hungary being the last five countries where creative jobs are the least widespread.
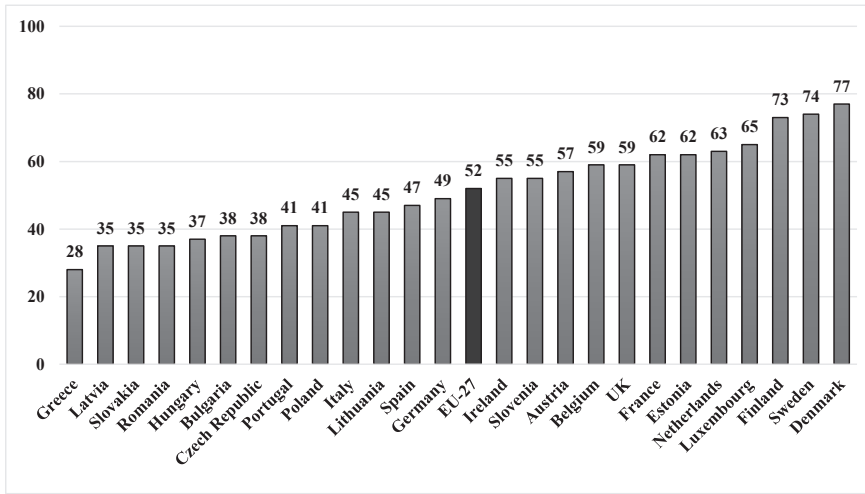
Figure 1. *The share of creative jobs in the European Union (2015).*
[Own compilation based on EWCS 2015.]

The jobs of Taylorised workers can be characterised by a low level of both creativity and employee autonomy. The next figure, illustrating the share of these jobs in Europe, is almost the inverse version of the previous one presenting the share of creative jobs. (See Figure 2.) This means that in most of the cases, in a country where creative jobs are more widespread we will find the least Taylorised workers. This is true, for example, for the Scandinavian and for the Central and Eastern European (CEE) countries: Denmark, Finland and Sweden are leader countries in terms of creative jobs and are lagging behind all other countries when it comes to Taylorised workers. In contrast, creative jobs are less prevalent in the CEE countries while we found the highest shares of Taylorised ones in this region.
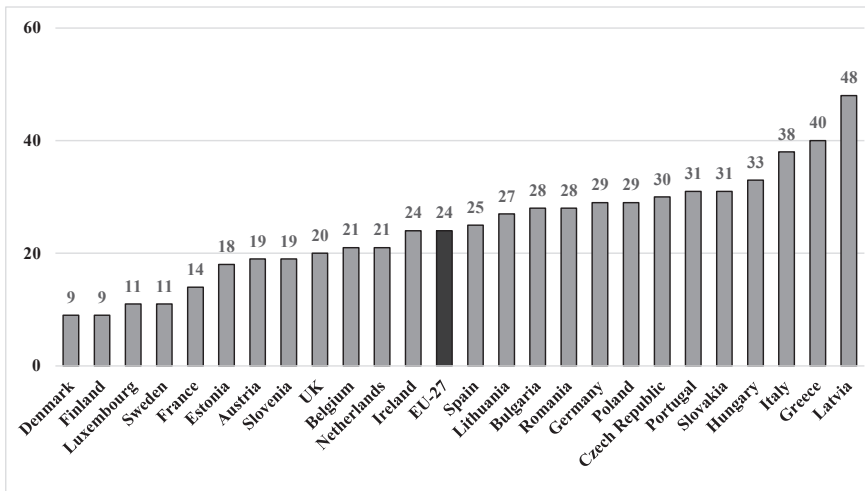
Figure 2. *The share of Taylorised workers in the European Union (2015).*
[Own compilation based on EWCS 2015.]

However, there are notable exceptions as well. It is surprising that almost one third of the German workplaces (29%) belongs to the Taylorised cluster and this is the 9th biggest share among the EU–27 countries. Italy is middle-ranked among the European countries in the share of creative jobs, but it is one of the most Taylorised countries with 38% of jobs being Taylorised. All in all, four countries have a significantly higher share of Taylorised jobs than the EU–27 average: Latvia (48%), Greece (40%), Italy (38%) and Hungary (33%). They are followed by Slovakia, Portugal, the Czech Republic, Poland, Germany, Romania, Bulgaria and Lithuania (27–31%). Spain and Ireland are around the EU–27 average (25% and 24%, respectively). The Netherlands, Belgium, the UK, Slovenia, Austria and Estonia are the countries where the share of Taylorist jobs is visibly below the average (18–21%), while we find the lightest presence of this type of work organisation in Denmark (9%), Finland (9%), Sweden (11%), Luxembourg (11%) and France (14%).

Constrained problem solvers are those employees whose jobs demand a relatively high level of cognitive capacities during the work but allow the lowest level of employee autonomy at the same time. Given the fact that creative jobs represent around three quarter of all jobs in the Scandinavian countries, it is not at all surprising that the share of both Taylorised employees and constrained problem solvers is among the lowest in Denmark, Sweden and Finland. (See Figure 3.) Their share is similarly low in the Netherlands, Italy, Latvia, Belgium, Ireland, the UK and Estonia (between 16–21%). The EU–27 average is 24% and we find eight countries very close to this rate: Germany, France, Luxembourg, Austria, Slovenia, Portugal, Spain and Lithuania (23–28%). The highest share of constrained problem solvers can be found in CEE countries, namely in Hungary, Poland, the Czech Republic, Bulgaria, Slovakia and Romania (30–37%), together with Greece (32%), the only representative of Mediterranean countries in this group of countries with the highest share of constrained problem solvers.
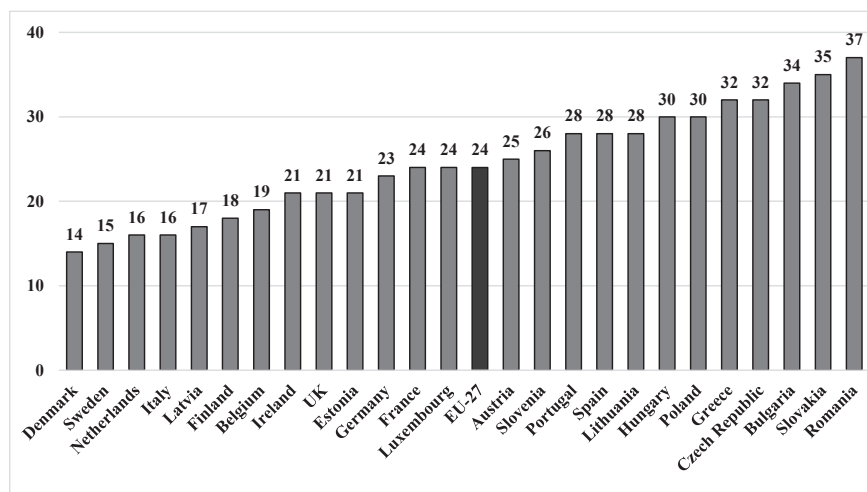

Figure 3. *The share of constrained problem solvers in the European Union (2015).*
[Own compilation based on EWCS 2015.]

If we add the share of constrained problem solvers to the share of Taylorist workers, it gives a good proxy indicator on those employees who enjoy less autonomy in their work. It is even more important because the lack of participative employee involvement sets serious limits to any kind of creativity having long-term impact on innovation. It is obvious that employees are important sources of innovation, their active participation in the implementation is a necessary precondition of any innovation: "The basic idea of Employee-Driven Innovation rests on the assumption that employees have hidden abilities for innovation, and that this potential can be made visible, recognised and exploited to the benefit of both the firm and its employees." [23: 66]
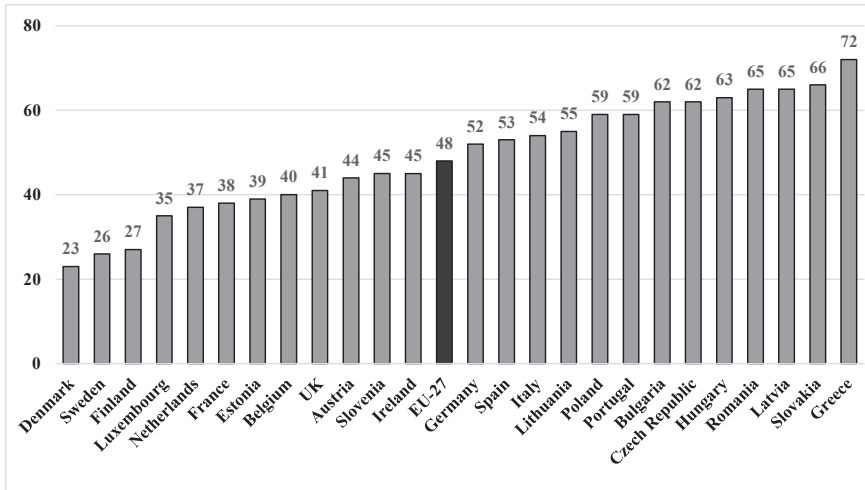
Figure 4. *The share of constrained problem solvers and Taylorist workers in Europe (2015).* [Own compilation based on EWCS 2015.]

As we can see from Figure 4 above, the three Scandinavian countries are visibly separated from the rest of Europe, the share of the two least autonomous job clusters is around 25%. The follower country group is composed by Luxembourg, the Netherlands, France, Estonia, Belgium, the UK, Austria, Ireland and Slovenia (35–45%). These countries are below the European average (48%). It is interesting to note that we do not find any Mediterranean country and only two CEE countries below the average: Estonia and Slovenia. These two country groups are overrepresented at the low end of the scale: more than every second job has limited level of employee autonomy in Spain, Italy and Lithuania. Their share is about 59–66% in Portugal, Poland, Bulgaria, the Czech Republic, Hungary, Latvia, Romania and Slovakia. The situation is the worst in Greece where the same ratio is 72%. This means that these countries have the lowest potential to develop innovative capabilities of employees and their work organisations.

Work Organisation in the Old Member States:
Significant Differences between and within Country Groups

The share of different employee groups varies greatly between countries. In the Old Member States (OMS), creative workers dominate in the Scandinavian country group: in Sweden, for example, four out of five employees had a creative job at the beginning of the period investigated (2005) and this ratio fell to 74% in ten years (see Table 6). In 2015, we found the highest share of creative jobs in Denmark (77%) with a slight increase between 2005 and 2015. Finland experienced a significant catch-up period: the share of creative jobs increased from 67% to 73%. The share of Taylorist jobs increased a bit in the first five years, but after that, it dropped back to its original ratio. Constrained problem solvers are the second most populous job cluster in this country group representing 14–18% of employees.

Table 6. *Distribution of job clusters in the Old Member States.*
[Own calculations based on EWCS 2005, 2010, 2015.]

	2005			**2010**			**2015**		
	CW	**CP**	**TW**	**CW**	**CP**	**TW**	**CW**	**CP**	**TW**
I. Scandinavian									
Denmark	74	13	13	75	11	15	77	14	9
Finland	67	20	13	66	20	13	73	18	9
Sweden	80	10	10	74	17	9	74	15	11
II. Continental									
Austria	51	29	20	51	30	20	57	25	19
Belgium	56	20	23	59	18	22	59	19	21
France	59	19	21	47	22	31	62	24	14
Germany	51	25	24	47	28	25	49	23	29
Luxemburg	63	18	19	57	23	20	65	24	11
Netherlands	72	16	13	66	18	16	63	16	21
III. Mediterranean									
Greece	40	32	28	30	29	42	28	32	40
Italy	40	28	33	49	14	37	45	16	38
Portugal	42	24	34	43	29	28	41	28	31
Spain	37	28	35	47	23	30	47	28	25
IV. Anglo–Saxon									
Ireland	58	19	22	49	25	27	55	21	24
UK	50	20	30	51	25	24	59	21	20
EU–27	**50**	**24**	**26**	**49**	**24**	**27**	**52**	**24**	**24**

Legend: CW = creative workers; CP = constrained problem solvers; TW = Taylorised workers

In the majority of the Continental countries, the share of creative jobs increased between 2005 and 2015, with the notable exceptions of Germany and the Netherlands. However, we can see a dramatic decrease between 2005 and 2010 in France and Luxembourg, too, with a remarkable recovery experienced during the following five years. The case of the Netherlands is exceptional as it shows a continuous decrease in the share of creative jobs from 2005 to 2010 and further to 2015. In fact, it started from the level of the Scandinavian

countries in 2005, whilst by 2015 it nearly touched the Continental country group average which is significantly lower. The share of constrained problem solvers decreased only in Austria, it remained the same in Belgium, Germany and the Netherlands, while it increased significantly in France and in Luxemburg. As concerning the Taylorist workers, their share did not change in Austria and Belgium between 2005 and 2015, it decreased to a notable extent in Luxemburg, while it increased radically in Germany and the Netherlands. The case of France is particularly interesting as radically opposite trends were observable between 2005 and 2010, and between 2010 and 2015. During the first phase, the share of Taylorist jobs increased from 21% to 31%, whilst it decreased even more significantly during the second phase from 31% to 14%.

Different job clusters are more evenly distributed in the Mediterranean countries than in other OMS. This means that the share of creative jobs is significantly lower, while the other two job clusters, especially the Taylorist one is overrepresented compared to the European average. These four countries show different dynamics in terms of the changes in distribution of job clusters over time. The share of creative jobs increased in Italy and Spain, while it decreased in Greece. In contrast, the share of Taylorist workers remarkably increased in Greece, to a lesser extent in Italy, where the share of constrained problem solvers decreased dramatically from 28% (2005) to 16% (2015).

Similarly to the Mediterranean country group, we can observe opposite trends in case of the Anglo–Saxon countries. In the UK, the share of creative jobs increased significantly from 2005 to 2015, while the share of Taylorist workers decreased by the same extent (10 percentage points). In Ireland, the share of creative employees decreased remarkably from 2005 to 2010 but it increased again since then. The opposite trends were observable in case of the two other job clusters: after an increase during the first phase (between 2005 and 2010), we detected a decrease of similar extent during the second phase (between 2010 and 2015).

New Member States:
Highest Density of Creative Jobs Found in Estonia and Slovenia

It is not surprising that the share of creative jobs is less prevalent in the New Member States (NMS) than in the OMS. This country group is closer to the Mediterranean countries in this regard than to any other European country cluster. There are two exceptions from this rule, Estonia, where the 62% of jobs are creative, and Slovenia, where the same ratio is 55%. (See Table 7.) Latvia also had a relatively good position in 2005 and 2010 (52% and 58% respectively) but the share of creative jobs has been decreasing considerably since then and became one of the lowest in Europe for 2015 with 35%. This loss was compensated by an incredible increase in the number of Taylorist jobs: the share of this type of workplaces more than doubled in only five years, from 2010 to 2015 (from 22% to 48%). This is by far the biggest ratio for Taylorist workers ever registered in a European country.

Table 7. *Distribution of job clusters in the New Member States ("CEE" country group).*
[Own calculations based on EWCS 2005, 2010, 2015.]

	2005			2010			2015		
	CW	CP	TW	CW	CP	TW	CW	CP	TW
Bulgaria	40	30	29	32	30	38	38	34	28
Czech Rep.	43	30	27	44	30	26	38	32	30
Estonia	57	25	19	62	21	16	62	21	18
Latvia	52	19	29	58	20	22	35	17	48
Lithuania	39	30	31	44	25	31	45	28	27
Hungary	44	29	27	48	29	23	37	30	33
Poland	46	32	22	42	29	29	41	30	29
Slovenia	52	24	24	52	31	17	55	26	19
Slovakia	37	32	31	35	32	32	35	35	31
Romania	37	39	24	35	34	31	35	37	28
EU–27	**50**	**24**	**26**	**49**	**24**	**27**	**52**	**24**	**24**

Legend: CW = creative workers; CP = constrained problem solvers; TW = Taylorised workers

A similar pattern of increasing share of Taylorist jobs at the expense of a loss in creative ones can be observed in Hungary, where the second highest share of jobs without significant level of employee autonomy and learning opportunity was registered among the NMS, and to a much lesser extent in the Czech Republic. In Poland, Taylorist jobs gained importance already from 2005 to 2010 and have been stabilised since then. In Bulgaria, this shift from the creative to Taylorist workplaces was experienced between 2005 and 2010 but the creative cluster regained its importance in the next five years. The distribution of different job types has been relatively stable over time in Romania and Slovakia with a low level of employee-level autonomy at work: the share of constrained problem solvers is the highest in these two countries. Lithuania, in contrast, shows a mild but steady rise in the share of creative workers.

The Role of the 2008 Global Crisis: New Member States on a Diverging Development Path

It remains to be explored in more details how the global financial crisis and economic downturn might influence the distribution of different job clusters. The data sets allow us to distinguish short-term and mid-term impacts. It is worth noting that in not less than eight OMS, the share of creative jobs decreased between 2005 and 2010. This loss in creative jobs was compensated by an increase in the share of constrained problem solvers in Sweden, Germany and Luxemburg. On the contrary, in Greece and France the share of Taylorist jobs increased in parallel with the decrease of creative ones, while in the Netherlands and Ireland the loss in creative jobs was evenly distributed between the other two clusters.

Among the NMS, the share of creative jobs decreased from 2005 to 2010 in Poland (46% vs. 42%), Romania and Slovakia (37% vs. 35%). A significantly bigger decrease was experienced in the long run (i.e. between 2010 and 2015) in Latvia (58% vs. 35%), Hungary (48% vs. 37%), and the Czech Republic (44% vs. 38%). Latvia is an especially interesting

case as we observed a 6 percentage point increase in the share of creative workplaces from 2005 to 2010 but their share decreased dramatically in the following five years. Surprisingly enough, we find some countries where the share of creative workers increased despite economic recession: in Estonia (57% vs. 62%), Lithuania (39% vs. 45%) and Slovenia (52% vs. 55%). There was a decline in the number of creative jobs from 2005 to 2010 in Bulgaria (40% vs. 32%) but their share has increased again in the following five years.

It is also interesting to note that while the differences between the country groups of the Old Member States have been shrinking over time, the CEE countries seem to diverge from this pattern. While the averages of Scandinavian and Continental country groups did not change much between 2005 and 2015, the Mediterranean countries show visible catching up tendencies in terms of both creative and Taylorised jobs, the first being augmenting and the second being decreasing. (See Tables 8, 9 and 10.) Also, the same is true for the Anglo–Saxon country group. Meanwhile, the shares of different job clusters develop in the opposite direction in case of CEE countries. For example, in case of creative jobs, the difference between CEE and EU–27 averages increased from 7 to 13 percentage points between 2005 and 2015. In case of Taylorist jobs, the CEE country group average was 1 percentage point below the EU–27 average in 2005, it turned to a 5 percentage points handicap in 2015.

Table 8. *The share of creative jobs by country groups in Europe (2005, 2010 and 2015).* [Own calculations based on EWCS 2005, 2010, 2015.]

	SCD	AGS	CON	MED	CEE	EU–27
2005	75	50	56	39	43	**50**
2010	72	51	50	46	42	**49**
2015	75	59	55	46	39	**52**

Legend: SCD= Scandinavian; AGS= Anglo–Saxon; CON= Continental; MED= Mediterranean; CEE= Central and Eastern European country group

Table 9. *The share of constrained problem solvers by country groups in Europe (2005, 2010 and 2015).* [Own calculations based on EWCS 2005, 2010, 2015.]

	SCD	AGS	CON	MED	CEE	EU–27
2005	13	20	22	28	32	**24**
2010	16	25	25	20	30	**24**
2015	15	21	22	25	32	**24**

Legend: SCD = Scandinavian; AGS = Anglo–Saxon; CON = Continental; MED = Mediterranean; CEE = Central and Eastern European country group

Table 10. *The share of Taylorised workers by country groups in Europe (2005, 2010 and 2015).* [Own calculations based on EWCS 2005, 2010, 2015.]

	SCD	AGS	CON	MED	CEE	EU–27
2005	12	30	22	33	25	**26**
2010	12	24	25	34	29	**27**
2015	10	20	22	29	29	**24**

Legend: SCD = Scandinavian; AGS = Anglo–Saxon; CON = Continental; MED = Mediterranean; CEE = Central and Eastern European country group

Although the individual country analysis calls attention to the differences within conventional country groups and there are some notable exceptions from the general trends at both the high-end (e.g. Estonia and Slovenia) and the back-end (Greece, Latvia, Hungary), the country group analysis gives a more nuanced picture and calls attention to the diverging path taken by the majority of former socialist countries during the global economic crisis. This calls for a deeper analysis of the effects of the global financial crisis and economic downturn and the individual country-level answers to it.

Sectoral Differences: The Public Sector is an Important Locus of Creative Jobs

In the followings, we will analyse differences in the share of job clusters from a sectoral perspective. As a first step, we distinguished work organisations operating in the private and public sectors.[9] In order to keep the analysis easy to understand, we will focus on Hungary and aggregate, country group-level data. As we can see from Table 14 (see Annex), the public sector is an important locus of creative jobs in all country groups as their share is visibly higher compared to the private sector. However, this is not true for Hungary where there were no differences between the two sectors in 2015. Longitudinal analysis shows that this is a relatively recent trend in Hungary, because the public sector had a notably higher share of creative jobs than the private sector both in 2005 (58% vs. 40%) and 2010 (59% vs. 44%). This shift was due to the expansion of Taylorised workplaces. In 2010, for example, only 16% of public sector jobs were Taylorised but this ratio doubled in only five years (16% vs. 33%, from 2010 to 2015). Similar trends were observable in other CEE countries but to a significantly lesser degree (24% vs. 26%). In contrast, the Anglo–Saxon country group showed a reverse trend: the share of Taylorised workers was 33% in 2005 and it declined to 18% in 2015. The case of the Mediterranean and Continental country groups is also interesting: in the public sector there was a slightly higher share of creative jobs in 2005, but during a 10-year time span, this difference has been growing significantly higher and the public sector became undisputable the leader in the share of creative jobs.

---

[9]   Based on the related question asked in each of the three waves of the survey ("Are you working in the…? private sector; public sector; joint private–public organisation or company; not-for-profit sector, NGO; other") we were able to distinguish between private and public sector employees ("joint private–public organisation or company"; "not-for-profit sector, NGO"; and "other" answers were excluded from the results presented in Table 14).

In the following, we will analyse in more detail the changes in public administration compared to other sectors such as manufacturing, construction, and utilities; retail and other services; and business and financial services. It is impossible to make a comparison at country level because of the low number of cases, therefore we will limit our analysis to country group-level investigation. As we can see from the table below (Table 11), public administration has a leading role in promoting creative workplaces in all country groups. Even the "business and financial services"—which is traditionally regarded as one of most innovative sectors—is lagging behind public administration in terms of the share of creative jobs. This is not a novel phenomenon, the results of the data analysis show a similar pattern for 2005 and 2010, public administration being one of the most creative sectors. (See Table 15 in Annex.) It justifies the argument that innovation in the public sector should not be overlooked, instead it needs much more attention from both policy makers and social scientists.

Table 11. *The share of creative jobs in some sectors by country groups (2015).*
[Own calculations based on EWCS 2015.]

Sector	SCD	AGS	CON	MED	CEE	EU–27
Manufacturing, construction, and utilities	75	64	53	44	38	**50**
Retail and other services	68	42	46	39	37	**43**
Business and financial services	78	70	63	54	46	**61**
Public administration	85	75	69	59	43	**64**
Average	**75**	**59**	**55**	**46**	**39**	**52**

Legend: SCD = Scandinavian; AGS = Anglo–Saxon; CON = Continental; MED = Mediterranean; CEE = Central and Eastern European country group

Despite this inherent innovative characteristic of the public administration in every country group, there are non-negligible differences, as well. Among them, the most striking is the high rate of constrained problem solvers in the public administration of the CEE countries. (See Table 12.) The share of these jobs varies between 11–20% in the Old Member States, while— in a sharp contrast—the same ratio is 35% in case of post-socialist countries, which is 14 percentage points higher than the EU–27 average. This is also the only country group in Europe where this type of job is the most prevalent in public administration in comparison with the other three sectors investigated.

Table 12. *The share of constrained problem solvers in some sectors by country groups (2015).* [Own calculations based on EWCS 2015.]

Sector	SCD	AGS	CON	MED	CEE	EU–27
Manufacturing, construction, and utilities	16	24	24	30	34	**27**
Retail and other services	17	25	26	26	28	**26**
Business and financial services	14	17	19	17	33	**20**
Public administration	11	17	18	20	35	**21**
Average	**15**	**21**	**22**	**25**	**32**	**24**

Legend: SCD = Scandinavian; AGS = Anglo–Saxon; CON = Continental; MED = Mediterranean; CEE = Central and Eastern European country group

Concerning the Taylorised jobs, it is worthy of note that these jobs are almost missing in the Scandinavian public administration. (See Table 13.) Only every 25th employee is working in such an organisational arrangement characterised by a low level of creativity and autonomy. CEE countries are closer to the European average mainly due to the fact that the Mediterranean countries perform relatively low as well. The real breach therefore can be found not between Old and New Member States but between Mediterranean and CEE countries on the one hand, and Scandinavian, Continental and Anglo–Saxon countries on the other.

Table 13. *The share of Taylorised jobs in some sectors by country groups (2015).*
[Own calculations based on EWCS 2015.]

Sector	SCD	AGS	CON	MED	CEE	EU–27
Manufacturing, construction, and utilities	9	12	23	26	29	**23**
Retail and other services	15	33	28	35	35	**31**
Business and financial services	7	14	19	29	22	**20**
Public administration	4	8	13	21	22	**15**
Average	**10**	**20**	**22**	**29**	**29**	**24**

Legend: SCD = Scandinavian; AGS = Anglo–Saxon; CON = Continental; MED = Mediterranean; CEE = Central and Eastern European country group

In order to put the analysis in a dynamic perspective, we also calculated the distribution of different job clusters for 2005 and 2010. As Table 15 shows (see Annex), while the rate of creative jobs did not change significantly from 2005 to 2015, however, this apparent stability hides important sectoral differences. For example, the share of creative jobs decreased in the retail and other services sector, as well as in business and financial services, while in manufacturing it slightly increased. In contrast, European public administration experienced an 8 percentage point increase and became the most creative sector among the investigated four branches. This growth was primarily due to the performance of the Mediterranean, Continental and Anglo–Saxon countries, producing an impressive increase of creative jobs (the growth rate varies between 14–17 percentage points). In the Scandinavian countries this ratio remained almost at the same high level. Meanwhile, the CEE country group experienced a significant loss in creative jobs as it was already pointed out earlier in this section.

In contrast to the creative jobs, the share of constrained problem solvers decreased significantly between 2005 and 2015 in the European public administration. (See Table 16 in Annex.) This was especially true for the Mediterranean countries where the growth of creative workplaces was compensated mainly by a loss in constrained problem solvers. It is also worthy of note that in case of Anglo–Saxon group, there was a fluctuation in between the two terminal dates of the investigation. The share of these workers increased from 18% to 27% between 2005 and 2010, and then fell back to 17% in 2015. On the contrary, the share of constrained problem solvers remained the same after 2010 in the post-socialist countries (23%, 35% and 35%, respectively in the three periods).

Similarly to the previously analysed job cluster, the share of Taylorist workers also decreased in the European public administration between 2005 and 2010, but to a lesser

degree (from 19% to 15%, see Table 17 in Annex). Anglo–Saxon countries experienced the biggest loss in this regard but the share of Taylorised workers decreased in all other country groups, as well. The only exception is the CEE countries in which their share grew from 18% to 22%. Almost the same dynamics characterised the manufacturing sector: there were significantly less Taylorised workers in Scandinavian, Anglo–Saxon and Mediterranean countries, while their share remained the same in the Continental countries. The only country group where a slight increase was detected is that of the CEE countries (from 27% to 29%).

Conclusions

People are playing a key role in the public administration innovation, "…so one of the goals of public human resource management should be to support employees in innovating—that is, ensuring they have the ability, motivation and opportunity to come up with new approaches. Ability requires not just technical skills but also creativity and associative thinking, as well as the behavioural and social skills needed to bring about change." [24: 11] In relation with the types of investment in the innovation ability, the majority of efforts is focusing on the development of the "human capital" (i.e. investment in vocational education). Much less effort is taken to understand and invest into the improvement of the "structural capital". Focusing on structural capital "…may imply creating and/or implementing learning-intensive forms of organisation or technology." [16: 22]

The ambition of our analysis is to better understand the characteristics of the "structural capital" fostering innovation in public administration. To create a new innovation policy framework, it is necessary to identify the pool of creative/innovative and less creative jobs reflecting the quality of structural capital in the European public administration in comparison to other sectors (e.g. manufacturing, knowledge intensive business services, etc.).

To make a general picture on the variation in creativity in the European economy, firstly a *cross-country analysis* was carried out in an ambition to map the share of job clusters —measured by six variables presented in the methodology section of the paper—labelled as "creative", "constrained problem solver" and "Taylorist" types. Secondly, we intended to indicate the differences of job clusters by sectors (e.g. private vs. public, public administration vs. manufacturing etc.).

One of the most important lessons of this exercise is that—in spite of the 2008 financial crisis and economic downturn—every second European worker is carrying out creative/ innovative work offering them both excellent learning possibilities and a substantial level of autonomy in their job. This type of job is one key factor in developing a learning/innovative organisation. [25] The remaining European workforce is characterised—with equal shares— by constrained problem solvers and Taylorist workers. Jobs belonging to the constrained problem solver cluster offer substantial learning opportunity and rather limited autonomy. The Taylorist jobs, as an emblematic mass production type of work, is characterised by lack of learning/innovation and low level of autonomy. Patterns of job clusters' distributions remained fairly stable as compared with the three waves of the EWCS (2005, 2010 and 2015).

In addition to this rather stable European trend of job clusters' structure during the last ten years (from 2005 to 2015) visible country group and sector (e.g. private vs. public; manufacturing, services, etc.) differences were identified. In our analysis, Old Member

States (OMS) and New Member States (NMS) were distinguished. In the OMS based on their national institutional settings, four country groups were further distinguished: "Scandinavian countries", "Continental countries", "Mediterranean countries", and "Anglo–Saxon countries". In case of NMS countries, in spite of the various theoretical streams, it was not possible to identify theoretically coherent framework based sub-groups of capitalism emerging in the NMS countries.[10]

Besides significant country group differences, the cross-country comparison of the job clusters based on the surveys of the EWCS 2005, 2010 and 2015 shows noticeable variation within the country groups, too. Similarly to the other studies using the dataset of the EWCS, [20] [21] we found that the Scandinavian country group has a strong leading-edge position in the job cluster of creative workers. For example, in Sweden, Denmark and Finland three quarters of the workers belong to this job cluster before and after the 2008 crisis. In the Continental countries, the share of the creative workers is above the EU–27 average in the similar period of time. Although, significant changes did also happen in this country group: in Germany, the share of creative jobs decreased between 2005 and 2010 and increased slightly between 2010 and 2015. In the Netherlands, the decreasing trend of the creative job cluster prevailed during the whole period (2005–2015). On the "creativity vs. lack of creativity" job scale, the Taylorist work is the archetype of the routine and non-creative (non-innovative) jobs. In this job category, the OMS countries perform below the EU–27 average, with the exception of the Mediterranean country group where we found above the EU–27 average rates during all the three waves of the EWCS 2005, 2010 and 2015.

It is necessary to stress the following surprising changes within the Continental country group: following the 2008 crisis, in France the share of the Taylorist workers increased and exceeded the EU–27 average (France: 31% vs. EU–27: 27% in 2010) as well as in Germany, where the rate of Taylorist workers surpassed the EU average in 2015 (Germany: 29% vs. EU–27: 24%).

Within the Mediterranean country group, not surprisingly, Greece has a "trailing edge" position among the OMS: the share of the creative job cluster decreased by almost one third and at the same time, the rate of the Taylorist job cluster increased between 2005 and 2015. Already before the Greek crisis (2014), this country has been in the weakest position even in this country group in terms of the share of creative job cluster and had the highest rate of Taylorist workers—followed by Italy—in 2010. According to the latest survey (EWCS 2015), the share of the least creative/innovative job cluster is the highest in Greece (40%) and in Italy (38%). A significant improvement took place in Spain following the 2008 crisis: the share of the creative job cluster increased significantly (from 2005 to 2015: +10 percentage points) and the rate of the Taylorist workers decreased importantly (from 2005 to 2015: –10 percentage points).

Assessing the position of the NMS, it is necessary to call attention to the declining rate of the creative job cluster in comparison to both the OMS and the EU–27 average during the decade surveyed (2005–2015). The share of creative public administration jobs in this country group was the second highest in Europe together with the Anglo–Saxon country

---

[10]   Among the various theoretical streams, the followings, [26] [27] [28] [29] are worth mentioning. However, there is no consent among the scholars studying the emerging capitalism and identifying the diversity of capitalism in the NMS countries. Further theoretically founded empirical researches are necessary to fill this knowledge gap.

cluster in 2005, but this ratio dropped by almost 30% for 2015 and the NMS quickly became the least creative country group in terms of public administration jobs and the lagging from other European countries is more than significant.

Combining the job clusters offering the least learning opportunity and autonomy in deciding on the task order and pace of work (constrained problem solvers + Taylorist workers), we may say that the share of this combined job cluster is above the EU–27 average in the overwhelming majority of the NMS countries, the only exceptions are again Estonia and Slovenia. A particularly high share of this combined job cluster characterises the following countries: Slovakia (66%), Romania and Latvia, (65%), Hungary (63%), Bulgaria and the Czech Republic (62%), and Poland (59%).

Comparing the impacts of the 2008 crisis on the pattern of distribution of the job clusters, it is necessary to call attention to the following contrasting trends. In the OMS, a converging developing path is taking place due to the shrinking country differences. While the average of the Scandinavian and Continental country groups did not change much in the last decade, a visible catching-up trend can be observed in the Anglo–Saxon and Mediterranean countries, especially in Spain and Italy in the share of creative job cluster (even though the differences between country groups remained considerably high). In contrast, a diverging development path characterises the NMS country group. Differences in the rate of the creative job cluster between this country group and the EU–27 average increased from 7% to 13% from 2005 to 2015. The share of the Taylorist job cluster was 1% lower than the EU–27 average in 2005, and ten years later 5% higher than the EU average. Comparing the development of the "learning economy" through job cluster analysis, we may say that within the NMS, two countries (i.e. Estonia and Slovenia) are catching up to the Continental country group, and the remaining NMS countries are following the Mediterranean economic development road.

Besides the cross-country analysis, the other core aim of this paper is to outline the *sector* differences in the distribution of the job clusters. In this relation, special attention was paid to the private versus public sectors. A more detailed comparison of various sub-sectors (e.g. manufacturing, retail and other services, knowledge intensive business services and public administration) was only possible at country group level because of the low number of cases.

The analysis shows that the sectors of public administration and knowledge intensive business services are the undeniable locus of the creative jobs in all European countries according to the surveys carried out before (2005) and right after the 2008 crisis (2010). Focusing on *public administration,* we have to stress that this sector boosts creative workplaces in all country groups. In this relation, it is worth noting that even the "knowledge intensive business service" which is the emblematic sector of the learning economy is lagging behind public administration in terms of the share of creative jobs.

The public administration is operating in a challenging environment coping with the following complex policy challenges: how to simultaneously solve the problems created by the citizens' high expectations on quality services and by the fewer or stagnant level of available resources. It is clear that our analysis based on such elements of job quality as learning/creative opportunities and the level of employee autonomy is highly relevant in this regard. An increasing rate of creative/innovative jobs may facilitate the implementation of the so-called "High-Performance Civil Service" or "High-Engagement Civil Services", where "…engaged employees participate beyond the expected level and contribute actively to the success of the organisation." [30: 60] This justifies the argument that creativity/innovation

in the public sector should not be overlooked, instead it needs much more attention from both policy makers and social scientists.

It is an urgent challenge for both policy makers and other practitioners as well as for researchers to better understand the roles of human and structural capitals responsible for the development of the creative job cluster. A decade-old empirical experience showing "…very clear patterns that in countries where a big proportion of employees are engaged in discretionary learning[11] (where many ordinary workers are offered such jobs), domestic enterprises were more engaged in radical innovation." [25: 3] Finally, in observing the size of investment in the workplace innovations improving creativity of jobs, it is necessary to extend the attention from the North–South asymmetry to the North-Western vs. South-Eastern divide: the Mediterranean and the NMS countries are belonging to the "trailing edge" category in relation to the investment in workplace innovations.

References

[1]   NIELSEN, P.: *The human side of innovation systems: Innovation, new organizational forms and competence building in a learning perspective.* Aalborg: Aalborg University Press, 2006.

[2]   DUTZ, M. A., KESSIDES, I., O'CONNEL, S., WILLIG, R. D.: Competition and innovation-driven inclusive Growth. *Policy Research Working Paper (World Bank),* 5852 (2011), 1–45. https://doi.org/10.1787/9789264168305-9-en

[3]   APPELBAUM, E., HOFFER, G. J., LEANA, C.: *High performance work practices and sustainable economic growth.* Washington, D.C.: Center for Economic and Policy Research, 2011.

[4]   RAMSTAD, E.: Can high-involvement innovation practice improve productivity and quality of working-life simultaneously? Management and employee views on comparison. *Nordic Journal of Working Life Studies,* 4 (2014), 25–45. https://doi.org/10.19154/njwls.v4i4.4706

[5]   KATTEL, R., KARO, E.: Is 'Open Innovation' re-inventing innovation policy for catching-up economies? *Technology Governance – Working Papers in Technology Governance and Economic Dynamics,* 30 (2010), 1–31.

[6]   Workplace innovation as social innovation. *Dortmund/Brussels Position Paper on Workplace Innovation.* (Summary) Dortmund and Brussels, 12 June, 2012.

[7]   POT, F.: Workplace innovation for better jobs and performance. *International Journal of Productivity and Performance Management,* 60 (2010), 404–415. https://doi.org/10.1108/17410401111123562

[8]   LUNDVALL, B. A.: Why the New Economy is a Learning Economy, Danish Research Unit for Industrial Dynamics. *DRUID Working Paper,* 04 01 (2004), 1–11.

[9]   CABOLIS, C.: *Education dilemmas in the digital area.* IMD World Competitiveness Center – Criterion of the Month. September 2017. www.imd.org/wcc/world-competitiveness-center-publications/2017-com-september/ (Downloaded: 26.03.2018)

---

[11]   Note: in our analysis, discretionary learning is almost an equivalent of the creative job cluster.

[10] ALASOINI, T., LYLY-YRJANAINEN, J., RAMSTAD, E., HEIKKILA, A.: Innovativeness in Finnish workplaces: Renewing working life to bring Finland to bloom. *Tekes Review,* 312 (2014).

[11] *Powering European public sector innovation: Towards a new architecture—Report of the expert group on public sector innovation.* Brussels: European Commission, Directorate-General for Research and Innovation Publication, Office of the European Union, 2013.

[12] SZUNYOGH ZS.: Az innováció mérésének módszertani kérdései. *Statisztikai Szemle,* 88 (2010), 492–507.

[13] HOLLANDERS, H., ARUNDEL, A., BULLIGESCU, B., VIOLA, P., ROMAN, L., SIMMONDS, P. E., ES-SADKI, N.: *European Public Sector Innovation Scoreboard 2013 (A Pilot exercise).* Brussels: European Commission, 2013. https://doi.org/10.2769/72467

[14] SAARI, E., LEHTONEN, M., TOIVONEN, M.: Making bottom-up and top-down processes meet in public innovation. *The Service Industries Journal,* 35 (2015), 325–344. https://doi.org/10.1080/02642069.2015.1003369

[15] RAMSTAD, E.: A systemic framework for a broad-based innovation policy: The expended triple helix as an innovation generating policy model. *EUWIN Newsletter,* 2016.

[16] CEDEFOP: *Learning and innovation in enterprises.* Thessaloniki, European Centre for the Development of Vocational Training, and Luxembourg: Publications Office of the European Union, 2012. https://doi.org/10.2801/94281

[17] EUROFOUND: *European Working Condition Surveys (EWCS).* www.eurofound.europa.eu/surveys/european-working-conditions-surveys (Downloaded: 26.03.2018)

[18] LORENZ, E., LUNDVALL, B. A.: Accounting for creativity in the European Union: A multi-level analysis of individual competence, labour market structure, and systems of education and training. *Cambridge Journal of Economics,* 35 (2011), 269–294. https://doi.org/10.1093/cje/beq014

[19] HALL, P. A., SOSKICE, D. (Eds.): *Varieties of capitalism. The institutional foundations of comparative advantage.* Oxford: Oxford University Press, 2001. https://doi.org/10.1093/0199247757.001.0001

[20] PARENT-THIRION, A., MACIAS, E. F., HURLEY, J., VERMEYLEN, G.: *Fourth European working conditions survey.* Luxembourg: Office for Official Publications of the European Communities, 2007.

[21] VALEYRE, A., LORENZ, E., CARTRON, D., CSIZMADIA P., GOLLAC, M., ILLÉSSY M., MAKÓ CS.: Munkaszervezeti modellek Európában és az emberierőforrás-gazdálkodás néhány jellemzője – Kísérlet a munkaszervezetek nemzetközi paradigmatérképének elkészítésére, I. rész. *Vezetéstudomány,* 11 (2009), 2–15.

[22] GALLIE, D., ZHOU, Y.: *Work organization and employee involvement in Europe.* Luxembourg: Publications Office of the European Union, 2013.

[23] KESTING, P., ULHOI, J. P.: Employee-driven innovation: extending the license to foster innovation. *Management Decision,* 48 (2010), 65–84. https://doi.org/10.1108/0025174101104463

[24] OECD: *Fostering Innovation in the Public Sector.* Paris: OECD Publishing, 2017. https://doi.org/10.1787/9789264270879-en

[25] TOTTERDILL, P.: Interview with Bengt-Ake Lundvall – The Learning Economy. *EUWIN Newsletter,* 2017.

[26] MAKÓ CS., ILLÉSSY M.: Segmented capitalism in Hungary: Diverging or converging development paths? In. DETEIL, V., KIROV, V. N. (Eds.): *Labour and social transformation in Central and Eastern Europe, Europeanization and beyond.* London, New York: Routledge, 2016. https://doi.org/10.4324/9781315682112

[27] BOHLE, D., GRESKOVITS B.: *Capitalist diversity on Europe's periphery.* Ithaca: Cornell University Press, 2012.

[28] MARTIN, R.: Post-socialist segmented capitalism: The case of Hungary. Developing business systems theory. *Human Relations,* 61 (2008), 131–159. https://doi.org/10.1177/0018726707085948

[29] EYAL, G., SZELÉNYI I., TOWNSLEY, E.: *Making capitalism without capitalists: The new ruling elites in Eastern Europe.* London, New York: Verso, 1998.

[30] OECD: *Engaging public employees for a High-Performing Civil Service.* Paris: OECD Public Governance Reviews, OECD Publishing, 2016. https://doi.org/10.1787/9789264267190-en

Annex

Table 14. *The distribution of job clusters in the EU between 2005, 2010 and 2015.*
[Own calculations based on EWCS 2005, 2010, 2015.]

Country grp.	2005						2010						2015					
	Private s.			Public s.			Private s.			Public s.			Private s.			Public s.		
	CW	CP	TW	CW	CP	TW	CW	CP	TW	CW	CP	TW	CW	CP	TW	CW	CP	TW
Scandinavian	73	14	13	83	11	7	72	16	12	76	15	10	74	17	9	80	10	10
Anglo–Saxon	52	19	30	49	18	33	50	23	27	61	27	12	58	22	21	63	19	18
Continental	55	21	24	56	25	20	48	25	27	55	25	20	52	23	24	67	19	14
Mediterranean	39	27	34	41	32	27	45	19	35	48	22	30	44	25	31	52	25	23
CEE	40	33	27	52	28	20	40	29	30	44	32	24	38	31	30	41	33	26
Hungary	*40*	*31*	*29*	*58*	*25*	*17*	*44*	*30*	*26*	*59*	*25*	*16*	*38*	*31*	*31*	*38*	*29*	*33*
EU–27	**50**	**23**	**27**	**53**	**24**	**23**	**48**	**24**	**29**	**53**	**26**	**21**	**50**	**25**	**26**	**58**	**23**	**19**

Legend: CW = creative workers; CP = constrained problem solvers; TW = Taylorised workers

Table 15. *Changes in the share of creative jobs in Europe between 2005, 2010 and 2015.*
[Own calculations based on EWCS 2005, 2010, 2015.]

Sector	Scandina-vian			Anglo–Saxon			Continental			Mediterra-nean			CEE			EU–27		
	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015
MNS	73	74	75	49	58	64	53	49	53	38	47	44	38	38	38	**46**	**48**	**50**
RET	68	60	68	42	34	42	49	37	46	38	37	39	46	37	37	**46**	**38**	**43**
BFS	84	82	78	63	60	70	70	70	63	38	56	54	52	57	46	**63**	**64**	**61**
PBA	87	86	85	61	67	75	55	56	69	42	51	59	60	48	43	**56**	**57**	**64**
Average	**75**	**72**	**75**	**50**	**51**	**59**	**56**	**50**	**55**	**39**	**46**	**46**	**43**	**42**	**39**	**50**	**49**	**52**

Legend: MNS = manufacturing, construction, and utilities; RET = retail and other services;
BFS = business and financial services; PBA = public administration

Table 16. *Changes in the share of constrained problem solvers in Europe between 2005, 2010 and 2015.* [Own calculations based on EWCS 2005, 2010, 2015.]

Sector	Scandina-vian			Anglo–Saxon			Continental			Mediterra-nean			CEE			EU–27		
	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015
MNS	14	16	16	28	25	24	24	29	24	28	20	30	35	30	34	**27**	**26**	**27**
RET	16	22	17	17	29	25	22	26	26	26	22	26	28	31	28	**22**	**27**	**26**
BFS	10	12	14	20	19	17	18	15	19	28	13	17	32	24	33	**21**	**16**	**20**
PBA	9	11	11	18	27	17	26	27	18	35	22	20	23	35	35	**25**	**26**	**21**
Average	**13**	**16**	**15**	**20**	**25**	**21**	**22**	**25**	**22**	**28**	**20**	**25**	**32**	**30**	**32**	**24**	**24**	**24**

Legend: MNS = manufacturing, construction, and utilities; RET = retail and other services;
BFS = business and financial services; PBA = public administration

Table 17. *Changes in the share of Taylorised workers in Europe between 2005, 2010 and 2015.* [Own calculations based on EWCS 2005, 2010, 2015.]

Sector	Scandina-vian			Anglo–Saxon			Continental			Mediterra-nean			CEE			EU–27		
	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015	2005	2010	2015
MNS	13	10	9	23	17	12	23	22	23	34	34	26	27	31	29	**26**	**26**	**23**
RET	16	17	15	41	36	33	29	37	28	36	41	35	26	32	35	**32**	**36**	**31**
BFS	7	6	7	17	22	14	12	14	19	34	31	29	16	20	22	**16**	**19**	**20**
PBA	4	3	4	21	5	8	19	17	13	23	27	21	18	17	22	**19**	**17**	**15**
Average	**12**	**12**	**10**	**30**	**24**	**20**	**22**	**25**	**22**	**33**	**34**	**29**	**25**	**29**	**29**	**26**	**27**	**24**

Legend: MNS = manufacturing, construction, and utilities; RET = retail and other services;
BFS = business and financial services; PBA = public administration

Essential Requirements for Hungarian Police Measures

György POKRÓCOS[1]

The general police measure related to the expectations I have gathered for the Hungarian policing measures is clearly recognisable by everyone. This can be said by the realisation of the criteria that the police measure was in order, achieved its purpose and met the requirements. I approached this topic from a legal and ethical point of view and I make a written proposal.

Keywords: *Hungarian police measures, lawful measure*

Introduction

Appropriate police measures can only be taken if they are based on sound foundations, that is, the theoretical knowledge of the policing police is assertive and assists in the formation of a positive police image. Law enforcement is a part of public administration, and public administration administers public functions with public authority powers. The resulting police image can be directly or indirectly associated with the state represented by the police officer. Police action must therefore meet a wide range of expectations in order to meet the requirements of the police. The requirements can be divided into objective and subjective pages. On the objective page are the laws, compliance with internal norms, commands and instructions, compliance with the instructions, completion of the action and its successful fulfilment. On the subjective side there is morality, ethics, culture, communication, style, which cannot be determined in a given law, but they do affect the mood, tone and end result of the action.

If there is no commonly accepted (collective consensus-based, consensual) value system in a society, then that society cannot last too long. If a statement (assertion, judgment) does not apply to what is good or bad, but to what is true and what is false, it is not a value judgment but an act. The task of public administration is to maintain the consensus values and security of the society at an acceptable level. If an event, story, action or measure is ethically not bad, in other words it is not to be rejected, i.e. it is not "undesirable" then it is not true that it is "desirable" but merely acceptable. The outcomes of certain events are within the scope of the agents of the society, other events are beyond the reach of force majeure cases, unforeseen natural disasters. Events are always risky; at most, their risk is negligible in certain circumstances. Absolute truth is that there is no absolute security. [1]

[1]   LL.M. media law specialist, Ph.D. student, National University of Public Service, Doctoral School of Public Administration Sciences; e-mail: dr.pokrocos@gmail.com; ORCID ID: 0000-0002-9831-7422

The objective conditions can be determined in some form. Here are the laws, normative instructions, commands and briefings. These include the conditions that must be met at every stage of action; the absence of any of these circumstances raises the responsibility of the police officer. The tactical methodological guide currently in force came about by the death of a policeman shot down in Esztergom during police action. Following his death, the police tactical training in Hungary began.

What is the Command?

No matter how strange, there is no command as a definite, specific concept either in the Police Act (the Hungarian abbreviation is: Rtv.) or in the Service Regulations. The Police Act is even more incomprehensible in this regard since the Service Regulation deals with the definition of the command, the issuing and implementation of a specific order. Although the Rtv. deals with the organisation and direction of the police, still each organisational unit operating under a sub-hierarchy determines its own leadership. Such a bureaucratic organisation is, according to Max Weber, the best possible ideal organisational form characterised by division of labour, formalism, service path, hierarchy, lack of integrity, objectivity, office-affairs, appointment status and written regulation. The question of a written regulation raises the requirement that in cases of substantive relevance which may have criminal consequences may be a criterion of literacy.

Turning the thread of thought backwards, the significance of the command becomes apparent if the command is not executed or violated. In another non-military organisational unit, this may have labour law and disciplinary consequences; the contractual relationship of the civil law constitutes a breach of contract, while in law enforcement the execution of a command or order may even be a criminal offense.

The police's decision and action must be objective, impartial and independent. Consequently, the official person performs a judicial activity towards the citizen. His merit "judgment" activity, therefore, cannot be influenced by a service command, which is a means of controlling military activity. Acting in matters falling within the jurisdiction of the police, the superior may issue a service order or order naturally in matters of administrative competence, but not the substantive judgment of a particular case.

The Objective Criteria for Each Measure are as Follows

Lawfulness: The measure is lawful if the service of the police takes place in accordance with the established duties and the duties of the law in force and other legislation (including internal travel, commands, measures, etc.) Lawfulness is fulfilled if the policing officer complies with the regulations in force and accomplishes his or her duties in the service, in case of his or her jurisdiction. Knowing legislation is therefore an indispensable prerequisite for the police profession, as observing and enforcing them is one of the tasks of the police.

Professionalism: The measure is appropriate if its implementation is carried out in accordance with the provisions of the regulations in force and the related necessary

techniques. The notion of professionalism involves the notion of legality. In order to talk about the provisions of the regulations in force, we also have to comply with legality. Legality is complemented by the tactics and techniques required to match professionalism. Practice is coupled with theoretical knowledge. Tactical and technical tricks and procedures are already part of the internship, no matter that they are self-defence or procedural tactics. It is necessary to know and examine a particular case, since it cannot be stated that a particular method can be applied appropriately for each type of action.

Proportionality: The measure is proportional if it does not cause any disadvantage that is manifestly unrelated to the legitimate purpose of the measure which, in addition to ensuring effectiveness, with the slightest limitation or damage is chosen from among several plausible and appropriate police measures or coercive measures. Proportionality under Section 15 of the Police Act seems to indicate that a police measure cannot cause any disadvantage that is manifestly unrelated to the legitimate aim of the measure. There are several possible and appropriate police measures or coercive instruments to choose.

Effectiveness: The measure is effective if it reaches its legitimate aim, prevents and abolishes conflicts and violations, meets the needs of society and public security for public order. One of the most important criteria of effectiveness is the statutory limitation set by law. Target bounds may vary by type of action, but must always comply with the provisions of the Fundamental Law. [2]

Objectivity: The measure is objective if the policeman takes action unbiased. Discrimination on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation is prohibited. The police officer is obliged to act impartially in accordance with the law. Specific data referring to racial origin, religious beliefs, sexual behaviour and political opinion can only be treated if it is a factual element of a criminal offense that is the subject of a law enforcement activity or the person concerned gives his or her consent in writing.

Safety: The measure is safe if the people or things involved in the measure do not have a higher risk or harm or injury than is warranted. In the selection of police measures and in their practical implementation, the policeman should endeavour to implement tactics and techniques that meet the listed objective criteria. If these conditions are fulfilled, then the public intervention is unquestionable, and thereafter may be a criticism of "just" no-liking, but it is difficult to start with, since the expectations are per measure and per person.

In addition to objective circumstances, it is important for the police officer to meet certain subjective factors in order to create a proper culture and to create a police image in connection therewith. The subjectivity and objectivity limit cannot always be clearly separated, as certain rules can be demanded on an objective and subjective side. At the same time, subjectivity is much closer to morality, ethics and behavioural culture than to a specifically defined norm.

Substantial factors are voluntary abandonments, limitations of fundamental rights, and general expectations unpublished by society, which are close to the ideal police image. A policeman is ready to be there and be available if somebody has to be punished, but in a differentiated manner, rather indulgent and forgiving.

Companionship to the board is expressed by the swearing-in at the time of the assignment, which also has a symbolic value. The issue of integrity is not a trade-related one. Duty of Honor, Honesty and Discipline is a General Virtue, not necessarily only for Police Officers. The civil society does not accept any behaviour that is contrary to them, but for a member of an armed

body it is a basic expectation. The office requires that the confidence in the state apparatus and the official person should not be compromised, and the people representing them should be worthy of their duties. Violence is accepted if it is used in the right place, manner, time and extent for the purpose to achieve the legitimate goal. Objectivity is uniform for all conditions and for all other measures. People are abused and hurt because of selfish interests, abusive conduct and revenge, still this is a criminal offense. It is the responsibility of a professional police officer to take action against it. This responsibility can be social, pertaining to labour law or criminal. It is most difficult to define social responsibility as a specific measure can be used to determine how the police action had replaced the requirements imposed upon it or caused a situation that is not unlawful but socially condemnable. Labour law responsibility is most commonly the disciplinary offense of misdemeanour and damages. One of the requirements of a professional policeman is to make decisions when working. These decisions can be good or bad, therefore objectivity is one of the most important expectation in the course of a proper and continuous training of the professional apparatus. A lawful measure can also be implemented if the police's theoretical knowledge is appropriate and can apply additional tactical and technical knowledge based on theoretical knowledge. There are strict legal regulations in force regarding data protection, which the police has to comply with. During the action, the police may have access to various sensitive data, which is their duty to preserve. It is also inconceivable that you never make any negative statements about your own employer or staff. The rules of dressing specifically define which outfit to wear and what accessories. The position of the uniformed staff is simpler in this respect, as they do not have the freedom of dressing. In civilian clothing, the freedom to choose one's outfit is dependent on good taste, but it is expected that it will not be compelling or challenging in any way and it also should not express any affiliation whatsoever.

Police uniforms in the public area most often meet the citizens' expectations. Their work and often the whole police will be judged by their dress, behaviour, speech, professional skills and style. The police are expected to act exemplary, do not commit criminal offenses, any offenses, do not waste life, do not gamble or lead a scandalous and intemperate life. Such a behaviour often involves the violation of many other points in the Code of Ethics.

Communication

On the subjective side I would also include police communication, since the realisation of the objective conditions has to be known to the outside world in some way and it is only possible through communication. Acceptable police communication facilitates police action; it is a part of the culture of action. It can create a positive police image, but more importantly it can help to achieve the legitimate goal of avoiding the use of legal physical violence. If a police officer can adequately perform good communication, it can make a disadvantageous situation look less harmful. Every organization and the leaders thereof want to be successful in their work. This requires the understanding, recognition, support, acceptance and appreciation of the environment communicating with them, alien to their reputation, acknowledgment and acceptance. Reputation, therefore, means the expression and appearance of public opinion, the knowledge, experience, image of our consciousness, a picture of the general characteristics of a given organization or its member.

We can formulate the following expectations regarding communication: [3]

Rapid Response: A police officer in a given situation is responsible for coordinating the police action, that is to say, he is the master of the case. As a matter of the case, you are expected to respond primarily to the events, to recognise the situation and to handle it. The sooner and the more is done to ensure that the victims of the events are well informed about the issues they face, about the realistic threats and how they can be remedied, the sooner and the better we can report bad news.

Credibility: When it comes to police communication – no matter in what kind of form – citizens tend to identify the entire police with the communicator and their reputation is built on this. The policeman, who has a negative police image, will also behave negatively during a police communication. Credibility is also important for gaining and retaining the confidence of citizens and for preserving public confidence in the activities of the relevant body of the police and public officials.

Consistency: There are no two identical police measures, as the people performing the action are not the same. As two people are different from one another, so are two police measures different from one another. It is an important requirement of the police officers to have a united communication, i.e. the police on the spot should communicate the same position, instead of arguing with their counterparts.

Consistency: Consistency requires that, as we communicate, we respond similarly to similar situations of life. Life situations may be similar, still they are not the same and one needs to be able to detach himself/herself and handle each case objectively and communicate accordingly.

Understanding: Police communication must be clear to everyone. The parties opposing the acting police officer are not required to know the internal rules. The acting police officer commences, conducts and finishes the proceedings as a matter of course, in which he must communicate in an intelligible manner to the parties in order to avoid misunderstandings and paralyses. You have to steer the action, but this is only possible if your partner in communication understands it and accepts the signals from the police officer.

Impartiality: The police are the neutral party. Any contrary communication, expression should be avoided and prohibited.

Appropriate communication enriches the culture of the measure, increases trust in the police and helps to avoid conflicts. More detailed rules could be addressed in a separate study.

Tourist Police Seasonal Programs

Several county police headquarters have signed a cooperation agreement with the schools in their area, whereby pupils studying there can provide community service, and for years, college students have also helped the work of the police in tourist-frequented places mainly by interpreting and providing information and guidance. They provided tourists with crime prevention and tourist bulletins. Young people working with the police helped to find abandoned and lost property.

The Tiszai Water Police Department of the Jász-Nagykun-Szolnok County Police Headquarters along with the Szolnok College and with the support of the Hungarian Tourist

Office launched the Tourist Police program on 20th July 2015. By 20th August 2015, the college students helped the police work in the area of competence of the Tiszai Water Police Department in tourism-frequented areas such as Szeged, Csongrád, Tiszakécske, Szolnok and Kisköre. The students who spoke foreign languages helped the work of the volunteers by interpreting. The tasks of the students included filling out questionnaires provided by the College of Szolnok and the Hungarian Tourist Office, disseminating other publications and keeping in touch with the local Tourinform Offices. [4]

The Szabolcs-Szatmár-Bereg County Police Headquarters in Nyíregyháza also guarded the security of those seeking relaxation by a beach director and Tourist Police. During the tourist season, the staff of the Nyíregyháza Police Station paid special attention to the places visited by tourists and those who wanted to relax. In the summer, young people speaking foreign languages drew attention to ways of preventing crime. In the tourist season, high school students speaking foreign languages, who served their volunteer community, helped to provide information to visitors of Nyíregyháza. For the first time, the Tourist Police Service has been supplemented by Transylvanian students so that tourists from Romania can also be better informed. Hungarian-speaking Transylvanian students served in Nyíregyháza–Sóstógyógyfürdő in the team of the Crime Prevention staff of Nyíregyháza from 20th July to 25th July 2015. [5]

In the area of the Baranya County Police Headquarters, pupils with community service speaking foreign languages were at the disposal of tourists and foreigners. In a pavilion set up for this purpose, crime prevention and tourism bulletins were available and helped to guide them. The Baranya County Police Headquarters concluded a cooperation agreement with several schools in Pécs, Mohács, Hops and Pécsvárad, whereby pupils studying there were in their service from 1st July to 31st August 2015. [6]

The Heves County Police Headquarters provided the opportunity for students in Eger and Gyöngyös between the 15th of June and the 30th of June 2015 to fulfil the required fifty-hour community service in the law enforcement area. The purpose of the program was to help high school students during the summer tourist season to assist in the police's crime and accident prevention work with interpreting, as well as providing information and guidance to tourists, mainly foreigners. The students took part in a general training on the 15th of June 2015 and soon after started a kind of professional training with uniformed police officers. [5]

Summary

The task of the police is to ensure that the task of law enforcement is accomplished by scientific means and methods. Magyary Zoltán, the father of the Hungarian public law, says in connection with this: "Due to the specificity of the task of law enforcement, the legislature is forced to abstain from the detailed regulation of the tasks and to consider the discretion and choice of the authorities which are more familiar with the unforeseen circumstances of the incurred or threatening disorder, to confine themselves to the establishment of legal barriers to threats." [7] Constructing the right concepts and funds is thus left to the care of the profession, even if it is initiated by law.

Feedback on the measures and confidence in the police is regularly done by specialised institutions. About 10 years ago, TÁRKI conducted the New Europe Barometer survey

in Hungary in 2005. [8] During the research, the opinion of the population on the crime prevention work of the police was investigated among 13 countries of the post-socialist block. Of the 13 countries, the highest recognition of the police was in Hungary, with the surveyed population in Hungary saying that the police worked well. In another study, the TÁRKI Social Research Institute Value Creation reported—in a Polarizing Political Space—entitled *The Social/ Cultural Conditions of Economic Growth,* [9] which was conducted in Hungary on the role of trust, norm tracking, state role and democracy. The culture and acceptability of police measures are, according to the opinion, appropriate.

Nearly 10 years after the results of the investigation, in the opinion of the Hungarian Academy of Sciences, the police enjoy most of the citizens' confidence. In contrast, according to other social institutions, there is more distrust than trust. As a conclusion of my study, I believe that policing measures in line with the listed criteria are characterized by the police's work, the justification of which is also reflected in the data of the social research institute.

References

[1] BUKOVICS I.: *A fenntarthatóság, mint katasztrófaelméleti probléma. Fenntartható fejlődés Magyarországon – jövőképek és forgatókönyvek.* Budapest: Új Mandátum Könyvkiadó, 2006.

[2] *Fundamental Law, Article 46: The primary task of the police is to prevent, detect crimes, protect public security, order and rule of law.*

[3] *Information on the Order of Information to Media Providers 10/2013. (III.14) ORFK instruction.*

[4] *Jász-Nagykun-Szolnok County Police Headquarters.* www.police.hu/ugyintezes/szerv/ orszagos-rendor-fokapitanysag/jasz-nagykun-szolnok-megyei-rendor-fokapitanysag (Downloaded: 22.02.2018)

[5] *Szabolcs-Szatmár-Bereg County Police Headquarters.* www.police.hu www.police.hu/ ugyintezes/szerv/orszagos-rendor-fokapitanysag/szabolcs-szatmar-bereg-megyei-rendor-fokapitanysag (Downloaded: 22.02.2018)

[6] *Baranya County Police Headquarters.* www.police.hu/ugyintezes/szerv/orszagos-rendor-fokapitanysag/baranya-megyei-rendor-fokapitanysag (Downloaded: 22.02.2018)

[7] MAGYARY Z.: *Magyar közigazgatás.* Budapest: Királyi Magyar Egyetemi Nyomda, 1942.

[8] TÁRKI: *Új Európa Barométer vizsgálat.* Budapest: Társadalomkutatási Intézet Zrt., 2005.

[9] TÁRKI: *A gazdasági növekedés társadalmi/kulturális feltételei.* Budapest: Társadalomkutatási Intézet Zrt., 2008.

Public Administration in Palestine

Saqer SULAIMAN[1]

The Palestinian administrative system is distinctive, relative to either the historical context or the political environment. The former is characterized by the absence of a national power, while the latter is perpetually unstable. The state-building process in Palestine has followed an inverse path, in that staffing preceded the drafting of structures, while goals and job descriptions have been pre-empted by seemingly random political appointments.

This study focuses on the history of this public administration, its main characteristics, and the system's efficiency. The methodology is descriptive. The paper demonstrates that, in spite of obstacles such as the restrictions of the occupation and the shortage of resources, the Palestinian administrative system is progressing. This progress was most obvious during the last years because of good governance practices, especially the reduction of expenditures and the improvements in public services. The Palestinian administrative system still suffers from problems like over-staffing, poor institutional coordination and inadequate attention to the agriculture and industry sectors, which limit progress and increases the public debt.

Keywords: *efficiency, administrative system, performance, public administration*

Introduction

Public administration is one of the most important pillars of the state in order to provide its services and achieve its development goals. "Administration is the most obvious part of the government; it is the government in action; it is the executive, the operative, the most visible side of the government, and is of course as old as government itself." [1: 198] Governments work constantly to improve performance and efficiency; however, institutional performance is an integrated system requiring interaction with both internal and external actors. As While Qaryouti pointed out: "The organizational efficiency is the organization's ability to achieve both long-term and short-term goals that reflect the balance of influential powers and stakeholders' interests". [2: 104] Robin and Wiersema linked performance with the ability of an organization to achieve long-term goals, which is to survive, the ability to adapt to changes and growth. [3: 278]

The peculiarities of the Palestinian situation result from the fact that the Palestinian National Authority (PNA) built its institutions and carried out its duties under military

---

1   Ph.D. student, National University of Public Service, Faculty of Science of Public Governance and Administration; e-mail: Saqersul@yahoo.com; ORCID ID: 0000-0002-4866-7694

occupation. The ability of the PNA ministries and institutions to survive and to provide services to the citizens in these complicated circumstances is both astonishing and tenuous.

This paper tries to answer three key questions: How is the public administration established in Palestine? What factors affect the performance of the public administration in Palestine? Is the Palestinian public administration efficient or not?

The Establishment of Public Administration in Palestine

Historically speaking, Palestinians have had little opportunity to practice public administration, as foreign states have ruled them from the Ottoman era (c. 1300) to the Israeli occupation (since 1949). From 1967 to 1993, the Israeli Military Occupation controlled all institutions and government offices in the West Bank and the Gaza Strip. Occupation policies mandated the subordination of Palestinian institutions and the Palestinian economy to their Israeli counterparts.

The Oslo Accords signed in 1993 between the Palestinian Liberation Organization (PLO) and the Israeli Government led to the creation of the PNA. The Central Council of the PLO in its setting in October 1993 authorized its executive committee to establish the PNA council. The President of the PNA was the President of the PLO, and most of the PNA leaders were, at the same time leaders in the PLO. [4: 66] This overlap in function and responsibilities between these two bodies increase "[T]he vague relationship between PNA and PLO institutions hindered the establishment of a proper governance system that is characterized by transparency, separation of powers, and rule of law". [5: 4]

Factors Affecting the Performance of Public Administration in Palestine

Public Administration in Palestine represents a unique case due to the continuity of occupation and the absence of control on resources. The PNA initiated its bureaucratic institutions and departments in an unstable political situation and unclear economic environment. In general, the main characteristics of the administrative system in Palestine can be summarized as follows:

- *Political Instability*
  The PNA thus has been working in an uncertain environment since its inception. This restricts its ability to provide public services in vital areas such as education, health and social welfare. Actually, "how Palestinian public administration was able to survive and function under incredibly hostile circumstances and insurmountable obstacles present a challenge to both scholars and practitioners in the field". [6: 1] Policymaking lacked continuity, as it was influenced by the absence of stability in the political arena.
- *Limited Sovereignty and Occupation Restriction*
  Moreover, the Oslo Accords did not give the PNA full sovereignty on all Palestinian territories. Indeed, this agreement divided the Palestinian land into three areas, i.e. A, B and C. The PNA granted full control over area A only, which constitutes about 18% of the total area "while Most of the Palestinian territories (areas C and B) and people

are still under occupation and the government prevented from utilizing and using its natural resources". [7: 1] Whereas this is not the case in the independent countries, in which the governments have full sovereignty and power to access and utilize their national resources without external restrictions. "The provision of public service to the local population was drastically affected especially in area C where large numbers of people live and depend on the government for essential services such as health and education." [6: 4]

Another main obstacle faced by the PNA is that Israeli authorities control all border-crossing points, and all raw materials and machinery are subject to inspection by the Israeli army. One of the worst examples of the Israeli authorities' control over the life of Palestinians is the clearness revenues. The Israeli authorities collect these revenues and then transfer them to the PNA. Sometimes the Israeli authorities hold over these revenues for political reasons. [7: 6]

In addition, Israel often interferes in the activities of international aid agencies. International development agencies reported in 2011 that Israeli policies forced these agencies to change their programs. [8: 2] The resulting programs are often less effective and do not serve the most vulnerable and poor people.

- *Patrimonial State and Political Appointment*
  Patrimonialism is a form of governance in which all powers flow directly from the leader. Historically, the Palestinian presidents practice the rule of the father within the family. Usually, the employees either civil or military are more loyal to the leader. One of the main features of the public administration in this kind of patrimonial state in Palestine was the political appointment based on party affiliation and loyalty "spoil system" "what determine the relations of the administrative staff to the chief is not the impersonal obligations of office, but personal loyalty to the chief". [9: 79] This created job duplication, and a complex bureaucracy that depleted financial resources without necessarily providing any services.

- *Resource Shortage and Dependency on International Support*
  The Palestinian Government, therefore, has relied on international aids for much of its funding. "The international assistance to the Palestinians from 1994 to 2000 totalled about $3.3 billion, an annual average of about $500 million." [10: 28] Whether or not this aid helps Palestine as intended, however, remains an open question. Al-Abed stated that the international aid helped Palestinian cover part of its deficit and supports some development projects. Other scholars argue though, "despite its importance, the international assistance effectively embodies an external constraint since it increases the dependency of Palestinian economy on external sources and exerts pressures on PNA's leadership options and priorities". [7: 7]

  Additionally, the goals of donors sometimes conflict with those of the PNA. The other main risk is that aid has transformed the PNA into a non-governmental organization whose main job is to facilitate projects financed by donors.

Corruption and Weakness of Accountability

Corruption is still one of the main obstacles to institutional development in the Arab and developing countries. In Palestine, the surrounding internal and external negative environment played a role in hampering anti-corruption efforts. According to Transparency Palestine (2016) "the continued Israeli occupation, the absence of the role of the Legislative Council, and the decline in public trust in the performance of the judicial authority are the main elements that hamper anti-corruption efforts". [11: 15]

The Efficiency of the Palestinian Public Administration

The efficiency of any government is manifested through its ability to manage the state resources to achieve the desired result with a minimum cost. In order to maximize their efficiency, governments should adopt clear administrative and financial policies and flexible structure that guarantees accountability and distribution of responsibilities. This paper discusses briefly the efficiency of the Palestinian Government through two main perspectives. The first one is the administrative perspective that implies accountability and distribution of responsibilities. The second is the financial perspective that implies efficiency in resource management.

Administrative System

The efficiency of the administrative system in Palestine has improved during the last ten years. The performance of many of the existing institutions compares with or even exceeds their counterparts in many countries. [12: 4] Moreover, the donor governments considered the Palestinian governmental reforms implemented over the last 10 years a resounding success. [8: 2] The PNA enacted laws organizing pensions, labour, local government and the civil service. The Basic Law was also amended and so on. In addition, the government reduced the employment rates and adopted evidence-based policies such as the national policy agenda.

The Palestinian administrative system still suffers from overstaffing though; the number of Palestinian public employees per capita is one of the highest in the world. Even though the percentage of salaries and wages of the government employees have decreased from 63.3% in 2002 to around 50% of the total public expenditure of the annual budget in the later years, [7: 53] their percentage is considered very high in comparison with other expenditures. (See Figure 2.)
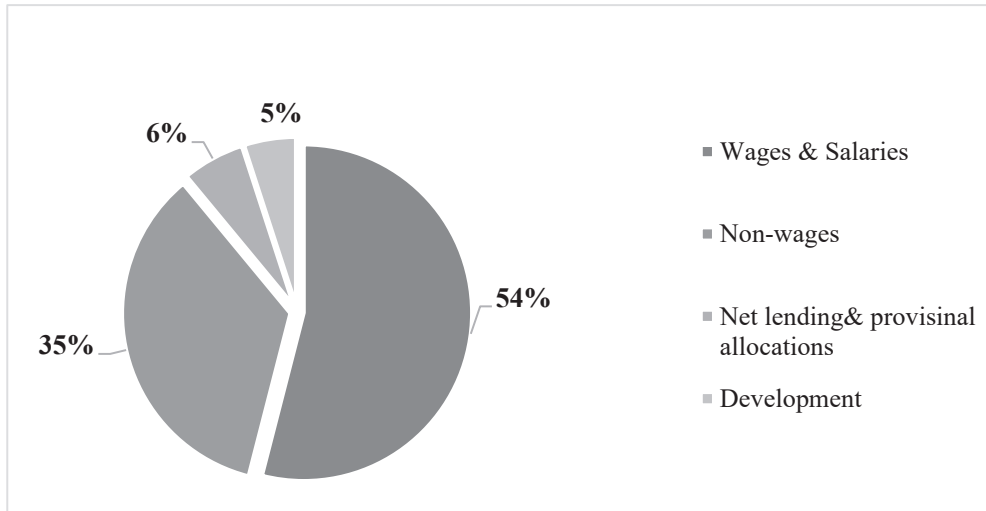
Figure 2. *The structure of Public expenditure in 2016.* [13: 8]

As the above-mentioned figure shows, the wages and salaries consumed 54% of the governmental budget, while the developmental projects and activities, for example, received only 5% of the budget.

Conflicts of powers also persist and lead to poor coordination between institutions and authorities. Despite the separation of powers stipulated in the Basic Law, overlapping mandates are common, and ambiguities in the legal texts often lead to conflict or misinterpretations. [14: 20] According to Article 61 and Article 62 of the Basic Law, the power and responsibilities of the Palestinian Legislative Council (PLC) include the approval of the general budget. [15] This prerogative has been undermined since the termination of the Hamas Government in 2007, since that time, the approval of the budget becomes the responsibility of the President.

There is also conflict between the executive and the judiciary authorities over the administrative supervision of courts, and another problem is the disrespect for judiciary decisions by the executive authority. [14: 24] The last example is related to the distribution of responsibilities between the Presidential Office and the Government. The post of Prime Minister, created in 2003, relatively restricted the President's power in favour of the Council of Ministers; however, the President's mandate simultaneously expanded as the legislative council weakened. Laws have been replaced by presidential decrees.

Financial Perspective

The Palestinian financial performance has improved gradually throughout the years. The government has taken some financial procedures in order to increase its efficiency. The government has recently reduced the salary bill by lowering the rate of employment. At the same time, the government reduced the subsidies for some sectors such as petroleum, restructuring

and electricity. Meanwhile, the executive power tends to speed up modification of the laws affecting the budget such as income tax law, public budget law, public debt law and civil service law. Consequently, the recent years have witnessed a remarkable improvement in the Palestinian economy. For example, "the growth in net public revenues during 2016 (20.4%) which was larger than that reported in public expenditure (6%), reduced the total budget deficit by around 55.2% to NIS 1.2 billion compared with 2015". [16: 10] At the same time, the percentage of the actual deficit to the total GDP increased in general "up to about 23% per the year 2009, then it decreased yearly until it reached about 5% in 2014". [7: 89] The budget has maintained this percentage of deficit during the previous two years. This decline shows an evolution in the financial performance of the Palestinian Government and the success of the fiscal policies of this government.

Data shows that there was little change in the composition of GDP over the consecutive quarters of financial years. "The absolute increase in the GDP between Q1 2016 and Q1 2017 amounted to about US$ 13.5 million, a growth by 0.7% which was achieved despite the decline in aggregate consumption expenditure (private and public) by US$ 3.2 million." [17: 3]

Regarding public debit, the Ministry of Finance data shows that this ratio has started from zero then increased gradually and wobbled according to the general economic conditions and international aid. "The public debit ratio to GDP reached 20.1% in 2015, but it decreased to 18.5% in 2016, where the public debt reached approximately NIS 9.6 billion, registering a slight decline compared to 2015." [18: 11] This decline came out as a result of the fiscal discipline policy and the rationalization of expenditures.

Meanwhile, the government's ability to collect taxes improved during the last years in such a way that "the contribution of taxes is currently between 19–22% of the GDP which is nearly the same of the surrounding countries." [19: 9] Undoubtedly, the development of the general revenue administration positively affected the collection of taxes. Meanwhile per capita share of GDP has fluctuated between periods of growth and periods of decline; according to the Palestinian Central Bureau of Statistics "the per capita share of the GDP in 2016 reached 1997 US per capita". [20: 2] It is the highest rate in twenty years.

The Palestinian financial performance still has shortcomings though, including an imbalance between the main operational sectors in Palestine. "Agriculture's share has declined; manufacturing has weakened in the absence of a national policy to build a modern industrial base; public and private sectors services dominate the structure of the economy, GDP, and employment with a big share constituted by public administration." [21: 9]

The agriculture share of GDP decreased from 12% in the mid-nineties to only 3% in 2015, at the same time service employment has increased at an annual rate of 0.75%. [22: 2]

The dominance of the service sector raises questions about its ability to produce economic growth in light of the weakness of investment opportunities. The commitment of the government to allocate all available financial resources to meet the current expenditure (primarily salaries and wages) has weakened its ability to invest in the construction and renovation. "The contribution of public investment in GDP in recent years, ranging between 2–4% per year." [19: 9]

Generally speaking, the budget of the Palestinian Authority suffers seemingly permanent deficits; they fluctuate largely with donor support.

Conclusions

The two main obstacles that restrict the ability of the PNA to build a sustainable institution and independent economy are occupation restrictions and a shortage of resources. Israel dropped the burden of government on the shoulders of the PNA, but it has not transferred to the PNA the necessary powers and resources that could help in building institutions of state or sustainable development. Actually, it is difficult to achieve sustainable development and institutional building in the presence of the occupation and its obstacles.

Public administration in Palestine nonetheless has made a slight progress. The government reduced the deficit, reduced the salary bill, restricted employment, reined in government spending, and increased tax collections.

The organized administrative system in this sense is a tool to develop more cohesion policies and initiatives in the course of which the need for administrative efficiency and the need for flexibility coexist. To achieve more changes on the domestic level, a robust accountability system, partnership between the Government and non-governmental organizations, restructuring the public sector to ensure an efficient allocation of functions and creating institutions with clear responsibilities and accountability should follow. To achieve a balance, a re-consideration of the agriculture sector is necessary, as is the adoption of vocational and technical training policies.

References

[1] WILSON, W.: The Study of Administration. *Political Science Quarterly,* 2 6 (1887), 197–222. https://doi.org/10.2307/2139277

[2] QAROUTI, M.: *Organizational Theory and Organization*. Amman: Dar Wael for Publishing and Distribution, 2000. (Translated from Arabic.)

[3] ROBINS, J. A., WIERSEMA, M. F.: A Resource-based Approach to the Multi-business Firm: Empirical Analysis of Portfolio Interrelationships and Corporate Financial Performance. *Strategic Management Journal,* 16 (1995), 277–299.

[4] GAGMAN, G., KHALIL, A., SHUAIBI, A., DWEIK, A., GEOSY, M., Al ARIAN, H.: The experience of the Palestinian political system under the Palestinian Authority. In. *The Palestinian political system and the peaceful transition of power.* Ramallah: The Palestinian Institute for the Study of Democracy – Muwatin, 2013.

[5] SAID, N., BADAWI, W.: *Public Administration in the West Bank & Gaza: Obstacles and Opportunities.* www.researchgate.net/publication/242148250_Public_Administration_in_the_West_Bank_Gaza_Obstacles_and_Opportunities (Downloaded: 15.02.2017)

[6] SHAHWAN, O.: *Building and rebuilding public administration in Palestine.* http://egpa2007.inap.map.es/egpa2007/workshops/WSI/WSI_Shahwan.pdf. (Downloaded: 17.03.2017)

[7] Al-RAZEQ, A. O.: *Assessing Fiscal Policies of the Palestinian National Authority*. Ramallah: Palestine Economic Policy Research Institute (MAS), 2016.

[8] SHIGAGI, I., SERINGO, G.: *Separation of Government from the Economy in Palestine: A recipe for a Failed State.* https://al-shabaka.org/briefs (Downloaded: 11.03.2017)

[9]   BROWN, D.: *The State and Ethnic Politics in Southeast Asia*. Routledge, 2003, 114. https://doi.org/10.4324/9780203209097

[10]   *Final Report Round Table Discussion (9), The Palestinian Economy After 20 years of Oslo Accords.* Ramallah: Palestine Economic Research Institute (MAS), 2013.

[11]   *Integrity and Combating Corruption, Ninth Annual Report.* Ramallah: Transparency Palestine, 2016.

[12]   KASSIS, N.: *Building an Efficient and Effective Public Administrative Structure despite Geographical Separation.* Ramallah: Palestine Economic Policy Research Institute (MAS), 2011. www.mas.ps/files/server/20141911094304-1.pdf (Downloaded: 16.01.2017)

[13]   *Social and Economic Monitor.* Ramallah: Palestinian Central Bureau of Statistics, Palestine Economic Research Institute & Palestine Monetary Authority (MAS), December 2016.

[14]   *Conflict of power and the absence of responsibility in the Palestinian National Authority.* Ramallah: Coalition For Integrity and Accountability – AMAN, 2007.

[15]   *Palestinian Basic Law, 2003.* www.palestinianbasiclaw.org/basic-law/2003-amended-basic-law (Downloaded: 11.05.2017)

[16]   *Social and Economic Monitor.* Ramallah: Palestinian Central Bureau of Statistics, Palestine Economic Research Institute & Palestine Monetary Authority (MAS), May 2017.

[17]   *Social and Economic Monitor.* Ramallah: Palestinian Central Bureau of Statistics, Palestine Economic Research Institute & Palestine Monetary Authority (MAS), September 2017.

[18]   *Social and Economic Monitor.* Ramallah: Palestinian Central Bureau of Statistics, Palestine Economic Research Institute & Palestine Monetary Authority (MAS), May, 2016.

[19]   Al-ABED, T. G.: *Palestinian Economy: The Way to a Better Future.* Ramallah: Palestine Economic Policy Research Institute (MAS), 2016. www.mas.ps/files/server/20173001150012-2.pdf (Downloaded: 15.01.2017)

[20]   *Social and Economic Monitor.* Ramallah: Palestinian Central Bureau of Statistics, Palestine Economic Research Institute & Palestine Monetary Authority (MAS), September 2016.

[21]   KALDI, R.: The Most Prominent Features of the Palestinian Economy. In. *Towards a New Vision for the Revival of the Palestinian Economy, final report.* Ramallah: Palestine Economic Policy Research Institute, 2016. 1–32.

[22]   FALAH, B: *Structure of the Palestinian Services Sector and its Economic Impact.* Ramallah: Palestine Economic Policy Research Institute (MAS), 2013. www.mas.ps/files/server/20141911103121-1.pdf (Downloaded: 09.01.2017)

Thoughts on Certain Aspects of the Brexit and its Management

Bálint TELEKI[1]

This article examines certain aspects related to Brexit and its management—both from the side of the UK and the EU. We search for the answer to such questions, whether the Brexit is a crisis, and if so, then what certain effects can it have on the economy, society, everyday life, etc. of those involved, and if these effects were and are handled properly by those in charge. In addition, we review the timeline of Brexit, including the planned dates and events. The institutional background of the crisis management will also be examined in case of both parties.

Keywords: *Brexit, crisis management, devolved administrations, European Commission, European Union, financial-economic crisis, nationalism, United Kingdom*

Introduction

Is Brexit a Crisis?

Brexit is defined by the Oxford Dictionary as: "The withdrawal of the United Kingdom from the European Union."[2] The word "withdrawal" here means a relatively long and complex procedure, but we should not forget, that the relations between the UK and the EU has always been a bit "rocky". Just think about e.g. the establishment of the EFTA as a "counter-EU" by the UK along with some other countries (e.g. Denmark and Norway) in 1960; or about their reluctance to submit themselves to the European Monetary Union; not to mention their broad and often used opt-out licenses regarding EU-legislation. It is no exaggeration to say that even after they joined the EU (back then EEC) in 1973, the UK has always had its separate ways and means. [1: 241–242] [2: 111]

The so-called Brexit referendum was held on the 23rd of June 2016 and had a result of 51.9% of voters demanding that the UK shall leave the EU. [3: 1019] It means that the majority—although not the vast majority—of the UK citizens, who cared enough to cast their votes in the referendum, thought that for the British it would be better to be outside of the EU. It seems that the government is committed to execute the will of the people. But would Brexit be a crisis at all?

---

[1]   Lawyer, Ph.D. candidate, National University of Public Service, Department of European Public and Private Law; e-mail: teleki.balint@uni-nke.hu; ORCID ID: https://orcid.org/0000-0003-3420-0900
[2]   See: https://en.oxforddictionaries.com/definition/brexit (Downloaded: 30.04.2018)

To answer the question, we have to give a definition to the word "crisis" (and also to the word "risk" since the two are closely tied). Drennan and McConnell quote the definition accepted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which defines "risk" as: "The combination of the probability of an event and its consequences". [4: 3–4] A manual issued by the House of Lords quotes former PM Tony Blair, who implicitly refers to risk as "a normal part of life" but "a potential damage". [5: 5] Koronváry defines crisis as: "A decision-making situation, in which events deteriorating the lives, physical safety, health, mental condition, or wealth of the individuum, or the member of a given group/organisation and those related to them, and others present take place." [6: 10]

In the next part we will detail how many risks does Brexit poses to those involved and prove that they suit the definitions above. Here we only give a typology of the risks which the author of this article has identified. First and foremost, there is an economic and financial crisis, which is quite apparent knowing that the EU is a primarily economic-focused entity. Then we have a complex political crisis, which also does not need too much further explanation. And the third category is denominated by the author of this article as human crisis, which embraces those social and human impacts of the Brexit, which do not fit into the previous two categories. As it was mentioned before, these will all be detailed below.

Structure and Methodology

The structure of this article is as follows. In the second part the abovementioned three main types of crises will be broken down to the exact crises and these will be detailed in order to help to understand why these are important for this article. In the third part we discuss the proceedings since the referendum, assess them from a crisis management aspect, and try to give predictions and scenarios for the future. Last but not least, in the conclusion, we summarize all knowledge on the issue.

The methodology is a quite simple qualitative approach here, since we have to examine phenomena from the aspect of certain terms (such as crisis and risk), therefore no quantitative analysis is required, except for the economic-financial risks, but fortunately the author of this article can depend on the works of economists with more comprehensive knowledge on the issue. The most important is perhaps the use of crisis management manuals. Some of them have already been introduced in the previous part.

Identifying Brexit-Related Crises

In this part we identify the exact potential crises which can arise or could have arisen from the simple fact of the Brexit. Therefore, here we describe these factors, and try to assess them along the potential risk they can pose.

Economic and Financial Crisis

The European Union is originally—and basically still—an economic integration. For this, the first and quickest effect of the Brexit referendum is a financial one—namely the depreciation of the British Pound. Also, the most durable impacts are those effecting the economy of the EU and the UK in its entirety. Therefore, in this part we focus on two things: the vulnerability of the British Pound (GBP)—and of the financial sector, and the potential economic effects of Brexit on the Common Market and on the British economy.

The Vulnerability of the GBP and the Financial Sector

Only within one single trading day, to the 27th of June 2016 (there was a weekend in-between) the Pound has virtually lost the 10% of its value and fell to £1.315 to the US dollar, reaching its 31-year low since 1985, below the value of the Pound's "Black Wednesday" in 1992 (the day when the Pound was forced out of the European Exchange Rate Mechanism). [7: 206] The severity of the uncertainty was considerably high even in 2017, the relevant authors all used the terms "uncertain" or "uncertainty" in relation to the term economy. [7: 207]

The City of London is geopolitically the heart of the finances of the whole of Europe: 40% of Europe's assets are under management and 60% of Europe's capital markets business are held by UK-based banks. And the City will definitely not relocate itself just because of the Brexit. When we say "geopolitical", we understand such advantages as the clearing infrastructure built up throughout the decades, the technological leadership of the City, etc. This is why the post-Brexit access of the City to the Common Market should be provided. The City of London embodies the archetype of Anglo–American financial capitalism, and still the abovementioned uncertainty and unpredictability makes the financial markets nervous. [8: 1–4] (Here we have to mention, that even the European Banking Authority, the banking supervision agency of the EU was located in London, but it has already been moved to Paris.)

In general, Brexit may force financial economic systems to transform more quickly and with much higher costs than previously anticipated, and reshuffle the spatial landscape of financial production accordingly, also with far-reaching impacts on the debt and equity markets that help financing states and the corporate world alike. [8: 1] However, there is place for optimism, because as an Italian investment banker made it clear after the referendum, there is a viable crisis management strategy for the situation: "We had worked before the referendum on how to prepare portfolios. Our decision to diversify asset classes and currencies proved right, so we did not experience any losses on the day of the vote. Indeed, Brexit has reinforced the idea that diversification works in times of crisis and that it is a better strategy than any others." [9]

General Effects on the Common Market

The "economics of international disintegration" as Sampson says can lead to serious consequences regarding the Common Market. Because the Common Market lowers trade

costs by reducing both border barriers to trade, which are imposed when goods and services cross borders, and behind-the-border barriers, which arise from international differences in regulation and economic policy. [10: 163–167]

First of all, the authors highlight the negative impacts of Brexit on the *international supply chains.* As Neuwahl puts it, the new situation is particularly damaging to supply chains. After Brexit, composite goods that previously circulated freely in the EU may no longer meet rules of origin and be subject to duties and certification procedures. This may lead to redirection of trade flows, reorganization and disinvestment, a situation that the UK Government seems to appreciate and accept, especially if shocks can be avoided. [11: 291–292]

In close relation with those mentioned in the previous paragraph, the problems of *immigration* and *foreign direct investments (FDI)* have to be discussed. Brexit will mean a reduction in both. Which means for instance that without the current model of FDI the UK's car production will reduce by 12%, and with a restricted immigration the GDP of the UK will be reduced by an estimated 0.9–3.4%. [10: 173] Naturally not only the UK, but the other party of the business will be affected in a negative way.

The UK itself has always been a *Euro-outsider.* For this, the Brexit has an implicit effect on the phenomena of voluntary and involuntary Euro-outsiderness. The leave of the strongest voluntary outsider will lead to incalculable consequences. Predictions say that the handling of the differentiated integration will depend on the one hand on the club of Euro-insiders, the institutional system of the Eurozone (e.g. ECB, Eurogroup, ECOFIN, etc.) who have to stay open to the non-members, and on the other hand on the preferences of the certain Member States themselves. [1: 238–246]

The resolution for these questions concerning the Common Market will highly depend on the way the negotiating parties will finally choose (see the scenarios below).

The Political Crisis

Under the category of political crisis, the author of this article understands different types of problems, which are interconnected of course. First of all, the legal regime of the EU has become part of the UK legal regime throughout the decades, and the British legal traditions are quite different from the continental Europe, however the EU legal regime shows some resemblances. Brexit itself is carried out through the initiation of the "Article 50 procedure" which refers to the leave clause in Art. 50 of the Treaty on the European Union (TEU). The final result of the negotiations, the "deal" itself is not only a legal, but also a political question, and the constitutionalist approaches cannot be neglected.

In relation to the aforementioned, *the future unity of the United Kingdom* itself is also at stake. In 2014 there was a referendum in Scotland, which almost lead to the separation of Scotland from the UK, but at the end the "remain" votes won. However, the "remain" votes won also at the Brexit referendum, in Scotland, and in Northern-Ireland. In the latter, the peace itself is very fragile. The question is, what will the future of Scotland and Northern Ireland be? These countries rather wanted to stay in the EU, but have to stay in the UK instead.

And connected to both questions above, we have to deal with another political term, which is *nationalism.* Just as in England and Wales, nationalism has led to the majority

of the "leave" votes, and as the outcome of the Brexit referendum fuels the Eurosceptic–Nationalistic movements and politicians throughout the EU, also the nationalism of the Scottish and the Irish can save—if such a scenario is plausible—almost half of the current UK for the EU. In consequence, this term has both positive and negative connotations here.

Legal Consequences and the Constitutionalist Approach

Art. 50 para. (1) TEU says: "Any Member State may decide to withdraw from the Union in accordance with its own constitutional requirements." As Tridimas points out, Article 50 is politically neutral. [12: 305] At the same time, as Eeckhout and Frantziou put it, this sparsely worded provision raises more questions than it answers, and is of course wholly untested. [13: 696]

What the authors tend to emphasize is the fact, that the withdrawal is legitimate, if it is "in accordance with its own constitutional requirements" of the Member State, as Art. 50 TEU says. In case of the United Kingdom, it is somewhat more complicated, than one would think at first glance. The outcome of the Brexit referendum is an expression of popular sovereignty, but is a consequence of an act of parliamentary sovereignty, the EU Referendum Act 2015. In the UK, both the government and the Parliament can legally choose to ignore a referendum. [3: 1020–1024] It is important because the notification—to the European Council in accordance with Art. 50, para 2 TEU, which is the formal start of the withdrawal procedure—can be revoked by the Member State in the following two years after which—in accordance with Art. 50, para 3 TEU—the Treaties cease to apply to the Member State. [12: 304] This is interesting because in conclusion of all the above said, a possibility of the revocation of the withdrawal is theoretically possible regardless of the outcome of the Brexit referendum. Nevertheless, there does not seem to be any political will by the British Government to do so, although the EU would give a warm welcome to it.

Nevertheless, the option of revocation should be considered because, as Eeckhout and Frantziou phrase it, the current political discourse on withdrawal, particularly in the UK, stands in a stark contrast with the constitutionalist approach to Art. 50, because this discourse completely disregards the fact that Brexit involves a seismic shock to individual rights. [13: 732] Why is that? Because as Douglas-Scott cites the former British judge at CJEU, Sir David Edward: "Withdrawal from the Union would involve the unravelling of a highly complex skein of budgetary, legal, political, financial, commercial and personal relationships, liabilities and obligations." Brexit will result in UK nationals losing their EU citizenship—a legal change whose implications has not yet been fully investigated. [3: 1028] Eeckhout and Frantziou add that extricating the UK from the *acquis communautaire* is a complex, wide-ranging and intrusive legal exercise, which raises questions of respect for constitutional guarantees relating to acquired rights and the rule of law. [13: 699]

How "United" is the Kingdom?

But the whole story would only be as "simple" as set out above, if the United Kingdom itself were not a union constructed by treaties. However, the United Kingdom consists of England,

Wales, Scotland and Northern-Ireland, from whom in Scotland and Northern-Ireland the pro-EU votes were in strong majority.[3]

First of all, Wales, Scotland and Northern-Ireland are so-called *devolved administrations.* Without getting into the details of the relevant legal framework, it is far enough to say that their relations with the Westminster (UK) Government and the EU is rather complicated, since a so-called *multi-level governance,* or *co-governance* is in function, which has altogether four levels (including the municipality level). Besides the division of power between the certain levels of government, it also means that we can speak about allocation of responsibilities between the UK and the EU; between the UK and the devolved administrations; and between the EU and the devolved administrations. [14: 766]

This latter relationship has a critical meaning in the field of *social policy,* since the devolved administrations have their separate EU funding, setting aside the EU Common Agricultural Policy, the most significant support comes through the European Investment and Structural Funds: Scotland and Wales profit from the European Social Fund; Northern-Ireland profits from the Structural Fund and most importantly from the specific Fund for Peace and Reconciliation. [14: 766–771]

The strongest "remain" voter was the Scottish electorate, with 62% of the votes for staying in the EU. [15: 98] Not so long before, in the Scottish Independence Referendum of 18 September 2014, the Scottish nation also voted for staying in the UK with a majority of 55.3%.[4] Considering all this, it is not surprising, that Scottish Prime Minister Nicola Sturgeon called to: "…take all possible steps and explore all options to give effect to how people in Scotland voted." One of this options is a new referendum on the independence, which relying on the public morale of Scotland after Brexit would probably result in the win of the separationists, driving Scotland and the UK Government in a hard political situation. [15: 766–767] The biggest question is whether there is a way for the devolved administrations to further profit from the *acquis communautaire*—especially the legal regime, e.g. the CJEU case law, and the EU funding—if the UK leaves the EU and they do not leave the UK?

In case of Northern-Ireland there are two more questions to be added: what will be the future of the results of the peace process, which was believed practically by everybody to be successfully ended in 1998, and in connection with that, what will happen on the Irish border, which is the only land border of the UK, in technical terms?

The Rise of Nationalism

It can be debated whether the outcome of the Brexit referendum was a pure victory of classic nationalism ("British bread for British toasters") or rather an economically rational decision, but it is clear that the result of it was a rise of the nationalistic political powers, and not only in the UK, but across the European Union.

In Scotland the pro-independence Scottish National Party (SNP) with the lead of Prime Minister Nicola Sturgeon, in the 2016 elections reached 56 seats of the 59 available Scottish

---

3   See e.g.: http://theconversation.com/the-geography-of-brexit-what-the-vote-reveals-about-the-disunited-kingdom-61633 (Downloaded: 01.05.2018)

4   See: www.theguardian.com/politics/ng-interactive/2014/sep/18/-sp-scottish-independence-referendum-results-in-full (Downloaded: 01.04.2018)

seats in Westminster, and 63 seats in Holyrood—the Scottish Parliament—from the 129, where with the also pro-independence Greens (6 seats) they are the governing majority. [16: 358–359] And as the American ethnologist Knight stated, based on his own empirical experiences on field, it was "uncomfortable" to see the "nationalist projects of both Edinburgh and London". But he also recognizes that in a global view, in spite of the "uncanny present" Scotland managed to maintain its cosmopolitan values, and regarding the SNP he says: "many people, me included, feel awkward about a nationalist party becoming the progressive voice of cosmopolitanism, freedom, and social liberty". [17]

The bigger problem according to some authors is the precedent the Brexit referendum has set. Scuira considers not only the resistance towards supranational policies and the rise of Eurosceptic political parties in the Eastern Member States dangerous [2: 115–117] but also fears a potential wave of other exits such as "Frexit" (France), "Nexit" (Netherlands), etc. in Western Europe as well, and has doubts whether the EU itself is enough to stop such tendencies. [2: 121–122] After the re-election of Merkel, the election of Macron, and the weak performance of Geert Wilders in Netherlands, the author of this paper is not so pessimistic.

The Human Crisis

According to specialists of the *health sector,* approximately 10% of doctors working in the United Kingdom are from other EU countries, with even higher figures in sectors such as social care in some parts of the country, such as London. [18] In conclusion, the National Health Service of the UK and the whole British society will be in serious trouble if the health workforce coming from other EU countries, not having UK citizenship, cannot stay after the Brexit.

Of course, other sectors could be pointed out as well, where the proportion of employees coming from the CEE region is still higher (e.g. Hungarians and Polish in the catering sector), but maybe the most shocking is always when human life and health is directly at stake. Nevertheless, the *four basic freedoms of the EU,* and within especially the *free movement of persons*—under which we now understand natural persons, i.e. employees, students, and their close family members—is essential for the proper function of the Common Market, and once the access will not be provided for the UK, that will be disadvantageous for the citizens of both the UK and the EU.

Dealing with the Consequences

Since the notification towards the European Council by the UK Government has already happened—in accordance with the provisions of Art. 50 TEU—and there is little chance that the process would be reversed by a revocation by the UK, we can conclude that the dice is cast, and Brexit is inevitable. Which means that all the risks and potential crises related to it will be a reality soon. In this part, we first review the timeline of Brexit from the EU Referendum Act to the planned end of the process. Then we look at the institutional framework of Brexit and after that the possible scenarios of the results of the negotiations. We try to discuss and assess all the aforementioned from a crisis management aspect.

The Timeline of the Events Since the EU Referendum Act

This is what exactly happened until now, but how the whole process is expected to continue until the very end:[5]

- The EU Referendum Act has received Royal Assent (which in accordance with the UK law is the final step in the legislation) on 17 December 2015, after both chambers of the Parliament accepted it.[6] The Act itself was a consequence of the way how David Cameron won the general elections on 7th May 2015, namely leading a campaign focused on holding a referendum on the further EU membership, in order to keep the pace with the Eurosceptic–Nationalist UK Independence Party (UKIP) of Nigel Farage, who had achieved an unforeseen success in the EP elections on 22nd May 2014 and also in the municipal elections afterwards.
- On 23th June 2016 the referendum sees "leave" campaigners win a narrow victory with 51.9% against and 48.1% for "remain". David Cameron resigns immediately as Prime Minister (because although he campaigned with the referendum itself, he was among those Conservatives who encouraged the people to vote "remain"). On 13th July 2016 the former Minister of Domestic Affairs of Cameron, Theresa May became Prime Minister.
- On 29th March 2017 Theresa May triggers the Art. 50 procedure, which starts the clock on the two-years long negotiation process for the UK on the terms of leaving the EU.
- On 8th June 2017—having surprised many by calling a general election—Theresa May loses her majority in Parliament. Northern Ireland's Democratic Unionist Party (DUP) —led by Arlene Foster—makes a deal with the Conservatives and its votes allow her to stay in power.
- On 26th June 2017 formal negotiations on withdrawal begin between the UK and the EU.
- On 20th November 2017 the EU27 ministers in the European Council voted on the relocation of two very important, previously London-based EU agencies to other Member States. The European Banking Authority is relocated to Paris, and the European Medicines Agency is relocated to Amsterdam.[7]
- On 13th December 2017 rebel Tory MPs side with the opposition, forcing the government to guarantee a vote on the final Brexit deal, when it has been struck with Brussels.
- On 15th December 2017 the EU agrees to move on to the second phase of negotiations after an agreement is reached on the Brexit "divorce bill", the Irish border and EU citizens' rights.
- On 19th March 2018 the UK and EU make decisive steps in negotiations. Agreements include dates for a transitional period after Brexit day, the status of EU citizens in the UK before and after that time and fishing policy. Issues still to be sorted out include the Northern-Ireland border.
- According to the EU's chief negotiator, on 31st October 2018 the negotiations must be complete, to give the 27 EU countries time to sign off the deal. MPs will also get to vote on the final deal in the UK Parliament before 29th March 2019.

---

[5]   See e.g.: www.bbc.com/news/uk-politics-43546199 (Downloaded: 02.05.2018)
[6]   See: www.legislation.gov.uk/ukpga/2015/36/notes/division/1/index.htm (Downloaded: 02.05.2018)
[7]   See: www.consilium.europa.eu/en/policies/relocation-london-agencies-brexit/ (Downloaded: 02.05.2018)

- 29th March 2019 is Brexit Day—according to the current plans, because the two-years long negotiation process can theoretically be extended in accordance with Art. 50, para 3 TEU. On this day the UK ends its membership of the European Union at 2300 GMT and enters a transition period.
- On 31st December 2020 the transition period is due to end and the new economic and political relationship between the UK and the EU to begin.

The timeline above clearly shows that the leading British politicians had and have a tendency to drive themselves and the UK into potential risks and crisis situations. However, if the negotiations are conducted properly, the outcome can be of minimalized losses.

The Implementation of Crisis Management on the Process

As Koronváry writes, the life cycle of a crisis normally consists of five stages, [6: 13–14] which are:
- *latent stage*—when the crisis is still not experienced and/or identified;
- *assessed/identified crisis*—the stage of prevention, deflection and preparation;
- *conflict/crisis incident*—the crisis is triggered by certain factors;
- *crisis management*—de-escalation of the crisis and minimization of the losses;
- *reconstruction and after-care*—care for the negative consequences and prevention of the escalation of further crises.

The *crisis management* itself consists of the stages of prevention, preparation, reaction and reconstruction. [6: 19–20] It is very important, that for a successful crisis management a *crisis manager* and a *crisis team* is needed. [6: 23–24]

In case of Brexit, the institutional background seems to be given. Both sides have an institution which can be identified as a crisis team. On the side of the UK, there is the *Department for Exiting the European Union*[8] currently led by Permanent Secretary Oliver Robbins, who can be called the crisis manager here.[9] And on the side of the EU there is the *Taskforce on Article 50 negotiations with the United Kingdom*, which is virtually a part of the Commission—the Commission is the negotiator organization—and is led by chief negotiator Michael Barnier.[10]

What is the real question here, is whether all the potential crises discussed in the second part of this paper —and the author is sure that there can be further ones, either because they are still latent, or simply because they were skimmed over by the author—are properly identified by the institutional frameworks of crisis management of the parties. Hopefully everything relevant will be taken into consideration and addressed properly.

---

[8]   See: www.gov.uk/government/organisations/department-for-exiting-the-european-union (Downloaded: 03.05.2018)
[9]   See: www.gov.uk/government/publications/biographies-of-the-civil-service-representatives-for-the-negotiations-with-the-eu (Downloaded: 03.05.2018)
[10]   See: https://ec.europa.eu/info/departments/taskforce-article-50-negotiations-united-kingdom_en (Downloaded: 03.05.2018)

Possible Future Scenarios

When we talk about possible future scenarios, we have to differentiate between two separate things: the Brexit deal itself, which means on what terms the UK leaves the EU; and another deal which settles the question of the further relations between the UK and the EU.

Possible Scenarios of the Brexit Deal

There are virtually two alternatives, which are dubbed in the civil discourse as "hard Brexit" and "soft Brexit". There is no strict definition of either, and they sometimes mean different things to different people, but they generally refer to the closeness of the post-Brexit relationship of the UK with the EU.

The "hard Brexit" could involve quitting without a deal in place. This would mean no compromise on issues like the free movement of people, leaving the EU Common Market and trading with the EU as if it were any other country outside Europe, based on World Trade Organization (WTO) rules. This would probably also mean that the UK and the EU would probably apply tariffs and other trade restrictions on each other.

The other option would be the "soft Brexit", which could involve keeping close ties with the EU, possibly through some form of membership of the European Union Common Market, in return for a degree of free movement.[11]

Possible Scenarios for Further Relations

A document was issued by the UK Government in 2016 under the title *Alternatives to the Membership: Possible Models for the United Kingdom Outside the European Union.* In this, three scenarios are sketched, based on the relationships of other third countries with the European Union. [19] These are briefly summarized in the document as follows:

- "The Norway model"—Norway is in the European Economic Area (EEA) 11 but not in the EU. This is the model outside of the EU which is most integrated with the Common Market. It means that Norway has considerable access to the EU market. It also takes part in some important non-economic cooperation negotiated separately, like counter-terrorism. The Norway model includes many of the key obligations of EU membership, and Norway makes contributions to EU spending. Norway is required to follow most of the rules of the Common Market, though without a vote or vetoes in how those rules are made. It has to accept the free movement of people and it has chosen to be part of the Schengen Area. Norway has a higher share of EU migrants per capita than the UK.
- "A negotiated bilateral agreement"—There are different ways this can be done. Such arrangements typically offer limited access to the Common Market, offering some combination of tariff-free trade, open access to the services market and guarantees that companies operating in these markets are treated in a fair and non-discriminatory way. But they rarely go far in establishing a Customs Union or addressing non-tariff barriers.

---

11   See: www.bbc.com/news/uk-politics-37507129 (Downloaded: 03.05.2018)

Switzerland's arrangements with the EU go furthest in replicating the benefits of EU membership, but bring an increased proportion of the obligations, including accepting the free movement of people, making a significant contribution to EU spending, and compliance with the majority of rules governing the Common Market. (For this, the CETA, the EU–Canada Comprehensive Economic and Trade Agreement could be a model. Neuwahl mentions the possibility of a so-called *CC–CETA, a Comprehensive Cross-Channel Economic Free Trade Agreement.*[12])

- "WTO membership"—The UK, like all other EU countries, is a member of the WTO. If the UK had not agreed a new relationship with the EU by the time we left, then we would have reverted to our common membership of the WTO as the basis for trade—just like Brazil does in its trade with the EU. Under WTO rules, this would not include any preferential access to the Common Market, or to any of the 53 markets with which the EU has negotiated Free Trade Agreements. It would also affect the price of imported goods paid by UK consumers, if reciprocal tariffs were imposed on imports from EU countries. It would involve no coordination or obligations in non-economic areas like fighting crime or terrorism. [19: 15]

Conclusion

This paper tried to focus on the potential risks and crises arising as a consequence of the Brexit and attempted to categorize these, rather than going into the exact details of the related crisis management process. The latter would have been pointless for two reasons, primarily because right now the parties are in the middle of the negotiations i.e. the crisis management process, and it will make much more sense to assess the whole retrospectively when it will be complete, and secondarily because both parties—hopefully—are in possession of the necessary resources (i.e. infrastructure, human resources, knowledge, common sense, etc.).

The categorization (of potential risks and crises) we give in the second part is of course arbitrary, but the author of this paper is convinced that it is a reasonable way to categorize these. As it was mentioned before, it cannot be excluded, that there are some potential crises related to Brexit which are still latent and are therefore not included here.

To sum it up, naturally it is enough to look at all these potential risks and crises and the resources necessary to tackle them to conclude how unfortunate is the whole Brexit phenomenon. But *alea iacta est,* and there is a good chance that the parties will find the solution to make the most of it.

References

[1]   ADLER-NISSEN, R.: *The Vocal Euro-outsider:* The UK in a Two-speed Europe. *The Political Quarterly,* 87 2 (2016), 238–246. https://doi.org/10.1111/1467-923x.12265

[2]   SCUIRA, L.: Brexit Beyond Borders: Beginning of the EU Collapse and Return to Nationalism. *Journal of International Trade Affairs,* 70 2 (2017), 109–123.

---

[12]   For details see source [11].

[3]   DOUGLAS-SCOTT, S.: Brexit, Article 50 and the Contested British Constitution. *The Modern Law Review,* 79 6 (2016), 1019–1040. https://doi.org/10.1111/1468-2230.12228

[4]   DRENNAN, L. T., McCONNELL, A.: *Risk and Crisis Management in the Public Sector.* London: Routledge, 2007.

[5]   *Government Policy on the Management of Risk.* London: House of Lords Select Committee on Economic Affairs, 2006.

[6]   KORONVÁRY P.: *A krízismenedzsment alapjai.* [The Basics of Crisis Management.] Budapest, ZMNE, 2009.

[7]   PLAKANDARAS, V., GUPTA, R., WOHAR, M. E.: The depreciation of the pound post-Brexit: Could it have been predicted? *Finance Research Letters,* 21 (2017), 206–213. https://doi.org/10.1016/j.frl.2016.12.003

[8]   DÖRRY, S.: The geo-politics of Brexit, the euro and the City of London. *Geoforum,* 85 1–4 (2017). https://doi.org/10.1016/j.geoforum.2017.07.003

[9]   ROMEO, V.: Paolo Galvani: 'Brexit shows diversification works in a crisis'. *Money Marketing,* 14 July 2016.

[10] SAMPSON, T.: Brexit: The Economics of International Disintegration. *Journal of Economic Perspectives,* 31 4 (2017), 163–184. https://doi.org/10.1257/jep.31.4.163

[11] NEUWAHL, N.: CETA as a Potential Model for (Post-Brexit) UK–EU Relations. *European Foreign Affairs Review,* 22 3 (2017), 279–302.

[12] TRIDIMAS, T.: BREXIT means BREXIT – Article 50: And Endgame without an End? *King's Law Journal,* 27 3 (2016), 297–313. https://doi.org/10.1080/09615768.2016.1254418

[13] EECKHOUT, P., FRANTZIOU, E.: Brexit and the Article 50 TEU: A Constitutionalist Reading. *Common Market Law Review,* 54 (2017), 695–734. https://doi.org/10.2139/ssrn.2889254

[14] BIRRELL, D., GRAY, A. M.: Devolution: The Social, Political and Policy Implications of Brexit for Scotland, Wales and Northern-Ireland. *Journal of Social Policy,* 46 4 (Brexit Special Issue) (2017), 765–782. https://doi.org/10.1017/S0047279417000393

[15] FLETCHER, M., ZAHN, R.: What Options Are Available to Scotland to Remain within the EU Given the 'Brexit' Referendum Result? *The Edinburgh Law Review,* 21 (2017), 98–103. https://doi.org/10.3366/elr.2017.0392

[16] McCORKINDALE, C.: Scotland and the Brexit: The State of the Union and the Union State. *King's Law Journal,* 27 3 (2016), 354–365. https://doi.org/10.1080/09615768.2016.1254405

[17] KNIGHT, D. M.: Anxiety and cosmopolitan futures: Brexit and Scotland. *American Ethnologist,* 44 2 (2017), 237–242. https://doi.org/10.1111/amet.12474

[18] PARK, J. J., ATUN, R.: Brexit: Severe Risks to Britain's National Health Service. *American Journal of Public Health,* 107 10 (2017), 1594–1596. https://doi.org/10.2105/AJPH.2017.304010

[19] *Alternatives to Membership: Possible Models for the United Kingdom Outside the European Union.* HM Government, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504604/Alternatives_to_membership_-_possible_models_for_the_UK_outside_the_EU.pdf (Downloaded: 03.05.2018)

Specific Apparatus of Vatican Diplomacy – Charity Organisations[1]

Lóránd UJHÁZI[2]

Throughout of its existence, the Catholic Church has always tried to protect the most vulnerable members of society. This is proven by the fact that even the earliest Church documents show how the new church tried to alleviate some acute social problems. The religious and secular legal regulations which govern the operations of Catholic charity organisations and the whole institutional structure of these bodies were created by a long historical process which led to the birth of the current web of multiple different Catholic charities. Furthermore, these institutions are not merely NGOs or humanitarian relief agencies. Instead their activities are based upon the activities of the Founder, Jesus of Nazareth, and upon the spirit of the Gospels. Catholic charitable actions are mainly motivated by theological concepts and the social teaching of the Church even if these activities are executed by formal institutions.

The current Pope expects a more active participation of national and international Catholic charities in multiple areas like looking after the poor and the refugees and in the struggle for universal peace.

International cooperation, partly because of the universal nature of the Church, is not an unknown concept for the Catholic Church. Therefore, its charities are willing to work with every national and international institution, including secular governments, which work to make life on Earth more bearable for mankind. Since many contemporary humanitarian catastrophes take place in war zones, Catholic charities must find acceptable ways of cooperation with the various armed forces operating in these territories. This paper demonstrates the legal framework governing the work of Caritas Internationalis, which is the official charity service of the Holy See and which also acts as an umbrella organization for the more than 160 national Catholic Caritas bodies. In this article I will only mention these national Caritas institutions and any other international NGOs if this is necessary for the better understanding of either the international nature or the international activities of Caritas Internationalis.

Keywords: *Catholic Caritas, Catholic Church, Canon Law, Civil–Military Cooperation*

---

[2] Ph.D., Senior Research Fellow, National University of Public Service, Faculty of Military Science and Officer Training; e-mail: ujhazi.lorand@uni-nke.hu; ORCID: 0000-0002-1630-8208

The Catholic Church has always been committed to people in need. Ancient ecclesiastical documents report that the church takes part in solving social problems. The structure, the canonical regulation and the secular legal classification of Catholic charity organizations, which still operate within multi-coloured bounds, has developed gradually. In our days the structure of Caritas is vast and complex. There are seven regional umbrella organisations (Caritas Africa with 46, Caritas Asia with 24, Caritas Europe with 49, Caritas Latin America with 22, Caritas North America with 3, MONA with 15 and Caritas Oceania with 7 member organizations). The national Caritas Organisations are divided into diocesan Caritas and these are further divided into Caritas of parishes. Moreover Caritas has well elaborated "management standards" (Laws and Ethical Codes; Governance and Organisation; Finance and Accountability, Stakeholder Involvement, all of which have eight articles). However, Catholic charity organizations are not merely NGOs or humanitarian charity organisations. Uniquely, their motivations derive from the activities of Jesus of Nazareth and the spirit of the Gospels. Philanthropic fondness is based upon theological principles and the social doctrine of the church, even if the organisations work within legally regulated institutional limits. The present Pope seems to count to a greater extent on the involvement of national and international Catholic organisations in caring for the poor, handling migration crisis and reinforcing peace.

International cooperation, due to the universal character of the church, is not far from the nature of the church. In humanitarian activities, Catholic charity organisations cooperate with any national or international organisation—mainly states—which struggle for the earthly welfare of humanity. Considering that the alleviation of present humanitarian disasters happens on areas with ongoing armed conflict, it is very important for Catholic organisations to cooperate with armed forces, especially with the army. In this study I am going to introduce the legal status and the regulation of the official charity organisation of the Holy See, *Caritas Internationalis*, which operates as the overarching body of more than 160 Catholic charity organisations. I am going to refer to other charity organisations as much as it serves the better understanding of the legal regulation of charity organisations. Similarly, I am going to refer to the national charity organisations below the overarching body as much as it serves the better understanding of the international character and activity of the organisation.

The Catholic Church has always lead the support of the poor. [1] [45] In the *Acts of the Apostles* we can read that the apostles gave away the money they got from selling properties to the poor. [Acts 2: 42–47] While the institutional frameworks of the church were developing, care for the poor became institutional as well, and the canonical regulation and the secular legal classification of Catholic charity organisations were taking shape. [2] Catholic charity organisations are not merely non-governmental organisations (NGOs) or humanitarian charity organisations. Uniquely, their motivations derive from the activities of the founder, Jesus of Nazareth and the spirit of the Gospels. [3] Philanthropic fondness is based upon theological principles and the social teaching of the church, even if the organisations work within legally regulated institutional limits. Moreover, Pope Francis has drawn attention to this fact several times. [4] The present church leadership [5] counts on the involvement of national and international catholic charity organisations in caring for the poor, handling migration crisis and reinforcing peace. [6]

International Caritas – Caritas Internationalis

As an impact of the economic and social changes of the 19th century, the social teaching of the church played a more and more significant role in the lives of religious communities. [7] Lorentz Werthmann formed the first Caritas organisation, Caritasverband für das Katholische Deutschland, which was approved by the German Episcopal Conference as a national organisation in 1916. In 1921 the organisation got its name: Deutscher Caritasverband. Werthmann created the emblem of the Caritas, the flaming cross, which has been used since then by national and regional Caritas organisations and by Caritas Internationalis, too. German organisations served as examples for other national Caritas organisations at the beginning of the 20th century. In Hungary the initiative started in 1914 as Katholikus Karitász (Catholic Caritas). However, this initiative remained an aid programme during WWI; it did not develop into an organisation. In 1931, after several initiatives, the organisation and the network of Katolikus Karitász (Catholic Caritas) was set up, when Cardinal Jusztinián Serédi appointed Zsigmond Mihalovics pastor of Herminamező, to be the Archiepiscopal Commissioner of the Caritas. In 1931, the Hungarian Catholic Episcopal Conference established Szent Erzsébet Karitász Központ (Saint Elizabeth Caritas Centre), whose Director was Zsigmond Mihalovics, to coordinate the national network. [8] To coordinate Catholic charity organisations and to promote the foundation of Caritas organisations, the first Caritas conference was convened in 1924 within the framework of the Eucharistic World Conference in Amsterdam. In 1924, the leaders of nine European countries (including Hungary) decided to establish an international Caritas organisation, which came to existence as Caritas Catholica in 1928. Pius XII aimed to form a more coordinated connection among international Caritas organisations, and the organisation became the official charity organisation of the Holy See in 1947. [9] Due to its peculiar connection to the Holy See, the centre of the organisation was transferred from Switzerland to Rome. Moreover, in 1954, to put emphasis on its international character, it got the name International Catholic Caritas. [10]

The international character of the charity organisation is significant because of the possibility to concentrate powers and to control the Catholic identity of the organisation. This way, when national sources have been used up, it is possible to concentrate more power to ease humanitarian disasters. In Lebanon, for example, to ease the migration crisis, International Catholic Caritas brought national Caritas organisations in managing the crisis. [11] The same happened during the civil war in Rwanda, or during natural disasters (the storm in Myanmar, [12] the earthquake in Haiti, [13] the flood in Poland and in the Czech Republic, the tsunami in Sri Lanka and the flood in the Balkan region). [14] Each national Caritas organisation joins in to handle the crisis in accordance with its strength. [15] The international character of the Caritas appears in its cross border aims. Good examples are their attempt to ease natural and civilizational disasters, to promote economic equity, to reduce the effects of climate change, furthermore to eliminate poverty which evolved due to climate change. Similarly, they pay attention to helping HIV/AIDS infected people and struggle against other viral and infectious diseases. Moreover, defending the rights of the ill, the poor, the socially excluded, women and immigrants gets a significant role. They participate in the global struggle against violent migration, deportation and human

trafficking. [16] Emphasis can change in accordance with international security challenges and humanitarian disasters. [17]

The legal regulation of International Catholic Caritas took a non-standard path. In 1951, the Holy See approved the first rules and regulations of the organisation, which was voted during the first full general assembly. However, Vatican—on Paul VI' initiative—endowed it with juridical personality on 19th July 1976. It was one of the rare cases when a Catholic organisation—according to the state law of Vatican State—held a juridical personality, but according to the canon law, which regulates the internal church order, it was not a juridical person. It is also true that the legal status and the rank in the national Catholic Church of each national Caritas was totally different. In some countries—e.g. France—the Catholic Caritas did not hold a canonically approved personality, but they had secular legal registration or legal status. Even though *Deutscher Caritasverband* was a legal entity and association according to the German civil law, in the canon law it was an association of the Christian faithful. [18] In many cases, the founders themselves thought that in an anti-religious environment, canon law status would adversely affect obtaining secular legal recognition or effective operation. [19] This model guarantees a wider independence from ecclesiastical hierarchy and a wider margin in secular forums, but it involves risking an organisation losing its Catholic identity, and dissolving among governmental and civil organisations with similar profiles. Difficulties arose from this in Germany.

In other countries, the national Caritas or in some cases the diocese Caritas holds a canonical status, as well. This can take several forms, as the activities of the Caritas are diverse, too. The fields of activity such as education, health care, social care, etc. all have different legal background from the side of both canonical and civil law. Competent ecclesiastical authorities often used to endow Caritas organisations—at the request of the organisation—with canonically approved juridical, mainly private juridical personality. The Catholic Caritas can be the part of either the conference of bishops or the diocesan office structure, which is established or approved by a competent church authority, which acts as an official legal entity. Canon law status is independent from secular legal approval. [20] For example in Hungary, national Catholic Caritas or diocesan Catholic Caritas are all juridical persons from the point of view of canon law, thus these organisations hold juridical personality in civil law, as well. The financial background of national Caritas organisations is diverse as well, which means that they take part in supporting Caritas Internationalis to a different extent. [21]

As the secular and the canon law status of national and diocesan Catholic Caritas organisations is significantly diverse, it is understandable that not only did the legal status of the overarching body develop slowly, but for a long time the overarching body was handled as a loose association of the national organisations. A major step occurred, when in 2004 John Paul II issued his letter *Durante l'Ultima Cena*, which—on the one hand—made Caritas Internationalis a public juridical person, on the other hand the letter assigned the structure of the Holy See. The Pope officially approved the rules and regulations of the Caritas. [22] According to the Papal direction, the rules and regulations, as well as the head office can be modified only with the Pope's permission.

According to Article (Art.) 146, Paragraph (Para.) 2 of the 2004 effective Apostolic Constitution, *Pastor Bonus* the Pontifical Council, *Cor Unum* was responsible for Catholic charity organisations. [23] So in accordance with the general rule, this Pontifical Council

became the general supervisory and monitoring authority of the International Catholic Caritas. [24] The council was responsible for—among others—the international activities of the Caritas, for local initiatives and for caring for the members' Catholic disposition. Caritas Internationalis was ordered to hand the statements, intended to be issued publicly, over to the Pontifical Council for preliminary approval. Due to the international character of Caritas Internationalis, the relationship with Holy See offices, concerned with humanitarian activities, had to be established. According to the former terms, it involved the Pontifical Council for Justice and Peace, the Council for Pastoral Assistance to Migrants and Itinerant Peoples [25] and the Council for Pastoral Assistance to Health Care Workers. As for the area of cooperation, the Apostolic Constitution, Pastor Bonus, which generally specified the responsibilities of each Holy See office, was relevant. The 2004 document includes further restrictions, as it says that regarding the persons of the president and the secretary, preliminary papal approval is needed, and the General Assembly can appoint officials out of the approved persons. [26]

It is the strength of the 2004 document that it clarifies the canonical status of Caritas Internationalis, its relation to the Pope of Rome and its relationship to the dicasteries of the Holy See. At the same time, the document, which is applicable together with rules and regulations, is a short, straightforward line of papal statements. Furthermore, according to certain opinions, the organisation is an important stage of the centralization plans of the Holy See, which hardly can be compatible with its character. Indeed, according to these opinions, Caritas Internationalis is not the central office of the Holy See, but a loose association of Caritas organisations under the national conferences of bishops. [27] As there was still no consent about its legal status, control and contacts outside the church, [28] Caritas Internationalis was regulated by the Holy See again in 2012.

However, Pope Francis integrated the Pontifical Council *Cor Unum,* endowed with wide-ranging powers, into the new Holy See office, the Dicastery for Promoting Integral Human Development with his *motu proprio, Humanam progressionem,* [29] declared on 31st August 2016. Motu proprio, Humanam progressionem, which established the new dicastery, is a short document, and it does not discuss the question of *Caritas Internationalis.* The statute which thoroughly regulates the activities of the dicastery clearly notes [Art. 4, Para. 9] the competency of the new dicastery in controlling Caritas Internationalis. In accordance with this regulation, where the former legal regulations mention the Pontifical Council *Cor Unum,* now the new dicastery should be meant.

New Holy See Regulations

In 2011 Pope Benedict XVI authorised the Secretariat of State—Secretary of State, Cardinal Tarcisio Bertone—to act in the name of the Pope with full authority over the questions in connection with the legal character of Caritas Internationalis and its activities in the church. [30] In Pope Benedict XVI's theological work, the active fondness of the church towards the poor was strongly emphasised. [31] It makes sense that the Pope attempted to give the official charity organisation of the Holy See a clearer legal status. [32]

The general decree, which is basically an act [Can. 29], in spite of the fact that it was issued by the Secretariat of State with executive power only, was issued on 2nd May 2012. [33] The Secretariat of State owned the authorisation of the supreme legislative power

[Can. 30] to arrange the legal framework of the activities of Caritas Internationalis with a general decree. [34] In contrast with the 2004 papal provision, the new general decision gives a more accurate and detailed regulation. However, it is striking that the decision is fairly strict with regard to the Holy See control system over Caritas Internationalis. It is probable that the supreme legislator envisaged that the new legislation would move towards strengthening, and so the thankless task was handed over, and the legislative power was delegated to the Secretariat of State, which owned only executive power. From the legislation and the explanation added to the Pontifical Council *Cor Unum,* it can be concluded that the circumstances were not organized in all respects at Caritas Internationalis.

The general decree does not abrogate Pope John Paul II's document *Durante l'Ultima Cena.* The ordinance, the general decree, the rules and regulations of the Caritas, the Code of Canon Law (especially its legislation about juridical persons [Can. 312–316; Can. 317, Can. 318–320] and the state legislation of the State of Vatican together constitute the legislation governing the activities of Caritas Internationalis.

As far as the structure of the decision is concerned, the major part focuses on the controlling mechanism of the Holy See, and the minor part on the canonical and civil law operational framework of Caritas Internationalis. It reinforces the general supervisory rights of the Pontifical Council *Cor Unum* over Caritas Internationalis. [Art. 1, Para. 1] It reinforces and extends the representation rights of the Pontifical Council *Cor Unum.* Namely, the council through its representative or commissioner with consultative rights participates the sessions of the managing body of Caritas Internationalis. [Art. 1, Para. 3] After the consultation—mainly with the Director of the Caritas—the council appoints an ecclesiastical assistant, a liaison for a set period defined in the rules and regulations. The liaison, due to this right, takes part in the meetings of the managing body, and takes care of the relationship between the Caritas and the Holy See. He discusses theological questions, and supports the Catholic identity of the organisation. [Art. 1, Para. 4] Probably, his role extends to informing the competent offices of the Holy See. So he can be regarded as an officer charged with intelligence service and internal affairs.

The general decision leaves the Caritas a fairly limited scope for action in building external relations. The cooperation with NGOs and other organisations had to be approved by the Pontifical Council *Cor Unum* in advance. [Art. 1, Para. 5] Nor does the Caritas negotiate with international, regional, political, diplomatic, state administrative and jurisdictional organisations, but the second section of the Secretariat of State does. It is especially true for Italian state organisations. [Art. 3, Para. 1] The only exception is humanitarian emergency situations, when *Caritas Internationalis* in its own right can conclude agreements with governmental and international organisations. In this *Caritas Internationalis* is obliged to inform the Pontifical Council *Cor Unum* and the second section of the Secretariat of State as quickly as possible. [Art. 3, Para. 2] Before the general decision was issued, the Caritas had owned principles for internal use that referred to the cooperation with other organisations (2003), especially with the army (2006). The internal "ethical" regulations and the failure of the practice could be the reason that the new legal regulation introduced some reinforcement. The network of Caritas Internationalis does not seem to have been transparent for the Holy See. Probably, it might have been the same on regional levels as *motu proprio, Intima Ecclesiae natura,* which details the relationship between regional Catholic charity organisations and diocesan bishops, forms similar principles emphasising the controlling role

of the diocesan bishops. Accordingly, local Catholic charity organisations cannot cooperate with organisations that are hostile towards Catholic teaching. [35]

The possessions of Caritas Internationalis, as a public jurdical person, are counted as ecclesiastical possessions. [Can. 1257, Art. 1] [36] During property management, the general decree for ecclesiastical goods must be kept. [Art. 6, Para. 7] Furthermore, the Pontifical Council looks after the accurate and transparent property management of the Caritas, [Art. 1, Para. 6] and it approves the contracts, the budget, the property management and the budget of employees and charity programmes after consulting with the Secretariat of State and the Prefecture for the Economic Affairs. [Art. 1, Para. 7] The property management jurisdiction of the Pontifical Council extends to the regional organisations of Caritas Internationalis and to its functional sub-organisations which are legal entities. The Pontifical Council, if it considers to be necessary, can appoint a delegate to supervise the regional organisations of the Caritas. [Art. 1, Para. 8] The general decision empowers the Pontifical Council to summon the leaders of the dicasteries concerned in order to discuss the actual affairs of Caritas Internationalis. [Art. 1, Para. 9]

The Holy See wanted to control the Caritas more vigorously regarding doctrinal questions, as well. *Caritas Internationalis,* respecting the executing power of the Congregation for Doctrine of the Faith regarding faith and ethic, is obliged to hand the documents—intended to be issued publicly—regarding faith and ethic over to the Pontifical Council for preliminary approval. [Art. 1, Para. 2] Doubts seem to have arisen in connection with the Catholic identity of the organisation, too. It is clearer from the explanatory documents of the Pontifical Council *Cor Unum.* (See below)

The general decision names the rights of the first and second section of the Secretariat of State. The first section:
- finalizes the rules and regulations, approved by the Pontifical Council *Cor Unum* of the Caritas;
- can change and explain, being aware of the opinion of the Pontifical Council, the rules and regulations, and the general decision in the light of the Code of Canon Law and the state jurisdiction of the Vatican; [Art. 2, Para. 1]
- guarantees employees' rights and fair social benefits; [Can. 231; 281, Art. 2, Para. 3]
- coordinates the competences among the Pontifical Council *Cor Unum,* other dicasteries, the Vatican Governorate and other Holy See dicasteries; [Art. 2, Para. 4]
- supports the Pontifical Council in controlling the property management of the Caritas Internationalis, especially in managing challenge inspections. [Art. 2, Para. 5]

The second section of the Secretariat of State:
- besides controlling the international activities of the Caritas, [Art. 2, Para. 1] represents the organisation before national and international courts; [Art. 2, Para. 1, 2]
- after the consultation with the Pontifical Council *Cor Unum,* only the second section can authorize those agreements according to which the Caritas receives support from governments, international and other organisations.

The Caritas is obliged to give reports generally towards the first section of the Secretariat of State and towards those Holy See offices that are involved in a certain issue. However, in each case a copy of the report must be sent to the Pontifical Council *Cor Unum.* [Art. 7, Para. 1]

The Caritas is obliged to give a report every four month towards both the second section and the Pontifical Council about those formal and personal contacts that the Caritas maintains with governments and diplomatic bodies accredited by the Holy See. [Art. 2, Para. 3] It seems, in a changed security environment, that the Holy See wants to persuade more strongly its humanitarian charity organisations to pursue intelligence service. However, it is not clear how the strong control on its room for manoeuvre or its intelligence tasks affect the international legitimacy of the Caritas.

The supervisory right of the Holy See extends to executives of Caritas Internationalis [Art. 6, Para. 2] The Director, the Secretary-General and the Trustee are elected according to a strict rule. The Pontifical Council *Cor Unum,* in an agreement with the first section of the Secretariat of State, hands the list of nominees over to the Pope for approval, and the names can be published only after his approval. The election of executives is held in accordance with the Code of Canon Law. [Can. 169–173] The three members of the governing board are appointed by the Pope in accordance with the proposal of the Pontifical Council *Cor Unum* and the Secretariat of State. [Art. 6, Para. 4] The Council, the Secretariat of State and the Prefecture of Economic Affairs having been heard, the experts—to the area of law, establishment and technique—of the consultative body of Caritas Internationalis are appointed by the Pope. After consultations with the Council, the tasks of the Council are determined by the first section of the Secretariat of State. [Art. 6, Para. 5] According to the general decision, the President, the Secretary-General and the Trustee take an oath, following a specific form, on accomplishing the tasks faithfully before the President of the Pontifical Council. The members of the governing board take the same oath in the presence of the Director, or his representative of the Caritas and the employees take the oath in the presence of the Secretary-General.

The Secretary-General represents *Caritas Internationalis* in legal issues. [Art. 6, Para. 9]

The general decision has greatly restricted the scope of activities of Caritas Internationalis. Probably, this strict Holy See behaviour was not unjustified from the point of view of the Holy See. The legislator may have intended to emphasize the hierarchical side of the church in the operation of Caritas Internationalis, and wanted the organisation to adopt Catholic spirituality more powerfully. This point of view appeared later on the national and diocesan level of the Caritas. In his motu proprio, Intima Ecclesiae natura (issued on 11th November 2011) Pope Benedict XVI explicitly discusses the diocesan bishop's legal obligations. [37] Similarly to the supervisory structure of Caritas Internationalis, the Pope expects local bishops and ecclesiastical authorities to supervise Caritas organisations more thoroughly. Presumably, there were problems on both national and international levels, which were answered with legal restrictions by the Holy See.

Other Holy See Documents Regarding Caritas Internationalis

It is not irrelevant for the Holy See whether *Caritas Internationalis,* as a public juridical person, the official charity organisation of the Catholic Church, meets the expectations of the Holy See, and whether its activities and statements are in line with the statements of the magisterium. Therefore, in different documents the Pontifical Council *Cor Unum* summarized the theological points which played roles in establishing new regulations and

a stricter supervisory structure for Caritas Internationalis. [38] The Pontifical Council *Cor Unum* participated in preparing the documents on the basis of its supervisory right, other Holy See dicasteries on the basis of different involvement. Due to the international character of the Caritas, the remarks of the Secretariat of State were considered, as well. After a short summary, the new document states that the Holy See always played an important role in the life of Caritas Internationalis, from the creation of the international organisation to the 2004 papal document. The latest made it certain that the rules and regulations of the Caritas had to be adjusted to the principles outlined in the document and to the place of the Caritas gained in the structure of the Holy See.

The Pope made it clear in an earlier statement which he sent to the general assembly of the organisation on 7th May 2011.

For the operation of Caritas Internationalis, the regulation accepted on 3rd May 2012 was determining. [39] The first paragraph refers to principles, the second to the name and legal status of the organisation, the third to the headquarters of the organisation. The introductory paragraphs are entirely the same as the propositions summarized in the general resolution of the Secretariat of State. The summary of the conditions according to which national and diocesan organisations can be the members of Caritas Internationalis can only be found in the rules and regulations. In this respect, the legal activity of the local ecclesiastical authority (Apostolic Conference or a diocesan bishop), with which it approves the regulations of a local organisation, is determinant. This condition is enough for the national or diocesan organisation to ask for gaining admission to Caritas Internationalis. [Art. 4, Para 4.3] If a competent ecclesiastical authority withdraws the rules and regulations of a national or diocesan caritas—so the possibility of its operation is suspended—it means losing its membership automatically. [Art. 4, Para. 4.3] The rules and regulation of Caritas Internationalis show some similarities with the discussed general decision, as it puts great emphasis on the supervisory role of the ecclesiastical authority. [40] The rules and regulations discuss the rights [Art. 5] and duties [Art. 6] of the member organisations in details. They are fairly general rights and duties, concerning that either national or diocesan Caritas organisations are independent organisations. Furthermore, the rules and regulations introduce the internal structure of Caritas Internationalis, [Art. 7] the regions, [Art. 8] the rights and duties of the general assembly, [Art. 9] of the board of representatives, [Art. 10] of the board of directors, [Art. 11] of the president (or director), [Art. 12] of the vice president, [Art. 13] of the secretary-general, [Art. 14] of the secretariat. [Art. 15] This part is very important as the rights and duties are discussed only here in connection with the Caritas. The rules and regulation discuss the legal representation [Art. 16] and the order of the papal approval regarding offices. [Art. 17] The latest clarifies the basic principle of the general decision, as it determines the order and periods of recommendation to the Pontifical Council. Furthermore, the rules and regulations clarify the general directions for the "ecclesiastical liaison" of the Secretariat of State, [Art. 18] and the general directions referring to the appointment, [Art. 19] to the election, the term in office and the activities of the trustee. Moreover, it clarifies the exact tasks of the consultative body of the Caritas, [Art. 21] to which we can find only a short reference in the general decision. The rules and regulations thoroughly discuss the questions referring to handling possessions, [Art. 22] to incomes [Art. 23] and to modifying the rules and regulations. [Art. 24]

The operational rules of Caritas Internationalis are more thoroughly given in the 28 paragraphs of the internal regulations attached to the rules and regulations. Moreover, the Caritas has a general code of ethic. [41] The following documents of basic principles were issued: The Caritas Partnership Guiding Principles (2003); Caritas Internationalis Child Protection Policy Framework (2004); Caritas Internationalis Guidelines on Relations with the Military (2006); Caritas Internationalis Guidelines on Environmental Justice (2006); Caritas Internationalis Management Standards (2013). In addition, Caritas Internationalis regards itself as bound by international regulations related to its operation.

In 2014, Pope Francis approved the managing directives of Caritas Internationalis. The document reflects the Pope's commitment towards the poor. Further stressed elements are responsibility for its actions, management and transparency:

- management and regulation;
- organisational infrastructure;
- financial sustainability and accountability;
- correspondence to the code of ethic and behaviour according to the methods and measures of the general assembly. [42]

Literally, the document points out the ecclesiastical and secular regulations which must be respected during its operation. The document gives directions about:

- mutual aid among national caritas organisations, which is considered to be obvious and it determines the possible ways of giving assistance;
- the minimum requirements;
- the principles of organization and development.

An appendix of four paragraphs was attached which includes:

- laws and codes of ethics referring to management directives;
- regulations and organisational structure referring to management directives;
- financial processes and obligation to accountability referring to managing directives;
- short summary of managing directives referring to the involvement of interested parties.

Caritas Internationalis and Civil–Military Cooperation

Caritas Internationalis cooperates with international, governmental and humanitarian organisations across a broad spectrum. [43] As it is present in war-torn areas, the cooperation with armed forces, especially with the army, is a priority area. [44] The Catholic Caritas, as the church itself, stays in crisis and war-torn areas when other organisations have decided to leave. The Caritas, as the charity organisation of the Catholic church, is aware of the conciliatory, mediatory role of the church, which is independent from states. Besides, it understands that to achieve efficiency and effectiveness in humanitarian aiding, it has to cooperate with political and military forces on a certain level. In order to achieve effective humanitarian aiding, it adopts the basic paradigms of those international organisations that take part in handling crises. Namely: prevention, the protection of the civil population

(especially the poorest), peacebuilding, reconciliation of warring parties, sympathy with victims, restoring the rights of victims or reinforcing social organisations.

The Catholic Caritas, as a humanitarian organisation, cooperates with military forces both on national and international level. It is difficult to lay down basic directives, as the experiences of Catholic Caritas organisations about the cooperation with military forces differ. Legal regulations, the relationship between the state and the church and the practice of cooperation between charity organisations and military forces are different in each country.

It is important for the charity organisation to establish the directives of cooperation on an international level, as well. So, in 2003 Caritas Internationalis tried to word some basic directives according to its experiences in handling crises during the Balkan wars in the1990s, during the interventions in Afghanistan in 2001 and in Iraq in 2003. [45] When wording the basic directives, the Caritas set out from its experiences of the cooperation with "Western" military forces, and Western military and political alliances. So, the basic paradigms were adjusted to these armies and military systems. The basic document was ready by 2006. Globally, it tries to word the basic directives that the staff of the Caritas has to consider when cooperating with military forces. The basic supposition of the Caritas is that the army have to take part in handling crisis in a way they do not endanger the independent and politics free operation of charity organisations. Caritas Internationalis learnt that military forces gradually took over humanitarian tasks, especially their control, when performing new crisis management and peace support operations. This phenomenon, according to the introduction of the document, weakens the abilities of humanitarian charity organisations. The basic directives of the UN referring to the cooperation between humanitarian charity organisations and military forces are determinant for Caritas Internationalis.

As crisis management can be divided into several parts, the basic document discusses the cooperation of the Caritas and military forces in different crisis management sections. They emphasize the importance of peacebuilding after armed conflicts or crises. The period of an armed conflict is more difficult, but the document finds it important that the Caritas should be present during a conflict and it should work hard to ease the difficulties of the poor. In a peacebuilding period the goals of the Caritas and UN peacekeepers, or other crisis management forces, are the same: to promote peace and reconciliation. Due to abuses committed by peacekeeping forces, the Caritas considers itself to be a control institution. In order to avoid abuses, it watches the activities of peacekeeping forces, as well. [46] As the UN itself encourages civil and church organisations to inform the UN headquarters about the abuses committed by peacekeepers, this controlling role is obvious for the Caritas.

The basic document of the Caritas focuses on the areas where it is extremely important for the Caritas to cooperate with the army considering its specific abilities. These areas are:
- prevent and ease emergency situation due to a natural disaster, as the army owns the appropriate logistic capacity and technique;
- epidemic prevention;
- the promotion of national vaccination programs;
- water clearing;
- reaching the areas that are highly inaccessible;
- helping refugees.

The document admits that the army can considerably help the effective work of a charity organisation in establishing communication, providing health care in inaccessible areas, organizing educational programs after a crisis, in reconstruction and in organizing defence against natural disasters. Besides, the document emphasizes that there are areas where employing the army is problematic. These problems are not characteristic features of Western national armies or international organisations. It is more difficult for the charity organisation if it has to cooperate with an army that supports one or the other party in a civil war instead of making peace. Similarly, if the army is compromised in an ethnic or a religious conflict, or if the army is involved in training child soldiers. According to the document, it is possible in democratic countries that charity activities become militarised, namely the whole humanitarian charity process is looked after by the army, which endangers the independence of charity organisations.

The basic document of the International Catholic Caritas words the directives of the cooperation with military forces:

- subsidiarity: the local decisions of the Caritas—even inside its own organisation—are considered to be more suitable and more realizable than decisions made on a higher level;
- partnership: the Caritas thinks it important to cooperate on the basis of trust which takes some time to be built;
- legality: the rules and principles of international law have special relevancy in the life of the organisation:
  - international law: complying with the Hague and Geneva Conventions and their additional documents;
  - Humanitarian Charter and Minimum Standards in Disaster Response (SPHERE), ICRC/NGO Code of Conduct, which words the basic principles referring to NGOs;
- human rights, refugees and the exiled (especially the views in the basic document of the UN Convention). As a significant part of the work of the Caritas is filled with aiding refugees, the norms referring to refugees have important roles in the life of the organisation.
- respect for human dignity;
- differentiation between militant and non-militant entities.

ICRC/NGO Code of Conduct:
- priority to humanitarian viewpoints;
- giving help regardless of religion, race or nationality;
- political neutrality:
  - foreign policy programmes are not supported.

The Catholic Caritas is an international organisation, so in a civil–military cooperation the legislation regulating organisations operating within country specific or international frameworks and military missions within alliance system should be considered at the same time.

Furthermore, the basic document words basic principles about operation: when an armed conflict has spread and none of the parties control the territory entirely, the possibilities of the organisations are limited on the war-torn territories. [47] The Caritas tries hard to

maintain a balanced relationship with each party, so that it can fulfil its humanitarian tasks. Establishing a relationship with armed forces and other organisations is significant as it is nearly impossible for civil or church organisations to get in a certain area during a conflict. According to the principles of the Caritas, when establishing a relationship with military forces, the Caritas should remain politically neutral. Cooperation and sharing information are important for the Caritas, but it respects politically, militarily and economic sensitive information. More principles are:

- establishing an appropriate distance towards military forces;
- the Caritas operates under non-military control;
- the Caritas respects the views of the local church;
- the organisation minimizes the relationship with those armed forces or/and soldiers that violate human rights;
- in advance, it determines those areas where it is going to operate, and determines the limits of its cooperation with military forces and local authorities.

If the army joins the humanitarian activities of the Caritas, the basic document expects the army to do it in accordance with international law and practice.

The basic document states that when aiding, soldiers cannot carry weapons, and those who help in health care should wear distinguishable uniforms on which the logo of the charity organisation can be seen.

According to the document there are three key areas where the Caritas cooperates with the army:

- regarding low intensity crises, the document draws attention that in spite of the crisis being low intensity, difficulties may arise during the cooperation of the organisations;
- during a low intensity crisis, the cooperation covers information sharing mostly:
- information sharing can be realized through appointing a liaison:
- dialogue—it involves getting familiar with the points of view of the organisation;
- information sharing—respecting classified and sensitive information.

According to the Caritas document, in case of high intensity crisis, adequate distance should be kept from military forces, but the Caritas may need military logistic or other support.

In high intensity crisis, the organisation has to accept military protection. It can happen that the political and the military parties rate the need of military protection differently. The directive is that the Caritas does not ask for military protection. It is an exceptional situation when the Caritas accepts this possibility, as local authorities, police and military forces cannot provide protection for the organisation. However, asking for protection and assistance depends on the decision of the Caritas management only, not of the authorities or military forces. Humanitarian viewpoints play important roles in the decision. The organisation does not accept protection from parties in conflict. The directive is that, even in this situation, the Caritas does not give the army any consignment so that it can distribute the donations. Last but not least, the Caritas does not act under military control, and rejects orders from military leaders.

Summary

Though a lot of charity organisations bear the attribute "Catholic", the official charity organisation of the Catholic Church is Catholic Caritas. The Catholic Caritas works on five continents in more than 160 countries, which shows the different environment and legislation it has to work within. The Catholic Church is an international organisation itself, with vast and complex structure, so each Caritas tries to meet global challenges under the control of an international overarching body. When national options have been exhausted, there are still possibilities to release major resources. Furthermore, there is more chance to control the Catholic nature.

The legal regulation of Caritas Internationalis has developed gradually. It gained its juridical personality first within the civil laws of the Vatican, later within the universal canon law of the Catholic Church. Earlier there were difficulties in connection with Catholic identity, possessions management and the communication with non-Catholic organisations. So, the Holy See gradually tightened both the operational legislation and the control of the organisation. It evoked the displeasure of those who imagined a looser alliance of each national Caritas under International Caritas. A new Holy See office, the Dicastery for Promoting Integral Human Development, established with motu proprio, Humanam progressionem, took over the controlling rights from the Pontifical Council *Cor Unum* on 31st August 2016, respecting the rights and tasks of the Secretariat of State and other Holy See dicasteries.

International Caritas is in relationship with international and national organisations, non-profit organisations and non-Catholic charity organisations. Regarding cooperation, the basic paradigms of international law, its rules and regulations and basic paradigms of the Caritas are significant. The basic principles regarding its cooperation with armies are also significant, as the Caritas is present in crisis-torn areas, and it cooperates with military forces in order to perform effective humanitarian aiding.

References

[1] LOMBARDI, V. L.: *Amicizia, carità, diritto.* Milano: Giuffrè, 1974.

[2] AYESTA, J.: González: Alcuni aspetti del servizio alla carità nella tradizione apostolica e nalla Didascalia dei Dodici Apostoli. In. MIÑAMBRES, J. (Ed.): *Diritto canonico e servizio della carità.* Milano: Giuffrè Editore, 2008. 441–456.

[3] FISCHL V.: Egyházi karitatív szervezetek szerepe a válságkezelésben. *Kard és Toll,* 2 (2006), 92–101.

[4] FERENC pápa: *Szolgáljátok a szegényeket! – A pápa előszava Teréz anya könyvéhez.* http://hu.radiovaticana.va/news/2016/07/23/a_p%C3%A1pa_el%C5%91szava_ter%C3%A9z_anya_k%C3%B6nyv%C3%A9hez/1246311 (Downloaded: 07.08.2017)

[5] A pápa a Nemzetközi Karitászhoz: legyetek a béke és a kiengesztelődés eszközei. *Vatikáni Rádió* (online), 2016. 11. 17. http://hu.radiovaticana.va/news/2016/11/17/a_p%C3%A1pa_a_nemzetk%C3%B6zi_karit%C3%A1szhoz_legyetek_a_b%C3%A9ke_eszk%C3%B6zei/1272891 (Downloaded: 07.08.2017)

[6] Szíria békéjéért: Ferenc pápa videó-üzenete a Nemzetközi Karitász békekampányához. *bonum* (online), 2019. 07.05. http://bonumtv.hu/sziria-bekejeert-ferenc-papa-video-uzenete-a-nemzetkozi-karitasz-bekekampanyahoz/ (Downloaded: 07.08.2017)

[7] Social Encyclicals Pope Leo XIII: 1891. *Rerum novarum;* XI. Pius: 1931. *Quadragesimo anno;* Paul VI: 1967. *Populorum progressio;* 1971. *Octogesima adveniens,* John Paul II: 1981. *Laborem exercens;* 1987: *Sollicitudo rei socialis,* 1991: *Centesimus annus.* See: TOMKA M., GOJÁK J.*: Az egyház társadalmi tanítása.* Budapest: Szent István Társulat. s.d. 27–55.

[8] ZAGYVA R: *Lángoló szeretet a Katolikus Karitász 80 éve*. Budapest: SZIT, 2011. 14–19.

[9] Caritas Internationalis. *NGO Monitor* (online), October 08, 2018. www.ngo-monitor.org/ngos/caritas/ (Downloaded: 07.08.2017)

[10] Caritas Internationalis. *Magyar Katolikus Lexikon* (online), s.d. http://lexikon.katolikus.hu/C/Caritas%20Internationalis.html (Downloaded: 07.08.2017)

[11] *A Katolikus Karitász is bekapcsolódott a Nemzetközi Karitász libanoni segélyakciójába*. Magyar Katolikus Püspöki Konferencia, 2006. 06. 24. http://uj.katolikus.hu/cikk.php?h=587 (Downloaded: 07.08.2017)

[12] ADÁNYI L.: Rendkívül súlyos a helyzet a Mianmarban. *Új Ember Hetilap,* 2017.05. 25.

[13] Nyolcvanéves a Katolikus Karitász. *Magyar Nemzet,* (online), s.d. https://mno.hu/eletmod/nyolcvan-eves-a-katolikus-karitasz-4473 (Downloaded: 07.08.2017)

[14] Ma 25 éve szerveződött újjá a Karitász Magyarországon. *Katolikus Karitász* (online), 2016. https://karitasz.hu/korabbi-hirek/ma-25-eve-szervezodott-ujja-a-karitasz-magyarorszagon (Downloaded: 07.08.2017)

[15] ADÁNYI L.: *A Magyar Katolikus Karitász Újjászervezése.* www.vhf.hu/sites/default/files/dokumentumok/rendezvenyek/2013/adanyilaszlo.pdf (Downloaded: 07.08.2017)

[16] Our mission. *Caritas* (online), s.d. www.caritas.org/who-we-are/mission/ (Downloaded: 20.08.2017)

[17] Nemzetközi Karitász találkozó. *Katolikus Karitász* (online), s.d. www.karitasz.hu/aktualis/korabbi-hirek/nemzetkozi-karitasz-talalkozo (Downloaded: 07.08.2017).

[18] HIEROLD, A.: Des deutschen Caritasverbands und die Diösenzancaritasverbände als Vereine von Gläubigen. In. AA. VV. *Das consoziative Element in der Kirche*. St. Ottilien: EOS Verlag. 1989. 939–941.

[19] DALLA TORRE, G.: La Caritas: Storia e natura giuridica. In. MIÑAMBRES, J. (Ed.): *Diritto canonico e servizio della carità*. Milano: Giuffrè Editore, 2008. 74.

[20] SECRETARIAT OF THE GERMAN BISHOPS' CONFERENCE: *The Catholic Church in Germany. Facts & Figures*. Bonn: DCM Druck Center Meckenheim GmbH, 2011, 38–40.

[21] Pope JOHN PAUL II: *Apostolic Letter Durante L'Ultima Cena.* 16.09.2004. w2.vatican.va/content/john-paul-ii/it/letters/2004/documents/hf_jp-ii_let_20040916_caritas-internationalis.html (Downloaded: 07.08.2017)

[22] SABBARESE, L.: Commentary on paragraph 146 of Pastor Bonus Apostolic Constitution. In. PINTO, P. V. (Ed.): *Cemmento alla Pastor Bonus e alle norme sussudiarie della Curia Romana*. Città del Vaticano: Libreria Editrice Vaticana, 2003. 213.

[23] ARRIETA, J: *Diritto dell'organizzazione ecclesiastica*. Milano: Giuffreè, 1997. 322.

[24] UJHÁZI L: A menekültek lelkipásztori és humanitárius gondozásnak szabályozása a katolikus egyház hatályos jogában. *Acta Humana: Hungarian Centre for Human Rights Publications*, 3 (2014), 57–86.

[25] MIÑAMBRES, J.: Status giuridico-canonico di Caritas Internationalis. *Ius Ecclesiae,* 1 (2005), 295–302.

[26] IVEREIGH, A.: Caritas: the takeover begins. *America* (online), 11 March 2011. www. americamagazine.org/content/all-things/caritas-takeover-begins (Downloaded: 09.08.2017)

[27] Pope FRANCESCO: Motu proprio. *Humanam progressionem,* 17.07.2016. w2.vatican. va/content/francesco/it/apost_letters/documents/papa-francesco-lettera-ap_20160817_ humanam-progressionem.html (Downloaded: 19 01 2017)

[28] Vatican Secretariat of State: Rescript 17/01/2011 Prot. N. 08397. *Acta Apostolicae Sedis,* 2 (2011), 2–127.

[29] Pope BENEDICT XVI: Encyclic Deus Caritas est. 2005. XII. 25. *Acta Apostolicae Sedis,* 3 (2006), 217–252.

[30] LAFFLITE, J.: Amore e giustizia nell enciclica Deus Caritas est: Prospettiva Teologica. In. MIÑAMBRES, J. (Ed.): *Diritto canonico e servizio della carità.* Milano: Giuffrè Editore, 2008, 6–18.

[31] Vatican Secretariat of State: General resolution Caritas Internationalis. *Acta Apostolicae Sedis,* 6 (2012), 910–918.

[32] GARCÍA, M. J.: *Le norme generali del Codex Iuris Canonici.* Roma: Ediurcla, 2002.

[33] Pope Benedict XVI Motu proprio. Intima Ecclesiae natura. 2012. XI. 11. n. 14–15. *Acta Apostolicae Sedis.* 104 (2012), 996–1004. [For the Hungarian Catholic Caritas see: *Együttműködési megállapodás a Katolikus Karitász és a Belügyminisztérium között.* www.karitasz.hu/korabbi-hirek/egyuttmukodesi-megallapodas-a-katolikus-karitasz-es-a-belugyminiszterium-kozott (Downloaded: 09.08.2017)]

[34] SCHOUPPE, J-P.: *Elementi di diritto patrimoniale canonico.* Mialno: Giuffrè, 1997.

[35] Pope BENEDICT XVI: Motu proprio. Intima Ecclesiae natura. 2012. XI. 11. *Acta Apostolicae Sedis,* 104 (2012), 996–1004.

[36] Pontifical Council Cor Unum: L'ispirazione teologica del nuovo quadro giuridico di Caritas Internationalis. *L'osservatore romano,* 2012. 05. 02.

[37] *Caritas Internationalis operation order.* Rome: Caritas Internationalis, 2003. www. caritas.org/wordpress/wp-content/uploads/2017/06/partnershipGuidingPrinciples.pdf (Downloaded: 08. 03. 2019.)

[38] FIORITA, N.: Dalla carità alle Caritas: un itinerario giuridico. *Stato, Chiese e pluralismo confessionale Rivista telematica,* 38 (2016) 19–23.

[39] *Statues.* Rome: Caritas Internationalis, 2017. www.caritas.org/wordpress/wp-content/ uploads/2017/05/StatutesEN.pdf (Downloaded: 08. 03. 2019.)

[40] *Code of Ethics & Code of Conduct for Staff.* Rome, Caritas Internationalis, 2014. www. caritas.org/includes/pdf/CodesEthicsConduct.pdf (Downloaded: 09.08.2017).

[41] Caritas Internationalis General Assembly. In. *Miscellaneous. International Review of the Red Cross.* 1972, 404.

[42] PADÁNYI J.: *Polgári-katonai együttműködés a békefenntartó műveletek során.* Budapest: Honvéd Vezérkar Hadműveleti Csoportfőnökség, 2001.

[43] *Caritas Internationalis Relations with the Military.* Rome: Istituto Salesiano Pio XI, 2003, 7.

[44] *Caritas Internationalis Relations with the Military.* Rome: Istituto Salesiano Pio XI, s.d. 10.

[45] UJHÁZI L.: A Magyar Katolikus Egyház szerepvállalása a migrációs válság kezelésében. *Honvédségi Szemle,* 1 (2017), 140–148.

Authors' Guide

AARMS is a peer-reviewed international scientific journal devoted to reporting *original research articles* and *comprehensive reviews* within its scope that encompasses the military, political, economic, environmental, social and public management dimensions of security.

The obligatory elements of the publication

- *the title of the publication;*
- *the name of the author(s);*
- *the academic degree, place of employment, type of job (status), e-mail address and ORCID ID of the authors;* (ORCID information and registration: http://openaccess. mtak.hu/index.php/kiadoknak/orcid and https://orcid.org/register)*;*
- *an* Abstract *of 8–10 lines presenting the main results and conclusions of the publication;*
- Keywords *(4–5 words);*
- *the exact (!) source of the figures and tables;*
- *conclusions in a separate chapter at the end of the publication;*
- *literature used (only those referred to).*

General information

The journal exclusively publishes articles and comprehensive reviews that have never been published before. Manuscripts that have already been published in *Hungarian (or any other language but English)* in another journal will also not be accepted by the editorial board. The length of the publication should be about 40,000 characters, i.e. 1 author's sheet.

Submission of the manuscript via Open Journal System (OJS):

http://journals.uni-nke.hu/index.php/aarms

Title system

The publication should contain no more than *three title rankings* in addition to the title of the article and chapters. Chapter titles should reflect the content of the chapters. When referring to the other chapters of the article, the numbering of the chapter titles might help. Otherwise, it is not a compulsory element.

Figures, tables, illustrations

- the figures and their explanation should be simple and clear;
- only English language illustrations are accepted;

- in the online version of the journal the publication of coloured illustrations and figures is possible; *nevertheless* the printed journal is exclusively black and white with a B5 format, so the coloured illustrations and figures must also have a grayscale version;
- the illustrations and figures must be given in a minimum 300 dpi definition in JPG or BMP format;
- in case the author does not use his/her own illustrations (pictures, photographs, figures, graphs, maps, tables etc.) *the precise source (in a verbatim citation!)* of the illustration must be provided; it is the duty and responsibility of the author to find out the owner of the copyright and, in case it is not freely applicable, purchase the authorisation for publication;
- the illustrations are to be placed in their appropriate places in the text;
- when applying mathematical graphs please use *MathType*.

References and literature used (the Harvard system)

Basic rules

No single name (source document) should appear in the main body of the text that is not present in the references and vice versa: no single name (source document) should appear in the references that is not present in the main body of the text!

References are given at the end of the publication in an alphabetical order, footnotes should only contain indications to the references at most.

References in the text: (author, year of publication); e.g. (Weber, 1978); or (Boss et al., 2015); in case of a verbatim citation (author, year of publication: page number[s]); e.g. (Weber, 1978: 16.); or (Boss et al., 2015: 33–35.) When there are references to author(s) with the same year of publication, then the differentiation is made by putting a, b, c, etc. after the given year of the publication; e.g. (Weber, 1958a) and (Weber, 1958b).

The name of the referenced institution or person (last name and the first letter of the first name) is to be given at the first occurrence. In references please give the DOI (Digital Object Identifier) code of the cited publication, as well as its Internet link, if available. In case the cited publication found on the Internet does not have an author or title, etc. its referenced form in the text should be (URL1), (URL2), etc. In the list of references this is to be given in the following form:

URL1: World Justice Project. worldjusticeproject.org/what-rule-law (Downloaded: 07.02.2018)

URL2: *Useful Tips for Social Media Security.* https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/ (Downloaded: 25.09.2016)

The URL sources are to be placed at the end of the list of references, and not at their customary places in the alphabetical order.

Formal requirements for references

DESCRIPTION		EXAMPLE	
Main types of referenced works	**Formal contents of the reference**	**A work included in the references**	**References in the text** **(in parentheses)**
Monograph	Author's Name (year of publication): *Title.* Place of publication, Publisher.	Weber, M. (1978): Economy and Society. Berkley, University of California Press.	(Weber, 1978) in case of verbatim citations: (Weber, 1978: 103.) or (Weber, 1978: 14–19.)
Study/ collection of studies	Author's Name (year of publication): Title. In Editor's Name (ed.): *Title of the volume.* Place of publication, Publisher. initial page–last page. [by languages: szerk./ ed., eds./Hrsg.]	Young, E. A. (2006): Taming the Most Dangerous Branch: The Scope and Accountability of Executive Power in the United States. In Craig, P. – Tomkins, A. eds.: The Executive and Public Law. Power and Accountability in Comparative Perspective. Oxford, Oxford University Press. 136–198.	(Young, 2006) in case of verbatim citations: (Young, 2006: 144.)
Article/ periodical	Author's Name (year of publication): Title. *Name of the journal,* Volume, Number. initial page–last page. DOI.	Howard, M. – Wilson, A. J. (1974): Military Science in an Age of Peace. *The RUSI Journal,* Vol. 119, No. 1. 3–11. https://doi.org/10.1080/03071847409421160	(Howard–Wilson, 1974)
More than one author for one work	every Author's Name (year of publication): Title. *Name of the journal,* Volume, Number. initial page–last page.	Boss, S. R. - Galletta, D. F. - Lowry, P. B. - Moody, G. D. - Polak, P. (2015): What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviours. *MIS Quarterly,* Vol. 39, No. 4. 837-864.	In the main body of the text: (Boss et al., 2015)
Other (e.g. manuscript)	Author's Name (year of publication): *Title.* Place of the publication. (The type of the document.)	Ürmösné Simon, G. (2017): *Technical English for Officers.* Budapest. (Manuscript.)	(Ürmösné Simon, 2017)
Internet content	Author's Name (year of publication): *Title.* website address (Access date) s. a. = sine anno (without year)	Lesch, A. M. (s. a.): Egypt's Spring: Causes of the Revolution. www.mepc.org/egypts-spring-causes-revolution (Downloaded: 03.06.2017)	(Lesch, s. a.)
Identical year of publication of the same author	Author's Name (year of publicationa): *Title.* Place of publication, Publisher. Author's Name (year of publicationb): *Title.* Place of publication, Publisher.	*We differentiate the works by putting Latin letters without space after the year of publication.* Weber, M. (1958a): The Three Types of Legitimate Rule. *Berkeley Publications in Society and Institutions,* Vol. 4, No. 1. 1–11. Weber, M. (1958b): *The Rational and Social Foundations of Music.* Carbondale, Southern Illinois University Press.	(Weber, 1958a: 1–11.) (Weber, 1958b)

Main abbreviations

(s. a.) = sine anno   –   without year
(s. l.) = sine loco   –   without place
(s. n.) = sine nomine –   without publisher's name
et al. = et alia   –   and others. (In case of more than three authors this abbreviation should (only!) be used in intra-text references. However, in the list of references the names of all the authors should be given in full!)
Vol. = volume
No.   = number