LUDOVIKA
UNIVERSITY PRESS

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE

Volume 19 (2020)
Issue 2

ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

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 and social dimensions of security and public management.

AARMS is published in one volume of four issues per year by the University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

All correspondence should be addressed to Prof. Dr. PADÁNYI József, Editor-in-Chief, University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary
aarms@uni-nke hu

AARMS
ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE
Volume 19
Issue 2
2020

An International Journal of Security, Strategy, Defence Studies,
Military Technology and Public Management
Published by the University of Public Service
PADÁNYI József (Chair of the Editorial Board)
SOLYMOSI József (Honorary Chair of the Editorial Board)

Publisher:

University of Public Service, Ludovika University Press
Responsible for Publishing:
KOLTAY András, Rector

Copy editor:

GERGELY Zsuzsánna

Typeset and print by University of Public Service

ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

Contents

AARMS Vol. 19, No. 2 (2020) 5–17.

10.32565/aarms.2020.2.1

The Balance of Power System of the Middle East[1]

Péter SELJÁN[2]

Since the onset of the Arab Spring, there has been a growing interest in the changing balance of power of the Middle East. The balance of power theory in global context has been extensively studied. However, little research has been dedicated to the theory's applicability solely at the regional level, especially with the contemporary Middle East in focus, while the region is suffering from armed conflicts involving virtually all the regional states as well as the great powers and many different non-state actors. This paper is an attempt to shed light on the applicability of the balance of power concept and the theory of omnibalancing in relation to the Middle East through reviewing the relevant literature.

Keywords: *balance of power, Middle East, omnibalancing, foreign intervention, proxy war*

Introduction

Recent studies have focused on the changing balance of power of the Middle East, however, the interpretation of this variously defined term/theory/concept remains a major issue for researchers. Since the end of the Cold War, many scholars have concluded that the balance of power is now outdated, and even some realists wonder if the concept still has relevance in the contemporary security environment. With regard to the balance of power of the Middle East, some argue that the balance of power theory is particularly inadequate as an explanation of developing world alignments because it does not consider specific characteristics of these regions.

According to previous studies, the competitive relations between Iran and Saudi Arabia today reflect the classical balance of power theory. However, the Middle East is currently suffering from armed conflicts involving virtually all the regional powers as well as the United States and Russia and many different non-state actors. The ongoing transformation of the region is mostly driven by local and regional factors, like the Arab Spring and the protracted civil wars as the drivers of an emerging new regional political order in the Middle East. This regional level conflict is more about establishing a balance of power,

[1] The present publication is the outcome of the project 'From Talent to Young Researcher project aimed at activities supporting the research career model in higher education', identifier EFOP-3.6.3-VEKOP-16-2017-00007 co-supported by the European Union, Hungary and the European Social Fund.

[2] PhD candidate, Corvinus University of Budapest, International Relations; e-mail: peter@seljan.hu; ORCID: https://orcid.org/0000-0002-9470-9509

or about the dominance of the region, while the country-level wars are about which elites govern a given state.

Additionally, proxy wars and foreign interventions are becoming a determining phenomenon of the international relations in the 21st century, especially in the Middle East, where since the start of the Arab Spring one external military intervention follows another. One can see this happening in some countries struggling with civil wars and armed conflicts such as Libya, Iraq, Yemen and Syria. The empirical literature on the phenomenon of proxy wars and foreign military intervention has made considerable progress in the last few decades, but there is still much to learn about the subject.

This paper is an attempt to review and summarise the relevant scientific literature in order to show how the balance of power and its related theories can be applied in relation to the contemporary Middle East region. The first section covers the interpretation of the balance of power at the regional level, describing the basic conditions of a regional system/order and its way of operation. The second section discusses the theory of omnibalancing, as an alternative to the original balance of power for the developing countries with special characteristics, the third section describes the complexities of the post-Cold War power structure. The last section of the paper provides a brief concluding summary of the discussion, along with a brief mentioning of the paper's limitations.

Theory, concept, system and order

The balance of power is a variously defined and much debated theory. At the same time, it is one of the oldest and most enduring concepts of international relations. It basically suggests that security is enhanced when power is distributed relatively equally so that no single state is strong enough to dominate all others. This means, that in a regional balance of power system, the power held and exercised by states is constantly checked and somehow balanced by the power of the other actors. Simply put, as a country's power grows to the point that it threatens other powerful states, a counter-balancing coalition emerges to restrain the rising power, in order to avoid the formation of a hegemony. According to one definition 'at its essence, balance of power is a type of international order', although its normal operation as such is still unclear.[3] Nevertheless, according to classical and neoclassical realists, the balance of power is a basic value of international relations and world politics, as a 'desirable institution and a good thing to strive for because it prevents hegemonic world domination by any great power'.[4]

The minimum requirements for a balance of power system can include the existence of at least two or more actors of roughly equal power capabilities, states seeking to survive and preserve their autonomy, alliance flexibility and the ability to wage war if it is necessary. Nine conditions can be jointly sufficient to bring about an effectively performing balance of power system. These are the following: (1) at least two actors; (2) cautiousness; (3) readiness; (4) standing by the weaker or less threatening side; (5) power projection capabilities; (6) war

[3] Randall L Schweller, 'The Balance of Power in World Politics', *Oxford Research Encyclopedia of Politics*, May 9, 2016, 9.

[4] Robert Jackson and Georg Sørensen, *Introduction to International Relations*. 4th ed. (Oxford: Oxford University Press, 2010), 70.

must be a legitimate tool; (7) smooth alliance formation; (8) pursuit of moderate war aims, and (9) striving for proportional compensations.[5]

Regarding the number of actors, for a balance of power to exist, obviously there must be at least two states that seek to survive under the anarchic conditions of the international relations, where the world lacks any supreme authority. States in a balance of power system act in ways that maximise their relative gains and avoid or minimise their relative losses.[6] States must be watchful and sensitive to changes in the distribution of capabilities with respect to actual or potential rivals and with regard to one's allies because the state must be able to recognise any deteriorating situation on either side and to take the necessary steps. As Gulick points out, states must not only be aware of any changes in the balance of power, they must be able to respond to them accordingly. Hence, 'policy must be continually readjusted to meet changing circumstances if an equilibrium is to be preserved'.[7] In addition, in a conflict states must join the less threatening side. States tend to flock to the weaker side, since the stronger side is what threatens them.[8] Structural realists argue that the most powerful state will always appear threatening because of the pervasive uncertainty. Thus, states flock to what they perceive as the less threatening side, whether it is the stronger or weaker.[9] It is important to note that 'it is not necessary that every state or even a majority of states balance against the stronger or more threatening side. Balancing behavior will work to maintain equilibrium or to restore a disrupted balance as long as the would-be hegemon is prevented from gaining preponderance […]. What matters is that enough power is aggregated to check preponderance'.[10]

Additionally, states must be able to project power through offensive military capabilities and war must be a legitimate tool of statecraft, since balancing behaviours are preparations for war actually.[11] It must be emphasised here, that the outbreak of war does not disconfirm, but in most cases, supports the theory, as the balancing of power rests on the expectation that states will settle their differences by fighting.[12] Furthermore, an effectively operating balance of power system requires continuous and unhindered alliance formation, which means that states must be able to align with other states freely, on the basis of power considerations, despite of the pre-existing 'alliance handicaps'.[13] For a balance of power system to operate, states should pursue moderate war aims and avoid eliminating main actors, since 'an equilibrium cannot perpetuate itself unless the major components of that equilibrium are preserved'.[14] Finally, in a balance of power system, proportional aggrandisement can maintain an existing equilibrium among the great powers through the

5 Schweller, 'The Balance of Power', 6–9.
6 Joseph M Grieco, *Cooperation among Nations: Europe, America and Non-tariff Barriers to Trade* (Ithaca, NY: Cornell University Press, 1993).
7 Howard E Gulick, *Europe's Classical Balance of Power* (Westport: Greenwood Press, 1982), 68.
8 Kenneth Waltz, *Theory of International Politics* (Massachusetts: Addison-Wesley, 1979), 127.
9 Stephen Walt, 'Alliance Formation and the Balance of World Power', *International Security* 9, no 4 (1985), 3–43.
10 Schweller, 'The Balance of Power', 7, 9.
11 Robert Jervis, 'From Balance to Concert: A Study of International Security Cooperation', *World Politics* 38, no 1 (1985), 60.
12 Harold Lasswell, *World Politics and Personal Insecurity* (New York: Free Press, 1965).
13 Jervis, 'From Balance to Concert', 60.
14 Gulick, *Europe's Classical Balance of Power*, 72–73.

prevention of any great power from making unfair relative gains at the expense of the others.[15]

In effect, all these conditions are met in case of the Middle East region, however, they need to be discussed further, since they can be debated or questioned. Nevertheless, there are sufficient number of regional powers under anarchic conditions.[16] States in the region are vigilant, that is, very sensitive to changes in the distribution of capabilities, and most of them are able to respond quickly and decisively to these changes in the balance of power. Additionally, states tend to flock to the weaker or less threatening side of a conflict, the regional powers are able to project power, war is a legitimate tool of statecraft, and the states in the region are pursuing moderate war aims and avoiding eliminating main actors so far. Perhaps the only problematical condition in case of the Middle East is the one which requires continuous and easy alliance formation. However, taking into consideration the warming Israel–Saudi relations – which was unthinkable a few years ago –maybe it can be concluded that today there are no alliance handicaps in the region.

Since this argument is about a regional balance of power system as an international order, it must be mentioned here how this term applies to the Greater Middle East[17] region. There are three types of balance of power systems. Structural realists believe in the 'automatic version' of the theory, whereby the balance in the system is spontaneously generated, self-regulating and basically an unintended outcome of power politics. According to the earlier 'semi-automatic' version of the theory, a 'balancer' state must throw its weight on one side of the scale or the other to regulate the system. And there is also the British School's version of a 'manually operated' system, where the state of equilibrium is the result of human contrivance.[18] It might be argued that the regional balance of power system of the Middle East region is an automatic one by default. However, when one takes into considerations the recent increase in the number of foreign interventions and the question of proxy wars, it can be considered rather a semi-automatic system.

A system exhibits order when there is an identifiable pattern in the relationship of its actors, or rather some discernible organising principle. When the operation of a system is highly predictable, order prevails, while disorder is a condition of randomness. The degree of order is partly a function of stability, which is the property of a system that causes it to return to its original condition after it has been disturbed from a state of equilibrium. Some

---

15 Schweller, 'The Balance of Power', 9.

16 As Spykman noted: 'It is obvious that a balance of power policy is in the first place a policy for the Great Powers. The small states, unless they can successfully combine together, can only be weights in a balance used by others.' See Nicholas J Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt, Brace, 1942), 20; Regional power can be defined as a power that is effective in its own region, but has limited global effect, while it can have an impact on the policies of great powers. Additionally, regional power could be defined as a state that has a hegemonic function and potential in its region. See Barry Buzan and Ole Wæver, *Regions and Powers: the Structure of International Security* (Cambridge: Cambridge University Press, 2003), 37.

17 The Middle East has always been a very vague term, in which countries were added and removed depending on the context. Our research area as the Greater Middle East and North Africa includes countries from West Africa to India (including Iran, Israel, Turkey, Afghanistan and Pakistan). In this regard, we use the term Middle East not as a merely geographical term to describe a region that lies between Asia and Africa, but more as a political one, as was introduced by George W Bush in 2004.

18 Schweller, 'The Balance of Power', 5; Inis L Claude, Jr, *Power and International Relations* (New York: Random House, 1962), 43–51; Michael Sheehan, *The Balance of Power: History and Theory* (London: Routledge, 2007), 67.

orders are durable, while others are unstable. Especially complex and delicately balanced systems, which may appear orderly at one moment but can become unpredictable and disorderly quiet unexpectedly.[19]

According to one definition of social order, international orders vary according to the amount of order displayed; whether the order is purposive or unintended; and the type of mechanisms that provide order.[20] On the one hand, there is rule-governed, purposive order, while on the other hand, there is an international order with entirely unintended recurrent patterns.[21] Here, in case of a regional balance of power system, international order is spontaneously generated and mainly self-regulating, since balance of power arises, though none of the actors may seek actual equality of power. All states may seek greater power than the others, but their power maximising actions produces the unintended consequence of a balance of power. As one theorist puts it, 'the actors are constrained by a system that is the unintended product of their coactions'.[22] The predictability of a social system partly depends on its degree of complexity. The operation of a balance of power system is relatively automatic and predictable, since it only requires states seeking to survive through pursuing power and security in an anarchic, self-help international system.[23] However, it is important to note here, that the balance of power systems does not function always properly and predictably, as balancing behaviour can be late, uncertain, or non-existent.[24]

Omnibalancing and foreign interventions in the Middle East

If one really intends to adapt the balance of power theory to the Middle East region, one must look at the possible balancing behaviours of the regional actors, which may serve as evidence for an operating regional balance of power system. For example, one must examine the alliance formation processes in the region. Alliances are usually viewed as a response to threats, yet there is still no agreement on what that response will be. States may either *balance*, that is, ally in opposition to the main source of danger, or ally with the state that poses the major threat, in one word, *bandwagon*.[25] Walt argues that if balancing is more common than bandwagoning, then states are more secure because aggressors will face combined opposition. But if bandwagoning is more prevalent, then security is scarce because aggression is rewarded. Walt in his Alliance Formation and the Balance of World Power presents each hypothesis in its simplest form and then revises them, arguing that balancing prevails over bandwagoning.[26] On the other hand, some scholars claim that states

19 Schweller, 'The Balance of Power', 9.

20 Hedley Bull, *Anarchical Society*. 3rd ed. (Houndmills: Palgrave Macmillan, 2002), 3–22.

21 There are three types of international orders: a negotiated or rule-based order, an imposed or non-voluntary order among unequal actors, and a spontaneously or automatically generated self-regulating order, which is an unintended consequence of actors seeking only to maximise their power.

22 Schweller, 'The Balance of Power', 10.

23 Richard K Betts, 'Systems for Peace or Causes of War? Collective Security, Arms Control, and the New Europe', *International Security* 17, no 1 (1992), 11–12.

24 Schweller, 'The Balance of Power', 11.

25 Here we use the terms 'balancing' and 'bandwagoning' as Walt used them. Walt's use of these terms follows that of Kenneth Waltz. Waltz, *Theory of International Politics*; Walt, 'Alliance Formation', 4; Arnold Wolfers, *Discord and Collaboration* (Baltimore: The Johns Hopkins University Press, 1984), 122–124.

26 Walt, 'Alliance Formation'.

have bandwagoned with or hid from threats far more often than they have balanced against them. Others, for instance argue that bandwagoning is more prevalent.[27] Furthermore, some find that balancing is relatively rare, since balances of power sometimes form, but there is no general tendency toward this outcome. States frequently wait, bandwagon, or, much less often, balance.[28]

As Steven R David points out in his Explaining Third World Alignment, while most of the earth's people live in developing, or, according to Cold War terminology, in Third World[29] countries, the foreign policy of these states and especially why they align as they do remains overlooked and under-researched. He argues that balance of power theory is particularly inadequate as an explanation of developing world alignments because it does not take into account specific characteristics of these regions. He suggests that the theory of 'omnibalancing' can be applied in case of the developing world, since it draws upon the key assumptions of balance of power while also correcting those elements that make it inapplicable to these regions. Thus, omnibalancing agrees with the core assumption of balance of power, that is: threats will be resisted. But, whereas balance of power focuses on the state's need to counter threats from other states, omnibalancing considers both internal and external threats to the leadership.[30] The theory of omnibalancing combines the need of leaders to appease secondary adversaries, as well as to balance against both internal and external threats in order to survive in power, taking into consideration the common conditions of the developing countries that leaders are generally weak and illegitimate and that the stakes for domestic politics are usually high. This theory assumes that the most important determinant of alignment is the drive of these weak and illegitimate leaders to ensure their political and physical survival.[31]

So, the main difference between balance of power theory and omnibalancing is that the latter asserts that realism must be broadened to examine internal threats in addition to focusing on external threats and capabilities, and that the leader of the state rather than the state itself should be used as the level of analysis. Despite important differences among the states considered developing states of the region in question, there are fundamental similarities among them, like their situation in which internal threats are far more likely to challenge their leader's hold on power than external threats from other countries. As David notes, the leaders of developing countries must pay more attention to retaining their hold on power, especially in the face of domestic challenges, while internal threats are more prevalent in these countries due to their special characteristics. We should bear in

---

27 Schweller, 'The Balance of Power', 11–12.

28 Robert Powell, *In the Shadow of Power* (Princeton, NJ: Princeton University Press, 1999), 196.

29 During the Cold War, the Third World referred to the developing countries of Asia, Africa and Latin America, the nations that are not aligned with either NATO or the Communist Bloc. Since the end of the Cold War, this terminology has been used less and less, and it is being replaced with terms such as developing countries or least developed countries. Researchers normally prefer the term developing countries; however, its definition is not universally agreed upon, and there is also no clear agreement on which countries fits this category. According to the International Monetary Fund's World Economic Outlook Database of October 2018, the following are considered developing economies of the Greater Middle East or Region: Afghanistan, Algeria, Bahrain, Djibouti, Egypt, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Somalia, South Sudan, Sudan, Syria, Tunisia, Turkey, United Arab Emirates, Yemen. (International Monetary Fund, 'World Economic Outlook', October 2018.)

30 Steven R David, 'Explaining Third World Alignment', *World Politics* 43, no 2 (1991), 233.

31 Ibid. 236.

mind that the great majority of them had been colonies out of which foreign powers created states where none had existed before. Thus, many began and remain more an artificial construct than a coherent unit. In many cases the state is often simply just the representative of a group that holds power in the capital. In consideration of this, legitimacy is likely to be weaker for the leaders of developing countries. It is also important to note, that since the consequence of loss of power in the developing countries of the Middle East region is often loss of life, leaders are understandably more aggressive than other leaders in their efforts to maintain their hold on power. Most of these states are governed by authoritarian rule, which also means that decisions in foreign policy are usually made by a single individual or by a narrow elite, perhaps.[32]

One of the unique characteristics of the Middle East region is the interrelationship between internal and external threats, since leaders and insurgents in the region commonly seek outside support to advance their interests, and their requests for help are often granted by outside states.[33] As David notes, internal threats are so prevalent in these countries that they represent an ideal vehicle for advancing the interests of foreign actors and outside states. Since the leadership of these states is often determined by the outcome of internal threats and conflicts, foreign actors with a special interest in the state's affairs may seek to influence that outcome. This generalisation about the developing countries of the Greater Middle East region is not intended to suggest that all of them share these characteristics equally, since we are all aware that different states manifest different strengths and weaknesses.[34]

It is important to note that at present, there are no studies confirming the overall applicability of omnibalancing to the developing countries of the Greater Middle East, and only an in-depth analysis of the region's alignment decisions could do that. However, in our opinion, with regard to the role of proxy wars and foreign interventions in the balance of power system of the greater Middle East, the logic of omnibalancing provides a better guide or additional explanation for foreign policy decisions.

The post-Cold War regional power structure

Currently, the Middle East is suffering from armed conflicts involving virtually all the regional states as well as the United States and the Russian Federation, and many different non-state actors. It is also important to note that while the Russian Federation and the United States are still engaged in the region's conflicts, the transformation ongoing today is mostly driven by local and regional factors, like the Arab Spring and the ongoing civil wars as the drivers of an emerging new regional political order in the Middle East.[35]

The current power dynamics in the Middle East can be traced back to the onset of the Cold War and the simultaneous emergence of many of the Arab countries from the rule

---

32 Ibid. 238–240.

33 Herbert K Tillema, 'Foreign Overt Military Intervention in the Nuclear Age', *Journal of Peace Research* 26, no 2 (1989), 179–185; Sebastian von Einsiedel et al., 'Civil War Trends and the Changing Nature of Armed Conflict', *United Nations University Centre for Policy Research*, Occasional Paper 10, March 2017.

34 David, 'Explaining Third World Alignment', 239–242.

35 Marc Lynch, *The New Arab Wars: Uprisings and Anarchy in the Middle East* (New York: Public Affairs, 2016).

of European colonialism into independence. It was the collapse of the global Cold War system nearly four decades later that set the Middle East on its current course. The end of the Cold War, and the period of American unipolarity that followed, led to a regional power imbalance, which the Middle East still contends with today. However, the conflict in the Middle East is more than just about revisionist and status quo powers, since the civil wars turned the region into a tripartite system, consisting of a struggle for power between Iranian, Arab and Turkish nationalisms.[36]

The advent of the Cold War and the security and economic needs of independent Arab states resulted in a situation that started to mimic the bipolar structure of the international system, dividing the Arab world into two camps. The Cold War period engendered a Middle East political order that persisted from the 1940s until the collapse of the Soviet Union in the early 1990s, which ultimately resulted in significant global geopolitical changes that contributed to the current power struggles that can be seen in the Middle East today. This geopolitical transformation created a new power structure for the region, consisting of states tilted towards the United States like Israel, Saudi Arabia, Jordan, U.A.E. and Egypt on one side, and a revisionist front on the other side with Iran in the lead, along with Syria tilted towards Russia, and with non-state actors like Hezbollah and Hamas, that have arrayed themselves to resist U.S. influence in the Middle East.[37]

Beyond doubt, the formal collapse of the Soviet Union in 1991 delivered a final blow to the Cold War regional order of the Middle East. There were several important effects of this event for all states. For instance, once Soviet allies like Syria, Iraq, Libya and Yemen had to reconfigure their economic and political establishment, as well as their foreign policies. Additionally, former Soviet allies also lost their security umbrellas and their ideological source, while the end of the Cold War ended the regional power balance. It is no mere coincidence that these states are civil war-torn countries today.[38] After the collapse of the Soviet Union, the United States remained the sole superpower, pursuing the policy of dual containment towards Iraq and Iran, in effect imposing a Pax Americana on the Middle East in the absence of a global rival.[39] Years later, in the immediate wake of the terrorist attacks of 11 September 2001, when the United States brooked no active resistance by Middle Eastern regimes, this unipolarity translated into military invasions of both Afghanistan and Iraq. By then it became more and more obvious, that the unity of the Arab world has been finally broken, if it has existed at all. These events turned out to be good opportunities for Iran to build deterrence against possible U.S. and Israeli invasions and to develop the wherewithal to push back against the regional influence of the United States.[40] The so-called Arab Spring standing for a series of pro-democracy uprisings that enveloped several largely Muslim countries, including Tunisia, Egypt, Libya, Yemen, Syria and Bahrain, signalled a new era for the Middle East.[41] Eventually, the American unipolarity led to a new rivalrous

---

36 Ross Harrison, 'Shifts in the Middle East Balance of Power: A Historical Perspective', *Al Jazeera Centre for Studies*, September 2, 2018, 14.

37 Ibid. 8.

38 Ibid. 6.

39 F Gregory Gause, 'The Illogic of Dual Containment', *Foreign Affairs* 73, no 2 (1994), 56–66.

40 Kayhan Barzegar, 'Iran's Foreign Policy in Post-Invasion Iraq', *Middle East Policy* 15, no 4 (2008), 47–58.

41 Erzsébet N Rózsa, 'Új világrend a Közel-Keleten?', *Nemzet és Biztonság: Biztonságpolitikai Szemle* 4, no 2 (2011), 2; Erzsébet N Rózsa, *Az arab tavasz: A Közel-Kelet átalakulása* (Budapest: Osiris Kiadó – Külügyi és Külgazdasági Intézet, 2015).

power structure in the region, defined by competing Sunni and Shi'i sectarian identities, and Iranian and Arab nationalisms, while during the Cold War, the Middle East reflected the simple bipolarity of the international system.[42]

After the Arab Spring: A multilayered and dysfunctional power system

The Arab Spring forced all the regional powers to manage the 'revolution' and to try to find a new Middle Eastern order. In their search for this new order, Saudi Arabia and Iran are acting on their claims to regional leadership, keeping in mind their national interests and foreign policy priorities.[43] As some point out, 'after the US invasion of Iraq, Iran's increasing power projection in the region has increased its area of influence through its support for the pro-Iranian Shia in Iraq, the Shi'ite opposition in Bahrain and the increased activity of the Shi'ite population in western Saudi Arabia, through the mobilization of the Zaydis of Yemen against the Saudi-backed Yemeni government, and the conversion of Alawites to Shi'ism in Syria'.[44] In addition, there must be mentioned the Iranian support for the Shi'ite Hazara people in Afghanistan, Lebanon's Hezbollah and the Palestinian Hamas in the Gaza Strip. Thus, in the last two decades Iran has built its regional alliances by promoting itself as an 'axis of resistance', while also pursuing a nuclear program as a critical element to increase internal national solidarity, as well as to bolster its claim for regional leadership in a new order. At the beginning of the Arab Spring, Iran even supported the protest movements, as the reaction of Muslim peoples against 'the Western-supported secular dictators'.[45]

Saudi Arabia is, beyond doubt, one of the most important countries in the Middle East, as a close ally of the United States, a supporter of various Salafist movements, and a leading state of the 'Sunni bloc' against Iran. According to Duran and Yilmaz, the Saudi model represents a conservative Wahhabi authoritarian regime. Even though it is a pro-status quo model, it still has an important role in shaping the new regional order. Saudi Arabia provided asylum to the fallen leader of Tunisia, supported Mubarak and the *coup d'état* in Egypt, and sent troops of the Gulf Cooperation Council to Bahrain, in order to maintain the regional status quo. However, Saudi Arabia supported the forces of the Arab Spring when the revolts appeared in favour of Riyad in Libya, Syria and partially Yemen, even though they threatened the regional status quo. Saudi Arabia follows sectarian and polarising policies by utilising the Iranian threat to gain the leadership role of its Sunni bloc. Saudi Arabia's basic role, as a leading member state of the GCC, has long been the protector of the Gulf monarchies against Iraqi and Iranian influence, and Riyad still wishes to be the guardian of the status quo.[46]

The civil wars in Yemen, Syria and Iraq turned into hotly contested proxy battles between formerly coexisting regional powers, and these wars created security vacuums that presented good opportunities for Saudi Arabia, Iran and Turkey to project their power. These

---

42 Harrison, 'Shifts in the Middle East Balance of Power', 9.

43 Burhanettin Duran and Nuh Yilmaz, 'Islam, Models and the Middle East: The New Balance of Power Following the Arab Spring', *Perceptions* 18, no 4 (2013), 140–141.

44 Ibid. 143.

45 Ibid. 143–147.

46 Duran and Yilmaz, 'Islam, Models and the Middle East', 147–148.

regional powers are pulled into these armed conflicts by 'vertical contagion', which means that conflicts do not just spread across borders horizontally to vulnerable neighbouring states, but also vertically to stronger and larger regional powers.[47] The civil wars in Syria, Iraq, Yemen and Libya have transformed into a regional conflict among the major regional powers, where, as Harrison emphasises it, 'a vicious competition for short-term regional dominance completely overshadows longer-term shared interests of a stable and prosperous Middle East'.[48] This regional level civil war is more about establishing a balance of power, or about the dominance of the region, while the country-level wars are about which elites govern the state.

The Russian military intervention in the Syrian Civil War has added a new layer of complexity to the distribution of power in the Middle East, turning the region into a three-layered power system. As Harrison points out, the first layer is the battle for the state being fought between the rebels and government in each civil war in question. The second layer is the battle for regional dominance being waged between Iran, Saudi Arabia and Turkey. And the third is the competition between Washington and Moscow, in Syria and the broader region. Today the main element of the regional power politics is the contest between Iran, Saudi Arabia and Turkey, playing out in the region's civil wars along indigenous ideological lines, while this time the United States and Russia shares some common interests in the Middle East, such as regional stability, counterterrorism and the cooperative management of the refugee crisis. As Harrison notes, 'while this is a multi-layered system consisting of local, regional and international actors, it is far more complex than the Cold War system of the past'.[49]

Conclusion

The aim of this paper was to shed light on the applicability of the balance of power concept and the theory of omnibalancing in relation to the Greater Middle East region. Since the collapse of the Soviet Union, many scholars of international relations have come to believe that the balance of power theory is now obsolete. According to liberal critics, international politics has been transformed as democracy expands, as interdependence and international institutions get stronger. Even some realist thinkers wonder if balance of power still operates at the global level in our contemporary world. Balancing behaviour practically makes no sense in today's world, since nuclear arsenals assure great powers of the ultimate invulnerability of their sovereignty.[50] However, this does not necessarily mean that the theory of balance of power cannot be applied at the regional level, for instance to the Middle East.

---

47 Harrison, 'Shifts in the Middle East Balance of Power', 9; Erika Forsberg, 'Transnational Dimensions of Civil Wars: Clustering, Contagion, and Connectedness', in *What Do We Know about Civil Wars?* ed. by T. David Mason and Sara McLaughlin Mitchell (Lanham – Boulder – New York – London: Rowman & Littlefield, 2016), 75–90.

48 Harrison, 'Shifts in the Middle East Balance of Power', 10.

49 Ibid. 11.

50 Edward Rhodes, 'A World Not in the Balance: War, Politics, and Weapons of Mass Destruction', in *Balance of Power: Theory and Practice in the 21st Century*, ed. by T V Paul, James J Wirtz and Michel Fortmann (Stanford: Stanford University Press, 2007).

The competitive relations between Iran and Saudi Arabia today reflect the classical balance of power theory, which in the narrow and simple sense can be described as a condition and structure with no hegemonic power among states and where states have relatively equal or similar powers. Balance of power is a realist concept and a separate theory at the same time, that is, a theoretical concept.[51] Balance of power also offers a structural approach according to which bipolar or multipolar balance of power structures emerge in the international regional system. With regard to the Middle East region, it is probable to notice a multipolar structure in the region, while balance of power could be established either bilaterally or multilaterally. Balance of power is fundamentally related to the international distribution of power. If the theoretical concept is adopted to the Middle East, there is a simple balance of power between Iran and Saudi Arabia in the narrow sense, while the complex balance of power – which refers to the condition of more than two rivalries – may include Iran, Saudi Arabia, Turkey and Israel as regional powers.

A fundamental concept of the realist school of international relations is that states seek to maximise security by maintaining a balance of power, whether in response to a growth in capabilities[52] or a growth in threats.[53] Accordingly, in response to the growing power and perceived as threatening behaviour of Iran, realism predicts rational actors, whose security is threatened by such a shift in power capabilities, will begin to balance Iran. Thus, actions taken by states like Saudi Arabia, the United Arab Emirates, Egypt and Israel can be considered understandable. Additionally, since Kenneth Waltz and Stephen Walt formulated the simple balancing and bandwagoning behaviours,[54] developments in the discipline of international relations over the past decades have identified a wider array of potential state behaviours including buck-passing (or free-riding), soft balancing, omnibalancing, underbalancing, offshore-balancing and so on. This variety of possible balancing behaviours might provide alternative theories to account for certain nations' foreign policy.

This paper focused on the applicability of the balance of power theory at the regional level as an order forming principle in case of the Middle East, offering an alternative with the introduction of the theory of omnibalancing. However, there are no studies confirming the overall applicability of omnibalancing to the developing countries of the region. Future in-depth analysis of the region's alignment decisions should provide evidence for that.

References

Barzegar, Kayhan, 'Iran's Foreign Policy in Post-Invasion Iraq'. *Middle East Policy* 15, no 4 (2008), 47–58. DOI: https://doi.org/10.1111/j.1475-4967.2008.00368.x

Betts, Richard K, 'Systems for Peace or Causes of War? Collective Security, Arms Control, and the New Europe'. *International Security* 17, no 1 (1992), 5–43. DOI: https://doi.org/10.2307/2539157

Bull, Hedley, *Anarchical Society*. 3rd ed. Houndmills: Palgrave Macmillan, 2002.

51 TV Paul, James J Wirtz and Michel Fortmann, *Balance of Power* (Stanford: Stanford University Press, 2007).
52 Waltz, *Theory of International Politics*.
53 Walt, 'Alliance Formation'.
54 Waltz, *Theory of International Politics*; Walt, 'Alliance Formation'.

Buzan, Barry and Ole Wæver, *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003. DOI: https://doi.org/10.1017/CBO9780511491252

Claude, Inis L Jr, *Power and International Relations*. New York: Random House, 1962.

David, Steven R, 'Explaining Third World Alignment'. *World Politics* 43, no 2 (1991), 233–256. DOI: https://doi.org/10.2307/2010472

Duran, Burhanettin and Nuh Yilmaz, 'Islam, Models and the Middle East: The New Balance of Power Following the Arab Spring', *Perceptions* 18, no 4 (2013), 139–170. Online: https://dergipark.org.tr/tr/download/article-file/816037

Einsiedel, Sebastian von et al., 'Civil War Trends and the Changing Nature of Armed Conflict'. *United Nations University Centre for Policy Research*, Occasional Paper 10, March 2017. Online: https://collections.unu.edu/eserv/UNU:6156/Civil_war_trends_UPDATED.pdf

Forsberg, Erika, 'Transnational Dimensions of Civil Wars: Clustering, Contagion, and Connectedness', in *What Do We Know about Civil Wars?* ed. by T David Mason and Sara McLaughlin Mitchell. Lanham – Boulder – New York – London: Rowman & Littlefield, 2016.

Gause, Gregory F, 'The Illogic of Dual Containment'. *Foreign Affairs* 73, no 2 (1994), 56–66. DOI: http://doi.org/10.2307/20045919

Grieco, Joseph M, *Cooperation among Nations: Europe, America and Non-tariff Barriers to Trade*. Ithaca, NY: Cornell University Press, 1993. DOI: https://doi.org/10.7591/9781501725043

Gulick, Howard E, *Europe's Classical Balance of Power*. Westport: Greenwood Press, 1982.

Harrison, Ross, 'Shifts in the Middle East Balance of Power: A Historical Perspective', *Al Jazeera Centre for Studies*, 2 September 2018. Online: https://studies.aljazeera.net/sites/default/files/articles/reports/documents/d5c3525d0759469eb1569983a729a408_100.pdf

International Monetary Fund, 'World Economic Outlook', October 2018. Online: www.imf.org/~/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx

Jackson, Robert and Georg Sørensen, *Introduction to International Relations*. 4th ed. Oxford: Oxford University Press, 2010. DOI: https://doi.org/10.1093/hepl/9780198707554.001.0001

Jervis, Robert, 'From Balance to Concert: A Study of International Security Cooperation', *World Politics* 38, no 1 (1985), 58–79. DOI: https://doi.org/10.2307/2010351

Lasswell, Harold, *World Politics and Personal Insecurity*. New York: Free Press, 1965.

Lynch, Mark, *The New Arab Wars: Uprisings and Anarchy in the Middle East*. New York: Public Affairs, 2016.

Rózsa, Erzsébet N, 'Új világrend a Közel-Keleten?' *Nemzet és Biztonság: Biztonságpolitikai Szemle* 4, no 2 (2011).

Rózsa, Erzsébet N, *Az arab tavasz: A Közel-Kelet átalakulása*. Budapest: Osiris Kiadó – Külügyi és Külgazdasági Intézet, 2015.

TV Paul, James J Wirtz and Michel Fortmann, *Balance of Power*. Stanford: Stanford University Press, 2007.

Powell, Robert, *In the Shadow of Power*. Princeton, NJ: Princeton University Press, 1999. DOI: https://doi.org/10.2307/j.ctv10crg4t

Rhodes, Edward, 'A World Not in the Balance: War, Politics, and Weapons of Mass Destruction', in *Balance of Power: Theory and Practice in the 21st Century*, ed. by TV Paul, James J Wirtz and Michel Fortmann. Stanford: Stanford University Press, 2007.

Schweller, Randall L, 'The Balance of Power in World Politics', *Oxford Research Encyclopedia of Politics*, 9 May 2016. Online: https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-119 DOI: https://doi.org/10.1093/acrefore/9780190228637.013.119

Sheehan, Michael, *The Balance of Power: History and Theory*. London: Routledge, 2007.

Spykman, Nicholas J, *America's Strategy in World Politics: The United States and the Balance of Power*. New York: Harcourt, Brace, 1942.

Tillema, Herbert K, 'Foreign Overt Military Intervention in the Nuclear Age'. *Journal of Peace Research* 26, no 2 (1989), 179–196. Online: www.jstor.org/stable/423868

Walt, Stephen, 'Alliance Formation and the Balance of World Power', *International Security* 9, no 4 (1985), 3–43. DOI: https://doi.org/10.2307/2538540

Waltz, Kenneth, *Theory of International Politics*. Massachusetts: Addison-Wesley, 1979.

Wolfers, Arnold, *Discord and Collaboration*. Baltimore: The Johns Hopkins University Press, 1984.

AARMS Vol. 19, No. 2 (2020) 19–28.

10.32565/aarms.2020.2.2

Artificial Intelligence as a Dual-use Technology

Éva AMBRUS[1]

The aim of this article is to give an overview of the state of artificial intelligence regarding malware attacks, its uses in the military and views regarding if it should be classified as a dual-use technology. As an emerging technology, with a wide variety of use and capabilities, more could be done to overview its uses, and some form of control over it. While the classical exports control might be counterproductive, a more closed approach towards critical information dissemination might be advisable until the full range of capabilities of artificial intelligence will be known.

Keywords: *artificial intelligence, dual-use technology, military use, malware*

Introduction

The security paradigm is changing. Until a new definition comes forward, policy-makers, academia and users will debate its nature and possible effects. Asymmetrical warfare, hybrid warfare, 'grey area' warfare, (dis)information warfare, unpeace are just a few names used trying to pinpoint the development of (IT) technology on security. Warfare and security includes more and more cyberspace, including cyber weapons, cyber espionage and cybersecurity. One driver of this change is the advances made in the last decade regarding artificial intelligence (AI). In this article I will present the idea that AI should be classified as a dual-use technology, meaning that it can be used for both civilian and military applications. I will start with presenting where AI weapons are today, followed by the nature of the relationship between state and technology. I will then present a case for thinking about AI as a dual-use technology.

AI as a weapon

Writing an article about artificial intelligence and its uses can leave one with more questions than answers. And as the 'grey area' warfare, or this era of 'unpeace', even questions have a high complexity. With these in mind, my aim with this article is to shed light to some of the questions asked today regarding the malign use of artificial intelligence. There is little

[1] PhD student, University of Public Service, Faculty of Military Science and Officer Training, Doctoral Schools of Military Sciences and Military Engineering, e-mail: ambrus.eva.eszter@gmail.com; ORCID: https://orcid.org/0000-0002-8354-1296

question that AI will make cyber warfare more powerful, increasing its scale, speed and power. Merriam-Webster defines artificial intelligence as: (1) a branch of computer science dealing with the simulation of intelligent behaviour in computers; and (2) the capability of a machine to imitate intelligent human behaviour.[2] Although this encompasses the basic notion, it is still not a complete definition. This lack of certainty also comes from the notion of intelligence. What is intelligence? In case of AI, science has focused on different aspects, such as learning, reasoning, problem solving, perception, language and many others. Another approach is to focus on the goals and aims of AI. This is the notion put forward by Russel and Norvig, as well. There is no agreed definition of artificial intelligence. Russel and Norvig summarised the four main schools of thoughts as AI in the following way: (1) thinking humanly; (2) thinking rationally; (3) acting humanly; and (4) acting rationally.[3] For this article, I will use the 4th approach, defining AI as a system that acts rationally, thus AI can be called a rational agent. 'A rational agent is one that does the right thing',[4] the 'right thing' being the most successful outcome for the agent (in this case, AI).

A branch of AI is machine learning. Machine learning refers to the ability of a computer to learn using large sets of data (not just predefined rule sets).[5] Machine learning can basically be supervised, reinforced or unsupervised. In supervised learning, the machine is trained to perform a specific task, such as recognising cats in pictures. For it to learn to distinguish this, it needs large amounts of tagged data, and this also includes checking the correct answers. Supervised training is used for tasks requiring information classification (for example filtering spam messages). Reinforced learning is giving direct feedback to the autonomous system about its output (for example did it classify correctly). In case of unsupervised learning, the program is not assigned any task and the data is unlabelled, so it is free to find its own correlations in the data. Learning from the data, the machine creates clusters in the given data and sets association rules that combine the various variables in the data. In cybersecurity, this can be the detection of malware.

An interesting part regarding machine learning and adaptability in the concepts of the human-in-the-loop (HITL). Basically, it combines human and artificial intelligence to create machine learning models with humans directly involved in training, tuning and testing the data. It is understood that HITL is important in cases when the cost of error is too high, when the ML algorithm cannot have any margin of error.[6] This would be the case in any military application, but also for autonomous driving. Literature distinguishes between human-in-the-loop, human-on-the-loop and human-off-the-loop. In the first case (HITL), the human has the final say in the execution of the lethal force (for example drones). In the second case, the decision can be made without the human operator, but the operator can override it. In the third scenario, the human operator cannot override the weapon system's triggering mechanism, so there is no human intervention possible.[7]

---

2 'Artificial intelligence', Merriam-Webster dictionary.

3 Stuart J Russell and Peter Norvig, *Artificial Intelligence. A Modern Approach* (New Jersey: Prentice Hall, 2010), 2.

4 Russell and Norvig, *Artificial Intelligence*, 4.

5 'Machine learning', Dictionary.com.

6 Mothi Venkatesh, 'What is Human-in-the-Loop for Machine Learning?', Hackernoon.com, July 17, 2018.

7 Seumas Miller, *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (Springer International Publishing, 2018), 100.

Reviewing the literature, it seems generally believed that an antivirus system with artificial intelligence and machine learning is the solution to modern malware attacks.[8] Malware can be defined as unwanted software which performs non-benign operations on any system. Avi Pfeifer et al. gave two insights into malwares. The first is that like biological viruses, they are rarely de novo; malwares are re-used to avoid detection and hide similarities. Secondly, regarding the functioning of malwares, it is harder to obfuscate what it does try to accomplish than how it wants to do it – it leaves a trace. It can be seen from these analogies, that malwares are changing fast, and the adaptability of AI and ML needs to be high.[9]

Adaptability faces at least two challenges: costs and adversarial attack. As we have seen, for ML to work well, it needs data (either labelled or unlabelled) to learn from. If the task is that it is trained for changes day-by-day, it means that it needs continuous training to be able to differentiate between benign or non-benign software. The second challenge, adversarial attack refers to the tactic of 'poisoning the well', or in this case, the training data sets. Recent research shows that deep learning is sensitive to contrasting, contradictory examples where the opponent can manipulate the input of the deep learning model in such a discreet way by adding minimal disruption to the input material to produce the desired result, that is, misclassification.

Its structure is due to the system of so-called neural networks. Neural networks are made up of elementary computing units – so-called neurons, which form interconnected layers. Each neuron applies an activation function to its input to create a specific output. Starting with model input, each network layer produces an output that the next layer uses as input. Networks with a single intermediate layer – hidden – are considered shallow neural networks, while models with multiple hidden layers are deep neural networks. They are sensitive to the manipulation of opposite examples of their inputs. 'Adversarial examples are inputs to a classifier specifically crafted to deceive the model, causing misclassification'.[10] Training models developed based on real and simulated data may be significantly more secure, but its development can come with a higher cost. One solution to this is counter-narrator training,[11] which is to improve the model's generalisation ability, that is, the prediction of patterns outside the learner's data set. Good generalisation also generally makes the classification less sensitive to minor disturbances and therefore, more resistant to conflicting examples.

Cybersecurity is often thought as passive, meaning the systems are waiting for the attack and all AI can do is help detect, categorise and respond to the attack.[12] AI-enhanced cyber weapons will have wider scope and greater speed than today's adversarial AI. One of the threats of the future would be that these AI-enabled tools would enable, for example

---

8 Sherif Saad, William Briguglio and Haytham Elmiligi, 'The Curious Case of Machine Learning in Malware Detection', Arxiv.org, May 18, 2019.

9 Avi Pfeffer, Brian E Ruttenberg, Lee Kellogg, Michael Howard, Catherine Call, Alison M O'Connor, Glenn Takata, Scott Neal Reilly, Terry Patten, Jason Taylor, Robert Hall, Arun Lakhotia, Craig Miles, Daniel Scofield and Jared Frank, 'Artificial Intelligence Based Malware Analysis', Arxiv.org, April 27, 2017.

10 Nuno Martins, José Magalhães Cruz, Tiago Cruz and Pedro Henriques Abreu, 'Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review', *IEEE Access* 8 (2020), 35417.

11 Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jonathon Shlens and Zbigniew Wojna, 'Rethinking the Inception Architecture for Computer Vision', *CVPR* (2016), 2818–2826.

12 Anna L Buczak and Erhan Guven, 'A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection', *IEEE Communications Surveys Tutorials* 18, no 2 (2016), 1153–1176.

'data-poisoning'. Data poisoning attacks are attacks when 'malicious users inject false training data with the aim of corrupting the learned model'.[13] As we have seen machine learning depends on datasets, and tampering with the input data to divert its results would mean it is at best underperforming, undetectably. The time for the human-in-the-loop to detect such functioning anomaly is essential, especially as more and more systems can (and will) become autonomous. Adaptability on the defence side faces more constraint than on the attackers' side. Some of these factors are financial (costs), personnel (retraining), performance (should not degrade system performance), usability and manageability, operations (fitting into the security operation), design (built-in preferred), perception (of the usefulness of defensive technology).[14]

Dual-use technology

There are valid concerns about the increase of autonomy of weapons system, and ethical questions are raised. Non-governmental organisations like International Committee for Robot Arms Control would limit the research and development of AI to civilian use only. On the other hand, these technologies are already being developed and tested. Large scale deployment will not happen until the margin of error of these systems will be close to zero, thus the importance of the mentioned human-in-the-loop in the process. But it is imaginable that in the future these autonomous systems will be more accurate than humans, thus new ethical questions will be raised.

Artificial intelligence and its uses in attacks or defences are emerging technologies. Emerging technologies can be described as 'technologies that have disruptive potential but have not yet been developed to their fullest potential'.[15] AI throughout its history had several 'growth' periods, when technological advances made it possible to develop it further. Its full scope of practical uses still cannot be determined and it is used in both military and civilian industry. In theory, there is the possibility of misuse by different actors. One can argue, that most technology can be used for more than one purpose, but the term 'dual-use' is reserved for technology that has a significant government application (and thus pertains to national security) and a private sector application, as well. At one point PlayStation 2 was briefly considered a dual-use technology by Japan.[16]

Gregory Lewis et al. in their article present the case of information hazard in biotechnology. Their view is that both openness and secrecy of information may backfire. They suggest 'that mitigation of these hazards can be improved if one can: (1) anticipate hazard potential before scientific work is performed; (2) consider how much the new

---

13 Jacob Steinhardt, Pang Wei Koh and Percy Liang, 'Certified Defenses for Data Poisoning Attacks', Arxiv.org, November 24, 2017.

14 Sean M Price, 'Adaptive threats and defences', in *Information Security Management Handbook*, vol. 4, ed. by Harold F Tipton and Micki Krause (Auerbach Publications, 2019), 44–45.

15 Daniele Rotolo, Diana Hicks and Ben R Martin, 'What Is an Emerging Technology?', Arxiv.org, January 4, 2016, 4.

16 Associated Press, 'Sony's High-Tech Playstation2 Will Require Military Export License', *Los Angeles Times*, April 17, 2000.

information would likely help both good and bad actors; and (3) aim to disclose information in the manner that maximally disadvantages bad actors versus good ones'.[17]

As per the EU's definition 'dual-use items are goods, software and technology that can be used for both civilian and military applications'.[18] We have seen the definition in the EU, but for its research and development programme, 'Horizon 2020, is more specific, requiring applicants for funding to ensure that "research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications," and they are required to complete an ethics checklist to demonstrate that they comply with this requirement'.[19]

AI systems and their design knowledge can be used for both civilian and military applications, and more broadly for beneficial and harmful purposes. Artificial intelligence is dual-use in the same sense as human intelligence. Many of the tasks that would be useful to automate are themselves dual-use. For example, software vulnerability detection systems have both offensive and defensive applications, and there is little difference between the capabilities of an autonomous drone used to transport packages and an autonomous drone used to transport explosives. In addition, basic research aimed at understanding AI, enhancing its abilities and controlling it is inherently dual-use. Machine learning (and AI) is a fairly open field, where researchers share details about their models and codes on the internet, as well. Hagendorff introduces the notion of 'forbidden knowledge', which is akin to Bostrom's 'information hazard'. While the latter is 'a risk that arises from the dissemination or the potential dissemination of (true) information that may cause harm or enable some agents to cause harm',[20] while the former is defined as (scientific) knowledge that is too dangerous to be disseminated unrestrictedly, for example in the fields of IT security or synthetic biology.[21]

One of the trends is the increase of existing threats. The cost of attacks is decreasing with the spread of AI to perform tasks that generally require human work, intelligence and expertise. As a result, the range of actors capable of carrying out certain attacks, the speed at which the attacks are executed and the set of potential targets will increase. An emerging threat of using AI systems to perform tasks that are virtually unmanageable by humans is the fact that attackers can exploit vulnerabilities in AI systems. The typical nature of threats is changing. With the increasing use of AI, attacks will become more effective, highly targeted, difficult to associate with a perpetrator, and are likely to exploit vulnerabilities in AI systems. Cybersecurity is an area that takes early and enthusiastic advantage of AI. The adaptability of AI systems can also change the strategic environment of cybersecurity, the attack/defence balance. The systems currently in use are quite effective against typical human-made malware, and research has already shown that AI systems will soon be able to circumvent their protection.

---

17 Gregory Lewis, Piers Millett, Anders Sandberg, Andrew Snyder Beattie and Gigi Gronvall, 'Information Hazards in Biotechnology', *Risk Analysis* 39, no 5 (2019), 1.

18 European Commission, 'Dual-use trade controls'.

19 Tara Mahfoud, Christine Aicardi, Saheli Datta and Nikolas Rose, 'The Limits of Dual Use', *Issues in Science and Technology* 34, no 4 (2018).

20 Nick Bostrom, 'Information Hazards: A Typology of Potential Harms from Knowledge', *Review of Contemporary Philosophy* 10 (2011), 45.

21 Thilo Hagendorff, 'Forbidden knowledge in machine learning. Reflections on the limits of research and publication', Arxiv.org, November 2019, 3.

Trends

Attitudes of society might change regarding AI as the coming generations are more and more confident in it. As with other technologies before, it may not be possible to clearly separate the civilian and military uses of it. Like the dual-faced God Janus, many of our everyday technology can be used for both purposes. We have to accept the fact that this technology will be used by actors for harm and prepare for it.

Carrick Flynn wrote a brief issue on the export control of artificial intelligence. His findings (regarding the *state of play* in the United States) are summarised in four main points:

(1) New export control regulations on general purpose AI software, untrained algorithms, and datasets without military use are unlikely to succeed and should not be implemented.

(2) Highly application-specific AI software, trained algorithms, and militarily sensitive data sets are useful targets for export control, but are already covered by the current export control regime.

(3) Equipment for manufacturing AI chips is likely a highly effective point of export control.

(4) The effectiveness of export controls on AI chips will depend on early implementation of export controls on chip manufacturing equipment. AI chips themselves are not yet a promising target for expanded regulation.

Per his findings, the (3) option could be a next step in export control regulation. In his view: 'The computing power required for AI increasingly relies on specialized microprocessors (AI chips) optimized for AI applications. AI chips are produced using highly advanced semiconductor manufacturing equipment that is relatively easy to define, monitor, track, and control.'[22]

New export control (option 1) would go against the fact that at this point innovation in AI relies on openness in the field, thus could harm research, as well as damaging relations between governments and the industry.

AI is becoming an important factor in maintaining the economic and national security of most countries, but as new technologies develop, so should new tools to address them. In the 20th century, one way of maintaining technological superiority was through export controls. Export controls are a web of regulations that prohibit the transfer of certain commodities or information, motivated by national security concerns or trade objectives, or both. Effectiveness of such measures in a globalised value-chain world remains dubious, as it needs to balance research and development needs (which thrive in an open environment) as well the interests of multinational technological corporations, allied countries and scientists.[23]

Norms prevailing in the AI research community show a strong tendency towards openness. Most new research is published online, often sharing all the information from

[22] Carrick Flynn, 'Recommendations on Export Controls for Artificial Intelligence', *Centre for Security and Emerging Technology*, February 2020.

[23] Jade Leung, Sophie-Charlotte Fischer and Allan Dafoe, 'Export controls in the age of AI', *War on the Rocks*, August 28, 2019.

the outline, through the algorithmic details to the source code. This level of openness has clear benefits in enabling researchers to rely on each other's work, fostering collaboration. Rather, it is a thought-provoking idea of what solutions may be needed when it comes to moving away from openness for security reasons. Should a risk assessment be conducted before publishing in detail AI attacks that can be used for attack? This is the norm, for example, in the field of biotechnology. Or would it be too early for this measure to await its widespread adoption, assessing which technical research is most important for safety? Should a community be established in which certain types of research results can be selectively shared among a predetermined set of criteria that meet certain criteria, such as effective information security and appropriate ethical standards? What can be learned from other models of dual-use technology sharing?

AI in the military

Regarding the uses of artificial intelligence in the military, one of the areas concerned is about decision-making.[24] The use of AI in analysis, classification is already in use (for example in the automotive industry) and will help decision-makers 'by providing easy-to-understand analysis and recommendations based on big data[25]'. The question of control in the military is especially important, although most articles underline that humans will remain the final decision-makers. Scott D Sagan explores the connection between ethics, technology and war. In his view, new technologies could reduce collateral damage, but also lower the political cost of engagement, thus more conflicts would emerge.[26] This is a trend seen in the 'grey area' conflicts, like cyber weapons. Artificial intelligence is changing the nature and principles of warfare by making decision-making cycles faster, advantages provided by AI will be for those that can apply AI in the broadest sense, and thus a revision of concepts regarding the organisation, control and command of military forces will be needed.[27]

Another distinction that can be made is that technology shapes warfare, the conduct of war. This distinction is important because more and more violence nowadays is not confined to a precise geographic area, and the opponents are also not clearly defined. Grasping a new definition of conflict, or extending its definition poses a problem. And with the rise of new technologies, an erosion of the state's monopoly over the use of force, combined with the proliferation of new technologies to non-state actors poses a new threat. On the other hand, wars are costly enterprises, even this new era of unpeace. As Sterling Pavelec notes, 'modern military technology is costly, founded by government resources and will require massive amounts of funding, brainpower, and a society that is willing and capable of technological evolution'.[28]

---

24 Gordon Cooke, 'Magic Bullets: The Future of Artificial Intelligence in Weapons Systems', Army.mil, June 11, 2019.

25 Cooke, 'Magic Bullets'.

26 Scott D Sagan, 'Ethics, Technology and War', *Daedalus* 145, no 4 (2016), 6–11.

27 Imre Porkoláb and Imre Négyesi, 'A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben', *Honvédségi Szemle* 147, no 5 (2019), 17.

28 Sterling M Pavelec, *War and Warfare since 1945* (Routledge, 2017), 156.

'War made the state and state made the war' is a famous saying, and technology can help or hinder both. After the Second World War, theorists talk about postmodern warfare as it became less physical; states could reach their aims below the threshold of war. Technological arms race persists today: we face uncertainty, complexity and over-reliance on technology. Alex Roland argues in his essay, that 'technology is like an "open door", as it adds what most accounts of technological innovation lack: human agency. Humans must decide if they are going to, or can, take up a given military innovation. And they must adapt it to their circumstances. Technology is a possibility, not an imperative'.[29] As the emerging and developing technologies raise new questions about ethics, morals and legality, it is important to notice that although the door is opening, we have not yet passed through it. As Feldman et al. wrote, 'context is critical: training exercises may look like war, but they are actually between allies; cold war may look like peace, but it isn't exactly. Any intelligent system (human, human/machine, or machine) must be aware of these and other complicating concerns'.[30]

Regarding the use of AI and ML in the military, in a recently published article James Johnson argues that 'the fusion of AI machine learning and human judgment to gauge an adversary's intentions (and predict escalation) for the purposes of planning and directing future wars for the pursuit of political objectives, is, therefore, a far less unlikely prospect in the near future than the use of AI to achieve tactical and operational ends (e.g. drone swarming and cyber defence)'.[31] The connection between war and technology is undeniable, but their logic differ on a fundamental level – 'technology perceives the universe as functioning rationally and predictably, while in war no success is possible which is not grounded in an ability to tolerate uncertainty, cope with it and make use of'.[32]

Conclusion

In this article I have attempted to give an overview of the main points regarding artificial intelligences' adversarial use, its place in the military and the questions regarding dual-use technology distinction. The development of new technologies raises the question of its uses, and in the case of AI, more so are questions of ethical nature. As yet it is an emerging technology, its full capabilities are hard to predict, but it is my view that erring on the side of caution would be preferable. Understanding that a technological race might unfold, a limited dissemination of information could be one of the possible solutions until we are aware of all possibilities that artificial intelligence may provide. Finally, at one point it would be advisable to have a distinction between military-level and civilian-level AI, either through capabilities, aims or by other criteria.

---

29 Alex Roland, 'War and Technology', *Foreign Policy Research Institute*, February 27, 2009.

30 Philip Feldman, Aaron Dant and Aaron Massey, 'Integrating Artificial Intelligence into Weapon Systems', Arxiv.org, May 10, 2019.

31 James Johnson, 'The AI-cyber nexus: implications for military escalation, deterrence and strategic stability', *Journal of Cyber Policy* 4, no 3 (2019).

32 Martin van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York: The Free Press, 1991), 316.

References

‘Artificial intelligence’, Merriam-Webster dictionary. Online: www.merriam-webster.com/dictionary/artificial%20intelligence

Associated Press, ‘Sony’s High-Tech Playstation2 Will Require Military Export License’. *Los Angeles Times*, 17 April 2000. Online: www.latimes.com/archives/la-xpm-2000-apr-17-fi-20482-story.html

Bostrom, Nick, ‘Information Hazards: A Typology of Potential Harms from Knowledge’. *Review of Contemporary Philosophy* 10 (2011), 44–79.

Buczak, Anna L and Erhan Guven, ‘A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection’. *IEEE Communications Surveys Tutorials* 18, no 2 (2016), 1153–1176. DOI: https://doi.org/10.1109/comst.2015.2494502

Cooke, Gordon, ‘Magic Bullets: The Future of Artificial Intelligence in Weapons Systems’. Army.mil, 11 June 2019. Online: www.army.mil/article/223026/magic_bullets_the_future_of_artificial_intelligence_in_weapons_systems

European Commission, ‘Dual-use trade controls’. Online: https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

Feldman, Philip, Aaron Dant and Aaron Massey, ‘Integrating Artificial Intelligence into Weapon Systems’, Arxiv.org, 10 May 2019. Online: https://arxiv.org/pdf/1905.03899.pdf

Flynn, Carrick, ‘Recommendations on Export Controls for Artificial Intelligence’. *Centre for Security and Emerging Technology*, February 2020. Online: https://cset.georgetown.edu/wp-content/uploads/Recommendations-on-Export-Controls-for-Artificial-Intelligence.pdf DOI: https://doi.org/10.51593/20190001

Hagendorff, Thilo, ‘Forbidden knowledge in machine learning. Reflections on the limits of research and publication’. Arxiv.org, November 2019. Online: https://arxiv.org/pdf/1911.08603.pdf DOI: https://doi.org/10.1007/s00146-020-01045-4

Johnson, James, ‘The AI-cyber nexus: implications for military escalation, deterrence and strategic stability’. *Journal of Cyber Policy* 4, no 3 (2019), 442–460. DOI: https://doi.org/10.1080/23738871.2019.1701693

Leung, Jade, Sophie-Charlotte Fischer and Allan Dafoe, ‘Export controls in the age of AI’. *War on the Rocks*, 28 August 2019. Online: https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai/

Lewis, Gregory, Piers Millett, Anders Sandberg, Andrew Snyder Beattie and Gigi Gronvall, ‘Information Hazards in Biotechnology’. *Risk Analysis* 39, no 5 (2019), 975–981. DOI: https://doi.org/10.1111/risa.13235

‘Machine learning’, Dictionary.com. Online: www.dictionary.com/browse/machine-learning

Mahfoud, Tara, Christine Aicardi, Saheli Datta and Nikolas Rose, ‘The Limits of Dual Use’. *Issues in Science and Technology* 34, no 4 (2018). Online: https://issues.org/the-limits-of-dual-use/

Martins, Nuno, José Magalhães Cruz, Tiago Cruz and Pedro Henriques Abreu, ‘Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review’. *IEEE Access* 8 (2020), 35403–35419. DOI: https://doi.org/10.1109/ACCESS.2020.2974752

Miller, Seumas, *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Springer International Publishing, 2018. DOI: https://doi.org/10.1007/978-3-319-92606-3

Pavelec, Sterling M, *War and Warfare since 1945*. Routledge, 2017. DOI. https://doi.org/10.4324/9781315175478

Pfeffer, Avi, Brian E Ruttenberg, Lee Kellogg, Michael Howard, Catherine Call, Alison M O'Connor, Glenn Takata, Scott Neal Reilly, Terry Patten, Jason Taylor, Robert Hall, Arun Lakhotia, Craig Miles, Dan Scofield and Jared Frank, 'Artificial Intelligence Based Malware Analysis'. Arxiv.org, 27 April 2017. Online: https://arxiv.org/pdf/1704.08716.pdf

Porkoláb Imre and Négyesi Imre, 'A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben'. *Honvédségi Szemle* 147, no 5 (2019), 3–20.

Price, Sean M, 'Adaptive threats and defences', in *Information Security Management Handbook*, vol. 4, ed. by Harold F Tipton and Micki Krause. Auerbach Publications, 2019, 42–65.

Roland, Alex, 'War and Technology'. *Foreign Policy Research Institute*, 27 February 2009. www.fpri.org/article/2009/02/war-and-technology/

Rotolo, Daniele, Diana Hicks and Ben R Martin, 'What Is an Emerging Technology?' Arxiv.org, 4 January 2016. Online: https://arxiv.org/abs/1503.00673

Russell, Stuart J and Peter Norvig, *Artificial Intelligence. A Modern Approach*. New Jersey: Prentice Hall, 2010.

Saad, Sherif, William Briguglio and Haytham Elmiligi, 'The Curious Case of Machine Learning in Malware Detection'. Arxiv.org, 18 May 2019. Online: https://arxiv.org/pdf/1905.07573.pdf DOI: https://doi.org/10.5220/0007470705280535

Sagan, Scott D, 'Ethics, Technology and War'. *Daedalus* 145, no 4 (2016), 6–11. DOI: https://doi.org/10.1162/daed_e_00407

Steinhardt, Jacob, Pang Wei Koh and Percy Liang, 'Certified Defenses for Data Poisoning Attacks'. Arxiv.org, 24 November 2017. Online: https://arxiv.org/abs/1706.03691

Szegedy, Christian, Vincent Vanhoucke, Sergey Ioffe, Jonathon Shlens and Zbigniew Wojna, 'Rethinking the Inception Architecture for Computer Vision', *CVPR* (2016), 2818–2826. DOI: https://doi.org/10.1109/cvpr.2016.308

Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present*. New York: The Free Press, 1991.

Venkatesh, Mothi, 'What is Human-in-the-Loop for Machine Learning?' Hackernoon.com, 17 July 2018. Online: https://hackernoon.com/what-is-human-in-the-loop-for-machine-learning-2c2152b6dfbb

AARMS Vol. 19, No. 2 (2020) 29–47.

10.32565/aarms.2020.2.3

Tasks of Voluntary Rescue Teams in Extreme Weather Situations[1]

László TEKNŐS[2]

The occurrence of weather phenomena associated with extreme precipitation, temperatures and winds are not unusual in the history of meteorology in Hungary. However, in view of the characteristics of damages, it can be ascertained that they are usually witnessed at local (settlement) level; they damage the natural and built environment, jeopardise the safety of people and their financial resources. This greatly burdens the human resources of forces designated to respond to these anomalies, also their deployments, logistics and the management system of their equipment. The current Disaster Management Act created a resolution to this tension between damage prevention, response and rescue by declaring the possibilities of involving the voluntarism of citizens in organised and regulated frameworks. It means: in order to increase the country's safety, central, territorial, later district and settlement-level voluntary rescue organisations and teams may be established. These units, considering their capabilities, are able to effectively and efficiently manage the impacts of anomalies due to the weather.

In this publication, the author attempts to present Hungary's vulnerability due to weather extremities with the help of the disaster management classification of settlements, to analyse the deployment possibilities of voluntary rescue organisations and rescue teams, taking into account their capabilities established in the framework of the national classification system.

Keywords: *disaster management, volunteering, volunteer rescue organisation, extreme weather, storm, disaster management classification of settlements, National Classification*

Introduction

Weather-related damage events are integral parts of Hungary's meteorological events. In the world, the rise of weather phenomena can be clearly presented which for example, appears

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Egyed István Postdoctoral Program.

[2] PhD, Assistant Professor of the Department of Disaster Management Operations, Institute of Disaster Management, University of Public Service; e-mail: teknos.laszlo@uni-nke.hu; ORCID: https://orcid.org/0000-0003-0759-5871

in domestic firefighting interventions.[3] The basis of this statement is the collection of data which is realised in data sheets uploaded to the Disaster Management Data Service Program.[4] The types of uploaded technical rescue operations cover natural calamities, treefalls, outdoor fires, local floods which demonstrate the effects of extreme weather events on firefighting operations.

There are plenty of standardisation methods to identify weather phenomena and to determine their parameters, such as the hazard warning system of the Hungarian Meteorological Service,[5] the national disaster risk assessment, the report on national disaster risk assessment methodology and its results. These documents reveal that the identification should be carried out related to temperature, rainfall and windstorm. For some domestic damage areas and damage sites related to extreme weather phenomena, it is typical that they influence the district level locally, increase the number of intervention forces, the wider defence-rescue capabilities, and the involvement of larger assets. The management becomes more complex (more administrative bodies, organisations, higher management levels are activated), the concerned infrastructures (vital-utility, residential) are damaged in every case. Damage-remediation activities may take from several days to several months, resulting in insurance claims, extremely high defence costs and material damage. There are possibilities for supporting intervention forces, such as rescue organisations and rescue groups which are based on the principle of volunteering.

This paper covers the disaster management aspects of domestic weather vulnerability, by its results the potential application of volunteer rescue organisations and rescue groups will be analysed.

Presentation of vulnerability caused by extreme weather phenomena by demonstrating the disaster management classification of settlements

According to point (1) of Section 21 of Chapter V of Government Decree 234/2011 (XI.10.), 'Hungary's settlements shall be classified in disaster management categories as a result of a risk assessment procedure conducted with respect to a given settlement'.[6]

Within the framework of a risk assessment procedure, according to Annex 2 of the Government Decree, hazard impacts should be considered in all cases. The disaster management classification procedure should be carried out for each settlement in the country.[7]

---

3 László Teknős, 'The Psychological Effects of Extreme Weather Conditions – The Importance of Crisis Intervention in Disaster Management', in *NISPAcee, Government vs. Governance in Central and Eastern Europe: From Pre-Weberianism to Neo-Weberianism?* ed. by Zsuzsanna Árva (Budapest: NISPAcee Press, 2014).

4 In Hungarian: Katasztrófavédelmi Adatszolgáltatási Program (KAP online). It includes the intervention statistics of the official disaster management organisation's deployment units. With the help of this, data related to storm damage can be extracted arisen from the topic of the present paper.

5 In Hungarian: Országos Meteorológiai Szolgálat (OMSZ).

6 Decree No. 234 of 2011 (XI.10.) of the Government implementing Act No. CXXVIII of 2011 concerning disaster management and amending certain related acts, point 1, Section 21.

7 László Teknős 'Kockázatelemzés a polgári védelmi területen', in *Katasztrófavédelem 2014 – Tudományos konferencia*, ed. by József Dobor (Budapest: NKE, 2014), 101–102.

After assessing the real hazard impacts typical of the valid local features, the result of the risk assessment process will be the classification of settlements into three disaster management categories. The vulnerability levels/categories of settlements are contained in Annex 1 of the Decree of the Minister of the Interior (MoI) 61/2012 (XII.11.).[8]

Table 1: *Changes in the disaster management classification of settlements between 2012 and 2017*

Extreme weather				
	County	**Class I**	**Class II**	**Class III**
1.	Baranya	–	33	249
2.	Bács-Kiskun	–	4	113
3.	Békés	–	4	72
4.	Borsod-Abaúj-Zemplén	–	43	177
5.	Csongrád	–	7	48
6.	Fejér	–	3	96
7.	Győr-Moson-Sopron	–	27	138
8.	Hajdú-Bihar	**1**	35	43
9.	Heves	–	3	75
10.	Jász-Nagykun-Szolnok	–	25	33
11.	Komárom-Esztergom	–	17	39
12.	Nógrád	**1**	20	87
13.	Pest	–	7	81
14.	Somogy	**2**	61	73
15.	Szabolcs-Szatmár-Bereg	**1**	6	179
16.	Tolna	–	4	84
17.	Vas	**1**	21	94
18.	Veszprém	–	13	200
19.	Zala	–	–	257
20.	Budapest, capital city	–	13	1
Total		**6 settlements**	**346 settlements**	**2,139 settlements**
Grand Total		**2,491 settlements**		
Population affected		**National: 6,047,872 persons Budapest: 1,088,619 persons**		

Source: László Teknős, 2017, based on NDGDM[9] data.

The 2016 data shown in Table 1 are the result of a risk assessment procedure. One of the elements of this process is the categorisation of the settlements themselves. The table shows that the number of settlements affected and threatened by extreme weather is 2,491, which is 74 per cent of all the settlements (3,177). The indicators of the weather extremities can be defined by the values found in the Hazard Warning System of the National Meteorological Service.

[8] Decree No. 61 of 2012 (XII.11.) on the disaster protection classification of settlements and on the amendment of certain rules of disaster protection of Decree No. 62 of 2011 (XII.29.) of the Ministry of the Interior.

[9] National Directorate General for Disaster Management, Ministry of the Interior. In Hungarian: Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF).

Table 2: Classification categories of settlements affected by hazard impacts of meteorological origin in Hungary in 2016

Hazard impact	Number of classified settlements total	Number of vulnerable population (persons)	Number of Class I settlements	Number of Class II settlements	Number of Class III settlements
			Persons affected	Persons affected	Persons affected
Extreme weather	2,491	6,043,798	6	346	2,139
			145,720	2,620,740	3,277,338
Extreme winter weather	1,034	4,287,496	14	236	784
			325,055	564,053	1,512,756
In 2016, there were 3,177 settlements in Hungary in total			179	1,325	1,673

Source: László Teknős, 2017, based on NDGDM data.

In Table 2, one can see the classification categories of settlements affected by hazard impacts of meteorological origin related to the number of the population. Extreme weather can be found in point a) of Annex 2 of Government Decree 234/2011 (XI.10.), under natural disasters and hazards of natural origin. It can be ascertained that out of the 3,177 settlements in Hungary, 2,491 settlements may be affected by hazard impacts of extreme weather origin. In the most vulnerable category (I), 6 settlements were classified; in Class II, 346 settlements and in Class III, 2,139 settlements, affecting altogether more than six million people. As far as winter weather vulnerability is concerned, one may ascertain that it is characterised by high risk despite the fact that due to the increase of mean temperatures in Hungary, the number of days with temperatures under freezing point is decreasing.

It can (also) be ascertained based on this that the weather phenomena incurring hazards should be addressed, and the disaster management-approach analysis should be continued.

Table 3: Changes in the number of natural disasters, storm-triggered incidents, fallen trees, water-triggered incidents between 2011 and 30 Sep 2017

Number of technical rescue deployments – on national level (based on closed TMMJ datasheets)					
	Incidents requiring response total	Natural disasters, storm-triggered incidents	Fallen trees (incidents)	Water-triggered incidents	TOTAL (incidents)
2011	27,344	2,188	5,910	3,033	11,131
2012	20,200	2,116	4,440	883	7,439
2013	23,985	2,143	4,241	2,086	8,470
2014	25,582	3,155	6,441	2,276	11,872
2015	24,846	3,674	5,292	951	9,917
2016	25,015	3,706	5,297	1,538	10,541
30 Sep 2017	25,414	5,726	7,409	1,661	14,796

Source: László Teknős, 2017, based on KAP online data.

Table 3 shows the total number of events related to technical rescue operations which required intervention from 2011. An increase can be noticed in case of natural calamities, storms and treefalls. It can be seen that natural calamities and storms rise compared to the data of 2011, an increase is showed illustrated in a linear trend. According to statistics, a higher number of intervention cases has to be calculated which predicts the fact that at a time of extreme intervention, the professional forces become more loaded. Based on KAP-online data, it is expedient to call up volunteers[10] who are qualified in disaster management in order to apply them for managing this type of events.

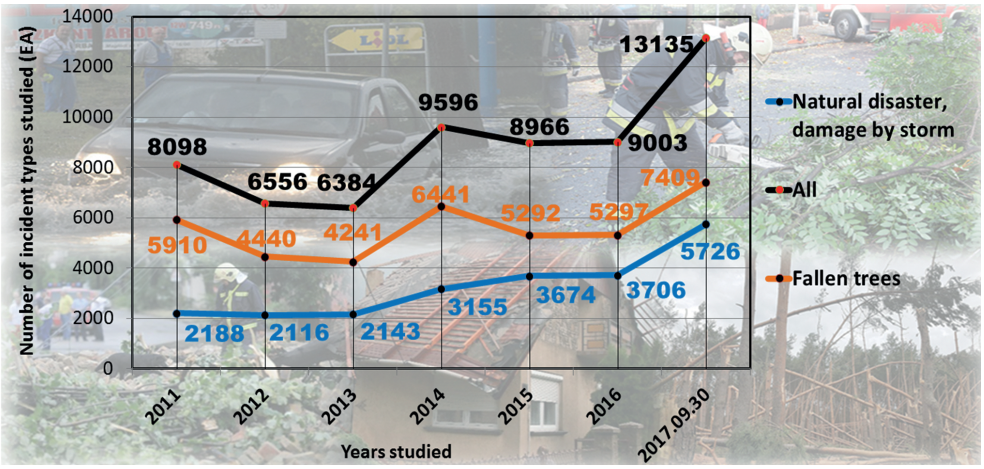


Figure 1: The occurrence of natural disasters, storm-triggered and fallen trees incidents within the technical rescue category between 2011 and 30 Sep 2017

Source: László Teknős, 2017, based on KAP online data.

Figure 1 is a complementary piece of information to Table 3. Within natural disasters, an increase may be observed with storm-triggered and fallen trees incidents. In case of storms, from 2013, it is even more significant. The content of the above figure also evidences that the trend in Hungary follows the increasing world-wide tendency of meteorological phenomena.

Regulation of the deployment of voluntary rescue teams – The national classification system

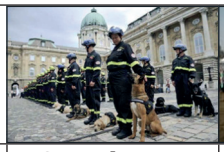
Under item (2) of Article G) of the Fundamental Law, one can read: 'Hungary protects its citizens.' To this end, it defines the rights and obligations. An obligation is, for instance, based on paragraph (1) of Article XXXI of the Fundamental Law, that: 'Every Hungarian citizen shall protect/defend the fatherland.'[11] Its content affecting the protection against disasters can be found in paragraph (2) of Section 1 of Act CXXVIII of 2011 (hereinafter

[10] Volunteer firefighting associations, rescue organisations, rescue groups.
[11] 'The Fundamental Law of Hungary', 25 April 2011.

referred to as Kat. tv.), according to which: 'Every Hungarian citizen has the right and the obligation to participate in disaster management.'[12] A citizen may comply with the above through voluntary social activities, since, based on paragraph (2) of Article VIII of the Fundamental Law: 'Everyone is entitled to establish organizations and join organizations.' It is stressed by the stipulation in Act CLXXV of 2011, since the Hungarian National Assembly acknowledges that the voluntary collaboration of people is inevitable for the development of Hungary. Paragraph (1) of Section 18 of Act CXXVIII of 2011 on disaster management and on the amendment of certain relevant acts states that persons providing voluntary assistance, the voluntarily participating social and charitable organisations may perform tasks related to disaster management.

The above-mentioned legislation, without being exhaustive, creates a voluntary institutional system of the protection against disasters.

Table 4: Division of voluntary rescue teams and organisations

				
Level	**Central rescue team**	**Regional rescue team**	**District rescue team**	**Settlement-level rescue team**
Examples	HUNOR Rescue Team	Budapest Voluntary Rescue Team[13]	South Békés Rescue Team[14]	Csepreg Voluntary Settlement-level Rescue Team[15]
Number of organisations	6	20	178	1,099
Personnel (persons)	1,000	1,900	5,800	11,400

Source: László Teknős, 2017, based on NDGDM data.

In Table 4, one can see the division of voluntary rescue teams and organisations, demonstrating the different levels by some examples.

The total number reaches 20,200, which shows that voluntary rescue organisations and teams in Hungary constitute realistic potentials, increase the self-defence capabilities of settlements. It can also be stated that the level-by-level divisions are aligned with the levels of protection management, supporting the activities of organisations and entities established to implement the protection/defence functions of the state. The state supports the establishment of these forces by which it fulfils the state obligations set forth in the Fundamental Law. Some of the pictures in the table show that volunteers are wearing uniforms, they are disciplined, and they make an image of a strong, cohesive country representing a strong power. It can be stated that they are able to support the intervention

[12] Teknős László and Gotthilf Schweickhardt, 'The role of the voluntary disaster management service in the education of the National University of Public Service', *Bolyai Szemle*, no 2 (2015), 106–114.
[13] 'Megkapta a nemzeti minősítést a Budapest Önkéntes Mentőszervezet', November 8, 2015.
[14] '… a helyes cselekedet jutalma maga a tett…', October 16, 2013.
[15] 'Önkéntes Települési Mentőcsoport alakult Csepregen', May 25, 2016.

units of professional disaster management forces, their potential application should be kept in mind.

Professional disaster management bodies, in addition to the professional management of voluntary rescue organisations, are involved in the protection against the impacts of disasters and damage remediation. If the use of special skills and specialised equipment is required, the involvement of voluntary rescue organisations in response activities is ordered by the head of the territorial body of the professional disaster management body (director of the County Disaster Management Directorate).

Chapter VIII of Government Decree 234/2011 (XI.10.) issued on the implementation of Act CXXVIII of 2011 on disaster management and on the amendment of certain relevant acts stipulates the rules of participation of voluntary rescue organisations, in which it defines in detail:

- general principles
- requirements on the personnel
- technical requirements
- rules of registration and deletion
- rules of classification and its renewal
- special rules of participation in international relief

According to item (1) of Section 57 of Government Decree 234/2011 (XI.10.), a voluntary rescue organisation operating in Hungary may participate in the protection against the impacts of disasters and emergencies in Hungary once it has obtained a classification determined by the National Classification System, meeting the basic skills and preparedness requirements, conducted by the regional entity of the professional disaster management organisation.[16] The classification procedure of voluntary rescue teams shall be conducted according to the National Classification System, based on the Act on Disaster Management and the provisions of Government Decree 234/2011 (XI.10.) issued on its implementation.

Procedures of the National Classification Exercises

The National Classification System is a classification, to be renewed every 5 years, elaborated by the central body of the professional disaster management organisation, based on the fulfilment of professional criteria.[17] The National Classification System is a system established and adjusted to the Guidelines and Methodology, consisting partly of theoretical education, partly of practical training, defined by the United Nations International Search and Rescue Advisory Group, and provides classification.[18]

The newly formed voluntary rescue organisation conducts a system integration exercise, and the organisation wishing to obtain reclassification conducts a trial classification exercise before the classification exercise. A system integration exercise is a joint field exercise carried out for the first time, involving the units of a newly formed rescue organisation,

[16] 'Nemzeti minősítési rendszer'.
[17] NDGDM Instructions 6/2013 (X.31.) stipulates the requirements of the National Classification System.
[18] Kristóf J Plébán, 'A települési önkéntes mentőcsoportok védekezésének feltételrendszere', *Hadtudomány* 26, no 1–2 (2016), 75–85.

where the units practice cooperation. A trial classification exercise is a command post and field exercise simulating a real situation, assisting in preparing the team for the National Classification Exercise, elaborated in accordance with the Organisational and Operational Guidelines issued for the rescue branch(es).

The National Civil Protection Inspector General organises the trial classification, system integration and national classification exercises in semi-annual cycles. A regional body (county directorate) prepares a conduct plan for the exercises, which will be submitted to the National Civil Protection Inspector General for approval 30 days prior to the exercise date by the head of the Department Emergency Management of the NDGDM.

The classification exercise should be prepared striving for conditions close to real life, to be performed in 36 hours continuously, without interruption. On the daily results of the classification exercise, the head of the Emergency Management Department of the NDGDM informs the Central Duty Office of the NDGDM by 18:00 hours in a digital way (electronic mail). The results are submitted by the Central Duty Office of the NDGDM in its Daily Report. The classified rescue organisations conduct annual exercises and regularly provide for the readiness level of the theoretical knowledge of their personnel and conduct refresher training courses.[19]

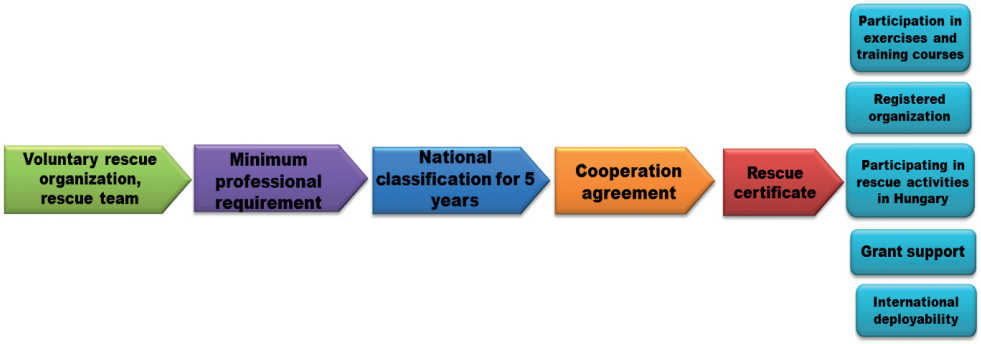


Figure 2: The sequence and elements of the Hungarian National Classification System

Source: László Teknős, 2017.

Voluntary regional civil protection organisations, after they are established, need to follow their Organisational and Operational Guidelines, considering both their structure and operation. For the first time, a voluntary organisation must submit an introductory background material, a so-called portfolio. With the help of this background material and the system integration field exercise, it must demonstrate its compliance with the Organisational and Operational Guidelines. The acquired skills and knowledge must be maintained by training, preparation and demonstration exercises held annually.

A rescue organisation, having acquired its certification, receives a rescue team certificate (rescue certificate/ID card), by which it is entitled to participate in rescue operations, to enter the confined incident site, and, at the same time, this certificate is also to prove that the organisation has appropriate equipment. A rescue organisation or team that qualifies for

[19] NDGDM Instructions 6/2013 (X.31.) stipulates the requirements of the National Classification System.

this certification, signs an agreement, thereby accepting the coordination and management rights of the central body of the professional disaster management organisation (NDGDM), thereby it is registered. This registry is kept by the regional body (county directorate) of the professional disaster management organisation.[20]

Criteria of acquiring the National Classification:

- introductory professional background material (portfolio)
- system integration exercise plan

Introductory professional background material (portfolio)

The necessary documents must be submitted in writing and in an electronic form to the National Civil Protection Inspector General by the head of the regional body. In the National Classification System, a voluntary rescue organisation that wishes to obtain national classification must comply with Sections 60 and 61 of Government Decree 234/2011 (XI.10.), related to the personnel and regulating the technical requirements, issued on the implementation of Act CXXVIII of 2011 on disaster management and on the amendment of certain relevant acts.[21]

Content and structure of the portfolio:

Chapters:

1. Brief presentation of the organisation (name, seat, function, date of establishment)
2. List of deployments (based on units)
3. Structure of the team (organisational chart and team composition, in a table)
4. Operation and presentation of units
5. Criteria for selecting team members
6. Mobilisation of the team, logistics and info-communication support
7. System of training, exercises, preparation
8. System of registry of equipment, its repair and maintenance
9. Method of health and medical care

Annexes:

1. Recommendation of the NDGDM regional organisation
2. Team operations procedure and functioning
3. Qualification documents
4. Team name list by assignment
5. List of equipment (cargoed and complete)
6. Certificates of life and accident insurance
7. Health care support (health records of the members, dog vaccination book)
8. Photos (with low resolution)

[20] 'Önkéntes mentőszervezetek'.
[21] 'Nemzeti minősítési rendszer'.

System Integration Exercise Plan

The rescue organisation prepares and submits an exercise plan for the National Classification Exercise 30 days prior to the exercise via the head of the regional body for approval to the National Civil Protection Inspector General.

Based on the exercise plan approved by the National Civil Protection Inspector General, the rescue team or organisation gives evidence to the National Classification Committee, by carrying out a field exercise, in compliance with the Organisational and Operational Guidelines. It implements the exercise according to the Organisational and Operational Guidelines chosen by it. The document certifying the acquisition of the certificate is certified by the signature of the head of the rescue organisation, the director of the regional body and the head of the classification committee appointed by the Deputy Director General of the NDGDM. The voluntary rescue team or organisation, having acquired the National Classification, may renew its certificate every 5 years, by repeating the classification exercise.[22]

Volunteers need to undergo a system integration exercise. This is a 36-hour field exercise to find out whether they have the skills meeting the basic professional requirements and whether they can meet the Organisational and Operational Guidelines. They have to continuously maintain their capabilities afterwards. Continuous training, preparation and demonstration exercises are suitable for this purpose. Another basic expectation of a voluntary rescue team is the appropriate level of readiness of the organisation, as rapid deployability is a key issue in their activity.

The classification exercise is mandatory to be repeated every five years. Participation in this classification procedure and a successful examination are necessary conditions in order that the rescue organisation may be involved and participate in rescue activities, furthermore, that the rescue team is included in the logistics system of the professional disaster management body. By way of participating in tenders and other non-cash benefits, its operation should be ensured. The operational strategy of voluntary rescue organisations, that is, the one related to the personnel, should be formulated as per Section 60 of the Government Decree, and as far as technical requirements, as per Section 61.[23]

NDGDM Instruction 6/2013 (X.31.) on the criteria of the National Classification System contains the minimum professional requirements. Although the document is only a recommendation, the central disaster management body intends and requires that only organisations be involved in rescue operations and damage liquidation that meet the minimum professional requirements, based on which they had been classified. These requirements have been elaborated based on the Guidelines of UN INSARAG,[24] thus ensuring that Hungarian voluntary rescue organisations may join the international search and rescue system. The structure, the management, the rescue and the logistics component type of division of Hungarian rescue organisations, as well as the classification of urban

[22] ‘Önkéntes mentőszervezetek’.
[23] Ibid.
[24] INSARAG: International Search and Rescue Advisory Group, INSARAG. In Hungarian: Nemzetközi Kutató-mentő Tanácsadó Csoport.

search and rescue activities by heavy, medium and light categories also contributes to international unity.[25]

The compliance with these criteria ensures professional response capabilities. Given the capabilities of voluntary rescue organisations, they are deployable to natural or other disasters, such as canine search, ruin and area search, tracking, scuba-diver and water search and flood search and rescue. They can be used for technical, high- and low-angle rescue, aerial reconnaissance, medical rescue and first aid, complex rescue operations, etc. According to local, real vulnerabilities (see settlement classification), rescue organisations and teams are established. The National Classification System defines the Organisational and Operational Guidelines, taking into account the disaster management categorisation of settlements, for seven specialised branches. It could also be stated that these areas cover the Hungarian capabilities such as water and flood rescue, canine search, scuba-diving and rope rescue, command and control, basic water damage prevention, and urban search and rescue activities.

The main classification type of settlement-level voluntary rescue teams is focused on basic water damage prevention activities; however, the capabilities include flood and water rescue, storm damage mitigation, firefighting, technical rescue, damage liquidation, urban search and rescue, person research, rope (Alpine) technology, population protection activities, command and control, logistics.

As a summary, in case of incidents, in disasters and emergencies, only voluntary rescue organisations and teams are eligible for deployment that have acquired certificates within the framework of the National Classification System, or only such teams may be deployed to the incident sites. Rescue organisations participate, with the professional management of disaster management organisations, in protection activities and response activities against the impacts of disasters. The instruction right is exercised by a member being commissioned by a professional disaster management body. This person is in charge of the entire personnel of the rescue organisation, assigned by the Disaster Management Director with respect to the regional and settlement-level civil protection organisation, or with respect to the central civil protection organisation, by the Director General of the NDGDM. Rescue organisations perform their duties based on agreements with the professional disaster management bodies.

[25] Mónika Nováky, 'Önkéntes mentőszervezetek alkalmazásának lehetőségei', in *Modernkori veszélyek rendészeti aspektusai*, ed. by Gaál Gyula and Hautzinger Zoltán (Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 2015), 325–331.

Deployment possibilities of voluntary rescue organisations and teams

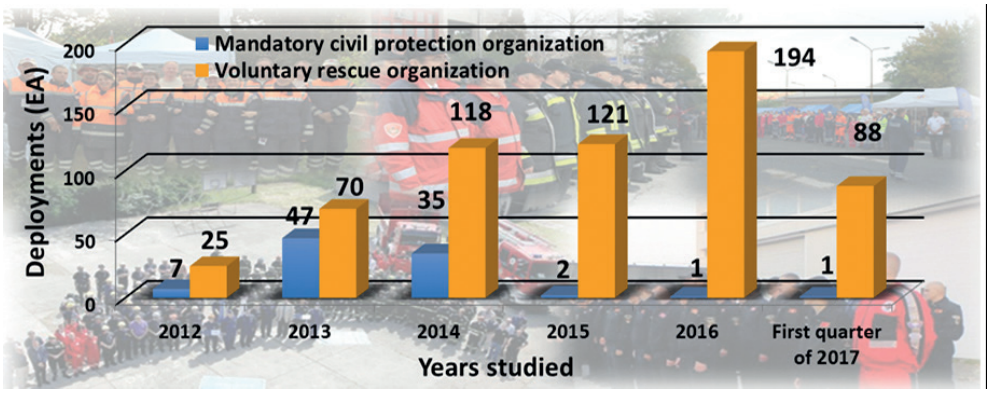


Figure 5: Deployments of mandatory civil protection organisations and voluntary rescue teams between 2012 and Q1 of 2017

Source: László Teknős, 2017, based on the data provided by the National Civil Protection Inspectorate General.

Volunteering is not just a European demand, but it is the best chance for a citizen to take part in the joint efforts against impacts endangering their lives, environment and valuables, according to their self-motivation.[26]

Between 2012–2017, voluntary rescue organisations and teams were deployed in incidents, such as life-saving, rescuing injured persons, search and rescue of missing persons from water and underwater, extracting persons from wells, saving and extracting animals, firefighting, technical rescue, storm damage mitigation, removal of hazardous trees, foiling roofs, patient transport, lifting of sunken small boats to water surface, rescue of cars in snowdrifts, rescuing crashed motor gliders, flood and inland water protection, protecting residential areas, water removal, removal of accumulated rainwater, water pumping, ditch clearing, clearing of the lock system of fishing ponds, drinking water distribution, providing alternative heating and power supply, etc.

[26] 'Mentőcsoportok – Önkéntes mentőszervezetek az állampolgárok védelme érdekében'.

Examples of deployments of voluntary rescue organisations and teams

Storm on 08 July 2014

Table 5: Disaster management operations on 08 and 09 July 2014 on a national level

Incident time and type	Consequence	Deployment of voluntary rescue teams
Management of the incident originating from the storm of 08–09 July 2014 and the elimination of its consequences	• affected counties: Békés, Csongrád, Hajdú • damage to residential buildings and outbuildings • trees fallen on residential buildings, broken electrical wires • lightning struck in a sheep barn and Police Hq building • multiplication of the number of disaster management forces (response personnel, operations control duty officers)	Békés County: in the settlement of Végegyháza, the South Békés District Rescue team with 24 persons, 4 sets of equipment to eliminate storm damages.
		Gyula District Rescue team with 6 persons in Gyula to eliminate storm damages.

Total	Fire	Technical rescue	Incidents due to weather extremities	Breakdown in percentages compared to all incidents
478	82	346	274	57
224	15	171	115	51

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

Sleet on 01 December 2014

Table 6: Disaster management operations between 01 and 04 December 2014 on a national level

Incident time and type	Consequence		Deployment of voluntary rescue teams
Management of incidents related to crushed grain formation and sleet, elimination of consequences 01–04 December 2014	• affected counties: Borsod-Abaúj-Zemplén, Budapest, Heves, Komárom-Esztergom, Nógrád, Pest • roadblocks • disruption of power supply • loss of mobile phone repeater station • halt of a passenger train at a railway station • multiplication of the number of disaster management forces (response personnel, operations control duty officers) • operation of a local operations staff		Pest County: The Pilis Rescue Team participated in the removal of fallen trees between Pilisszentkereszt and Dobogókő with 8 persons and 2 sets of equipment.
			Pest County: Gyál, Vác District Rescue Teams with 5 persons and 1 set of equipment each participated in the removal of fallen trees.
			Nógrád County: The Paló́c Rescue Team participated with 5 persons, 3 sets of equipment rescuing persons trapped in the Drégely Castle Resort; and with 3 persons and 1 set of equipment rescuing a vehicle skidded in a ditch in Mihálygerge.
			Nógrád County: Mátra Rescue Team with 10 persons participated in the removal of fallen trees in the Mátra Mountains and other damage liquidation tasks.
			Nógrád County: The mandatory civil protection organisation of Mátraszentimre settlement with 20 persons participated in the removal of fallen trees in Galyatető and Mátraszentimre.
Disaster management operations	01 Dec	335 equipment, 1,317 persons, 608 operations	
	02 Dec	260 equipment, 962 persons, 400 operations	
	03 Dec	487 persons, 131 equipment, 256 operations	
	04 Dec	173 persons, 39 equipment, 122 operations	

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

Extreme rainfall on 17 August 2015

Table 7: Disaster management operations between 17 and 20 August 2015 on a national level

Incident time and type	Consequence	Deployment of voluntary rescue teams
Management of incidents originating in downpours and gales, elimination of their consequences on 17 and 18 August 2015	• affected counties: Bács-Kiskun, Budapest, Nógrád Pest, Somogy, Szabolcs-Szatmár-Bereg, Veszprém • roadblocks • disruption of power supply • damages to residential buildings, outbuildings, rainwater inundating residential buildings • flash flood on a creek (Majs) • rescuing 31 persons, accommodating 110 persons • multiplication of the number of disaster management forces (response personnel, operations control duty officers) • operation of a local operations staff	Veszprém County: Tapolca settlement Civil Protection Organisation, with 6 persons, participated in sandbag protection in Tapolca. Pest County: Szigetszentmiklós District Rescue team, with 4 persons in Szigethalom, water pumping activity. Budapest: On 18 August, the Budapest Rescue Organisation with 40 persons, 28 sets of equipment in Budapest, water pumping activity. Baranya County: Majs Creek flash flooded Majs settlement in Mohács District, threatening 11 residential buildings, water inundated a house, 20 voluntary persons placed 200 sandbags.

Date	Total	Fire	Technical rescue	Incidents due to weather extremities	Breakdown in percentages compared to all incidents	Breakdown in percentages compared to technical rescue incidents
17 Aug	636	144	420	187 (storm)	29	44
18 Aug	427	52	326	238 (storm)	55	73

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

Storm at Lake Balaton between 10 and 14 July 2017

Table 8: Disaster management operations between 10 and 14 July 2017 on a national level

Incident time and type	Consequence	Deployment of voluntary rescue teams
Management of incidents with large amounts of precipitation and hurricane, eliminating their consequences between 10 and 14 July 2017	• affected county: Somogy • several inaccessible road stretches, road blocks • disruption of power supply • large number of fallen and cracked trees, breaking of electrical wires, fallen pylons • entire roofing of residential buildings removed by the gale • multiplication of the number of disaster management forces (response personnel, operations control duty officers) • operation of a local operations staff	Somogy County: Sió Rescue Team, between 11 and 14 July, 8 persons, 1 set of equipment, logistics tasks

Incident time and type	Consequence		Deployment of voluntary rescue teams
Disaster management operations	10 July	66 firefighting deployments, in damage liquidation: 24 firefighters of 3 professional fire brigades, 2 persons from CRT, 17 voluntary firefighters and 3 onsite commanders	
	11 July	44 firefighters of 9 professional fire brigades, 60 voluntary firefighters, 4 onsite commanders	
	12 July	49 firefighters of 10 professional fire brigades, 23 voluntary firefighters, 3 onsite commanders. From 13 July, damage liquidation (besides new calls) was only necessary in Siófok	
	13 July	33 firefighters of 6 professional fire brigades, 14 voluntary firefighters, 3 onsite commanders	
	14 July	28 firefighters of 6 professional fire brigades, 17 voluntary firefighters, 2 onsite commanders	

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

Storm in Orosháza, 06 August 2017

Table 9: Disaster management operations between 06 and 08 August 2017 on a national level

Incident time and type	Consequence	Deployment of voluntary rescue teams
Management of the incident originating from the storm of 06–08 August 2017 and the elimination of its consequences	• affected counties: Bács-Kiskun, Békés, Hajdú-Bihar • several inaccessible road stretches, road blocks • disruption of power supply at 4,645 consumers • large number of fallen and cracked trees, breaking of electrical wires, fallen pylons • entire roofing of residential buildings removed by the gale • multiplication of the number of disaster management forces (response personnel, operations control duty officers) • operation of a local operations staff	Békés County: Orosháza and Mezőkovácsháza District Rescue Teams with 8 persons and 3 sets of equipment, liquidating the storm damages in Orosháza Békés County: Körös Rescue Team with 2 persons and 1 set of equipment, carried out air reconnaissance in Orosháza settlement as damage liquidation task Békés County District Rescue Team with 3 persons and 3 sets of equipment liquidating the Orosháza storm damages

Date	Total	Fire	Technical rescue	Incidents due to weather extremities	Breakdown in percentages compared to all incidents	Breakdown in percentages compared to technical rescue incidents
06 Aug	636	144	420	187 (storm)	29	44
07 Aug	427	52	326	238 (storm)	55	73
08 Aug	215	46	113	60 (storm)	28	53

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

In the early afternoon of 06 August 2017, in addition to the stormy wind gusts, a heavy thunderstorm arrived in our county sleet, which resulted in nearly two hundred emergency calls coming from Orosháza till 21:00 hours. The professional firefighters removed the fallen trees, broken logs and restored the damages caused by the storm to roof structures of real

estates. In the downtown of Orosháza, power supply was intermittent or disrupted. Major damages occurred to the roof structure of the Chronic Department of the local hospital. Firefighting units of disaster management were supported by the South Békés Rescue Team and the Körös Rescue Team, as well as by the voluntary Firefighting Association of Nagyszénás.[27]

On 07 August 2017, the work of the local professional firefighters was supported by the Békéscsaba, Szarvas, Szentes and Hódmezővásárhely professional units, the Sarkad, the Tótkomlós, the Gyomaendrőd, the Füzesgyarmat and the Mezőberény voluntary firefighters associations and the members of the Sárrét Rescue Team and the drone unit of the Körös Rescue Team.[28]

Table 10: Disaster management operations between 29 and 31 October 2017 on a national level

Incident time and type	Consequence	Deployment of voluntary rescue teams
Management of incidents originating in downpours and gales, elimination of their consequences between 29 and 31 October 2017	• rainwater inundating residential buildings • flash flood on a creek (Majs) • rescuing 31 persons, accommodating 110 persons • affected counties: Bács-Kiskun, Baranya, Budapest, Csongrád, Fejér, Győr-Moson-Sopron, Komárom-Esztergom, Nógrád Pest, Somogy, Szabolcs-Szatmár-Bereg, Veszprém • roadblocks, railway traffic outage due to fallen trees • disruption of power supply at 71,742 consumers, delegation of some members into the Havaria Team of DÉMÁSZ • at several fire brigades, IP telephony and internet service outage due to power supply disruption • damages to residential buildings, outbuildings • multiplication of the number of disaster management forces (response personnel, operations control duty officers) • operation of a local and onsite operations staff	Budapest: Budapest Rescue Organisation with 77 persons and 23 sets of equipment, liquidating wind storm damages Komárom-Esztergom County: Környe, Oroszlány and Tatabánya settlement-level rescue teams with 16 persons and 6 sets of equipment, liquidating wind storm damages Bács-Kiskun County: Petőfi Rescue Team, Baja District, Kecskemét District, Kiskunfélegyháza District and Harta settlement-level rescue teams with 10 persons and 5 sets of equipment, liquidating wind storm damages Bács-Kiskun County: Kunszentmiklós and Kiskőrös District Rescue Teams in Kiskőrös, Kunszentmiklós, Lakitelek, Tass and Tiszaalpár settlements with 12 persons and 7 sets of equipment, liquidating wind storm damages

Date	Total	Fire	Technical rescue	Incidents due to weather extremities	Breakdown in percentages compared to all incidents	Breakdown in percentages compared to technical rescue incidents
29 Oct	2,625	48	2,485	1,679 (gusts)	63	67
30 Oct	1,088	33	961	731 (gusts)	67	76
31 Oct	309	31	217	132 (gusts)	42	60

Source: László Teknős, 2017, based on the Daily Report of the NDGDM Central Duty Office.

Storms between 29 and 31 October 2017

[27] 'Jégesővel csapott le a vihar Orosházára', August 6, 2017.
[28] 'Még mindig dolgoznak az orosházi tűzoltók', August 7, 2017.

On 29 October 2017, a very strong cold front drifted over Central Europe and the Balkan Peninsula. The cold front rushed down through Hungary in just three hours, and the gusts over 100–110 km/h, throughout the country, caused falling trees breaking electric wires and train delays. The wind was measured the strongest at Lake Balaton, in Siófok, a gust of 131 km/h. The unusual time of the storm and the circumstances of its occurrence well fit into to the extreme weather, often rich in storms, of 2017.[29]

The meteorological phenomena listed above well illustrate the response operations, increasing in such times, mainly numerical peaks related to technical rescue operations. It can be seen that voluntary firefighters, voluntary rescue organisations and rescue teams contributed to the liquidation of mass incidents. Based on the data of the above tables and their related content, it can be stated that, for example, in case of weather incidents, it is necessary to use the voluntary units as an additional potential force. Considering both their numbers and their equipment, they are suitable for participating in interventions lasting several days, to ensure the safety of settlements, and to protect the local population from a disaster management aspect. Provably, they contribute to the effectiveness of local, district and regional protection.

In order to maintain this high level of professionalism, inter alia, it is necessary to develop, elaborate and upgrade the intervention modules, capabilities, capacities and the procurement of the necessary up-to-date equipment facilitating specialised activities.

Conclusion, recommendation

According to paragraph 21 of Chapter V of the Hungarian Government Decree no. 234/2011 (XI.10.), for example as a result of municipalities' disaster classification, the term *extreme weather hazard* was defined. According to Table 1, 2 and Annex 1 of the Government Decree, it can be stated that municipalities in Hungary are affected by extreme meteorological events, and most of the population is at risk. It can be identified that endangering weather phenomena need to be addressed, and the analysis from disaster management perspective should be continued.

Furthermore, Table 3 shows that among the types of investigated technical rescue operations – in terms of the total number of events requiring intervention – a rise can be observed in cases of natural calamities, storms and treefalls. Referring to weather-related vulnerability, it can be stated that the increase of potentiality of predetermined forces could be necessary, and the risks with rising tendency require a greater degree of responsiveness.

This is illustrated in Figure 4, which presents the so far established rescue organisations, rescue groups based on volunteering. In Table 4 it can be observed that domestic voluntary rescue organisations and rescue groups provide realistic potentialities and increase the self-defence capabilities of municipalities. It has also been carried out that the levels of defence management are aligned with their segments, supporting the activities of organisations established for accomplishing defence functions of the state. Some of the pictures in the table show that volunteers are wearing uniforms, are disciplined, and they make an image

[29] Ákos Horváth, 'A 2017. október 29-i vihar meteorológiai elemzése', October 31, 2017.

of a strong, cohesive country representing a strong power. It can be stated that they are able to support the intervention units of professional disaster management forces, their potential application should be kept in mind. Why? Because volunteers must meet the high standards of stringent intervention minimum requirements drawn up in NDGDM instruction no. 6/2013 (X.31.) about the basic requirements of the National Qualification System, in order to get involved in domestic or international incidents, accidents, emergencies and disasters. The National Qualification System declares professional competence and the possibility of the domestic voluntary rescue organisations for joining the international search and rescue system. Based on intervention activities of events related to weather phenomena presented in this paper, it can be said that the co-operation with partners and co-operative organisations, furthermore, the disciplined and professional task execution of the intervening staff played an important role during the elimination of damages. Damage elimination and eradication activities were effective and took place continuously despite the numerous cases of mass incidents. The co-operation and the vocation of volunteer firefighters and rescue units were key factors to success and efficiency.

References

'… a helyes cselekedet jutalma maga a tett…', 16 October 2013. Online: www.delbekesmcs.hu/261/

Horváth Ákos, 'A 2017. október 29-i vihar meteorológiai elemzése', 31 October 2017. Online: www.met.hu/ismeret-tar/erdekessegek_tanulmanyok/index.php?id=2044&hir=A_2017._oktober_29-i_vihar_meteorologiai_elemzese

'Jégesővel csapott le a vihar Orosházára', 6 August 2017. Online: http://bekes.katasztrofavedelem.hu/hirek/3344-jegesovel-csapott-le-a-vihar-oroshazara

'The Fundamental Law of Hungary', 25 April 2011. Online: https://2010-2014.kormany.hu/download/a/1c/11000/The%20New%20Fundamental%20Law%20of%20Hungary.pdf

'Megkapta a nemzeti minősítést a Budapest Önkéntes Mentőszervezet', 8 November 2015. Online: www.kormanyhivatal.hu/hu/budapest/hirek/budapest-onkentes-mentoszervezet

'Még mindig dolgoznak az orosházi tűzoltók', 7 August 2017. Online: http://bekes.katasztrofavedelem.hu/hirek/3346-meg-mindig-dolgoznak-az-oroshazi-tuzoltok

'Mentőcsoportok – Önkéntes mentőszervezetek az állampolgárok védelme érdekében'. Online: www.katasztrofavedelem.hu/index2.php?pageid=polgarivedelem_mentesszervezes_beavatkozo

'Nemzeti minősítési rendszer'. Online: www.katasztrofavedelem.hu/index2.php?pageid=polgarivedelem_minositesek

NDGDM Instruction 6/2013 (X.31.) stipulates the requirements of the National Classification System.

Nováky Mónika, 'Önkéntes mentőszervezetek alkalmazásának lehetőségei', in *Modernkori veszélyek rendészeti aspektusai*, ed. by Gaál Gyula and Hautzinger Zoltán. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 2015, 325–331.

'Önkéntes mentőszervezetek'. Online: www.szentflorian.hu/?pageid=katved_onkentes&menuid=katved

'Önkéntes Települési Mentőcsoport alakult Csepregen', 25 May 2016. Online: www.repcevidek.hu/kozelet/onkentes-telepulesi-mentocsoport-alakult-csepregen.html

Plébán J Kristóf, 'A települési önkéntes mentőcsoportok védekezésének feltételrendszere', *Hadtudomány* 26, no 1–2 (2016), 75–85. DOI: https://doi.org/10.17047/HADTUD.2016.26.1-2.75

Teknős László, 'Kockázatelemzés a polgári védelmi területen', in *Katasztrófavédelem 2014 – Tudományos konferencia*, ed. by József Dobor, Budapest: NKE, 2014, 101–102.

Teknős, László, 'The Psychological Effects of Extreme Weather Conditions – The Importance of Crisis Intervention in Disaster Management', in *NISPAcee, Government vs. Governance in Central and Eastern Europe: From Pre-Weberianism to Neo-Weberianism?* ed. by Zsuzsanna Árva. Budapest: NISPAcee Press, 2014.

Teknős László and Gotthilf Schweickhardt, 'The role of the voluntary disaster management service in the education of the National University of Public Service'. *Bolyai Szemle*, no 2 (2015), 106–114.

Decree No. 234 of 2011 (XI.10.) of the Government implementing Act No. CXXVIII of 2011 concerning disaster management and amending certain related acts, point 1, Section 21. Online: www.informea.org/en/legislation/decree-no-234-2011-xi-10-government-implementing-act-no-cxxviii-2011-concerning-disaster

Decree No. 61 of 2012 (XII.11.) on the disaster protection classification of settlements and on the amendment of certain rules of disaster protection of Decree No. 62 of 2011 (XII.29.) of the Ministry of the Interior. Online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200061.BM&timeshift=fffffff4&txtreferer=00000001.TXT

AARMS Vol. 19, No. 2 (2020) 49–63.

10.32565/aarms.2020.2.4

The Place of the Sahel Region in the Theory of Regional Security Complex

Márton VARGA[1]

The theory of regional security complex is one of the main theories of the regional approach of the international security system. The international organisations, the different strategies and concepts use many different definitions for the Sahel region. However, the ongoing changes of the global and the regional security and the complexity of the crisis of the Sahel region bring up the question whether the Sahel region is a unit based on the Regional Security Complex Theory or not? Which countries are part of the Sahel? Can it be treated as a region? In this article I will give my answer to that question.

Keywords: *Regional Security Complex Theory, regional security, Sahel region, African security*

Barry Buzan and Ole Waever presented their thoughts about the Regional Security Complex Theory (RSCT) in *Regions and Powers – The Structure of International Security.* In this book, Buzan and Waever have continued their work about the new approach of security which was published in *Security: A New Framework for Analysis*.[2]

In *Regions and Powers*, we can learn about the theory itself in detail, and also the units of the global system by the theory. In the followings, I will summarise the main parts of the RSCT, examine the African security system and finally present the comparison of the theory and the regional features of the Sahel.

Africa is an everchanging continent, where the social structure, the security system, the challenges of the sustainable peace and development are constantly mutating.[3] This varied structure challenges the traditional state-based approach and demand the people-based human security and the regional approach also.

Regional Security Complex Theory

The end of the cold war has changed the international security system fundamentally. New theories, new approaches started to unfold, new relationships, new states appeared in the

[1] PhD student, University of Public Service, Doctoral School of Public Administration Sciences; e-mail: varga.marton1@gmail.com; ORCID: https://orcid.org/0000-0003-1201-5018

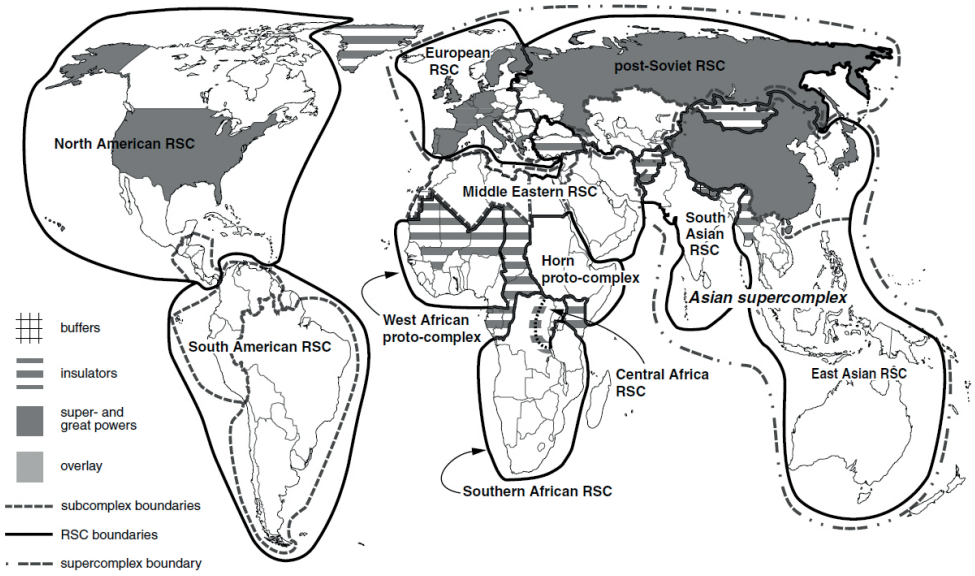
[2] Barry Buzan and Ole Waever, *Regions and Powers – The Structure of International Security* (Cambridge: Cambridge University Press, 2003).

[3] UN Economic Commission for Africa, 'Conflict in the Sahel region and the developmental consequences', *United Nations*, December 2016.

global dynamics after the first years of the 1990s. The relevance of the Regional Security Complex Theory has grown significantly from this time, but the idea was not completely new. As Buzan wrote, some version has already been made about local balances of power, but as a new approach for the international and the global security it was published in *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*.[4]

The RSCT has given a new level for the analysis which is wider than the level of the states as such; it grants a more complex view. At the same time, it is narrower than the general approach which means that we can examine the particular regions more specifically.

This regional perspective has been highly appreciated after the collapse of the bipolar security system and the unipolar moment. Since the rivalry between the United States of America (USA) and the Soviet Union existed no more, the role of the regional powers increased. The opinion of Waever and Buzan said that the new global security system built up as 1 + 4 + 11. 1 means the only state with global power, the USA. 4 is the number of the great powers: China, Japan, Russia and the European Union (EU). Finally, the security structure contains 11 regions: North American RSC, South American RSC, European RSC, Middle Eastern RSC, West African proto-complex, Horn proto-complex, Central African RSC, Southern African RSC, post-Soviet RSC, South Asian RSC and the East Asian RSC (Map 1).



Map 1: The global security structure

Source: Buzan and Waever, Regions and Powers, xxvi.

[4] Buzan and Waever, *Regions and Powers*.

What is a regional security complex?

The history of regional security complexes has three parts.[5] Before 1500 we cannot identify a permanent global level and system; therefore, there were only separated worlds with limited connection between them. The first part lasted from 1500 to 1945.[6]

This period was defined by the European impact, while most of the regions were ruled by European powers as colonisers or had tight connection with them. During these ages, there were not any regions like nowadays, but the whole world was one region under the European imperial powers. After the Second World War, the structure changed, and due to the decolonisation, numerous new states were born or reborn. New dynamics started between the new states and within the regions. In parallel, another process took also place, the building of the bipolar system by the Soviet Union and the USA. That bipolarity was the main principle in the second part from 1945 to 1990. After the fall of the Soviet Union, the third part has begun. This period started with the so-called unipolar moment, with the global power of the USA and has transformed into the multipolar system.[7] In this international regime, countries lost the safety net even if they officially were not part of the 'western' or 'eastern' block and they had to start to play their own role in the international system.

To understand the RSC, we got two definitions from Buzan and Waever. Buzan's original description from 1983 said: 'A group of states whose primary security concerns link together sufficiently closely that their national securities cannot reasonably be considered apart from one another.' In 1998, the authors redefined it as 'a set of units whose major processes of securitisation, desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another'.[8] The core of the definition did not change, but it lost the state-centred view and the primarily military based approach.[9] What does the definition mean? There can be some kind of cultural, historical, economic, religious or geographic link between them, but there has to be some kind of security link also.[10] In an RSC among the countries, there is security interdependence which defines the RSC itself. These connections can have some negative effects, like fears or progressive dynamics, like aspirations. The security link between the countries not only means that force brings them together, but also means something to differentiate them from the other security regions.[11]

In general, the main features of the countries (political system, geography, culture) can determine the security dynamics of a region. For example, based on the theory of democratic peace, war between democratic states is unlikely. But it is also true, that because of the many differences and the numerous combinations of the features, it is not possible to define clear types of the countries. On the other hand, there is a useable typology to place the state in a spectrum, the spectrum of weak and strong states. In this spectrum we are able to define countries based on the level of their stateness. This stateness means the level of the socio-

---

5 Barry Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Coventry: University of Warwick, Department of International Studies, 1983), 105–114.

6 Buzan and Waever, *Regions and Powers*, 15.

7 Béla Háda and Péter Tálas (eds), *Regionális biztonsági tanulmányok* (Budapest: Nemzeti Közszolgálati Egyetem Nemzetközi Intézet, 2014).

8 Buzan and Waever, *Regions and Powers*, 44.

9 Ibid. 44.

10 Ibid. 43–44.

11 Ibid. 48.

political cohesion of the governmental system and the civil society. In this way, there are strong and weak states according to the sovereignty the state owns. For strong states threats are coming from outside the borders, while weak states have significant internal challenges connected with more vulnerability of outside threats.[12] The socio-political cohesion is measurable by, for example, the level of democracy, legal reforms, good governance, human rights performance, movement of goods, labour or capital.[13]

Another question is where a country can be positioned on the postmodern, modern and premodern scale of the countries. Modern state stands in the centre of the scale as the Westphalian state type, with strong governmental power and sovereignty, ability to stand against outside influence in economic, political or cultural fields. A modern state is not necessarily a democratic or advanced capitalist state and it can also be weak or strong state.

The main representatives of the postmodern states are the members of the EU. In this category, states are mostly democratic and open minded in the field of culture and economy. Postmodern states build on cross-border cooperation for the interests of the society. In the field of security, the main factor is no more the inside/outside threats but the different structures, links, cooperation between the members to connect them together.

On the other end of the scale we find the premodern states, mostly from Africa and Central Asia. In this category we can see weak states at the beginning of the long road to build a functioning state and also failed states where strong sub-state actors affect security.[14]

According to the above, we can state that in spite of the many differences of the states, the various combinations of inner and outer features and the continuous changing of these means, any RSC can contain weak and strong, and also modern, premodern or postmodern states. These differences are one part of the security dynamics of the RSC.

After the presentation of some usable category of states, we are able to examine the relations between RSCs. Based on the inner relations, there are different forms of the RSCs: rivalry, balance-of-power and alliance. As Buzan and Waever stated, these relations are strongly affected and defined by durable patterns of amity and enmity. These relations are influenced by local and regional connections sometimes with long historical backgrounds.

Buzan and Waever also stated that in their opinion RSCs are mutually exclusive.[15] That means that we can draw the whole word with RSCs, global actors – who are able to influence more RSCs – and insulator states between larger units or powers (not the same as buffer states[16]). Smaller countries usually play only in their RSC with limited capacity to control it. While great powers can define the internal relations and have interests in other connected regions, and they are able to make activities there for their own security. Moreover, superpowers are able to act more freely than great powers and can play a leader role in any RSC.

Every RSC has four essential variables:[17]

1. boundary, which differentiates the RSC from its neighbours

[12] Ibid. 20–22.
[13] Ibid. 25.
[14] Ibid. 22–25.
[15] Ibid. 48.
[16] Ibid. 41.
[17] Ibid. 53.

2. anarchic structure, which means that the RSC must be composed of two or more autonomous units
3. polarity, which covers the distribution of power among the units, and
4. social construction, which covers the patterns of amity and enmity among the units

Based on the mentioned attributes, Buzan and Waever differentiated two main and some special forms of the regional security complexes.[18] The first group of the forms are centred RSCs, which can also divide into more groups, like unipolar or integrated. In the unipolar form, the leader power can be a superpower, like the USA in North America, or a great power like Russia in the Commonwealth of Independent States. The other type of centred RSC is a special form when the security dynamics of a region is mostly influenced by some integrated institutions. The best example of that form is the European Union.[19] In a centred RSC, we can name a regional or global power who dominates the security agenda of the region.

In contrast with the centred RSC, in a standard RSC we cannot name one power who defines its region. Also, that does not mean, that in standard RSC there are not any regional powers, but without one leading power the security structure is anarchic. Standard RSC can be unipolar, like Southern Africa with the regional power South Africa, or multipolar like South Asia with the two rival power India and Pakistan. These anarchic structures are defined by the relation between the members (rivalries, balances, alliances, friendships).

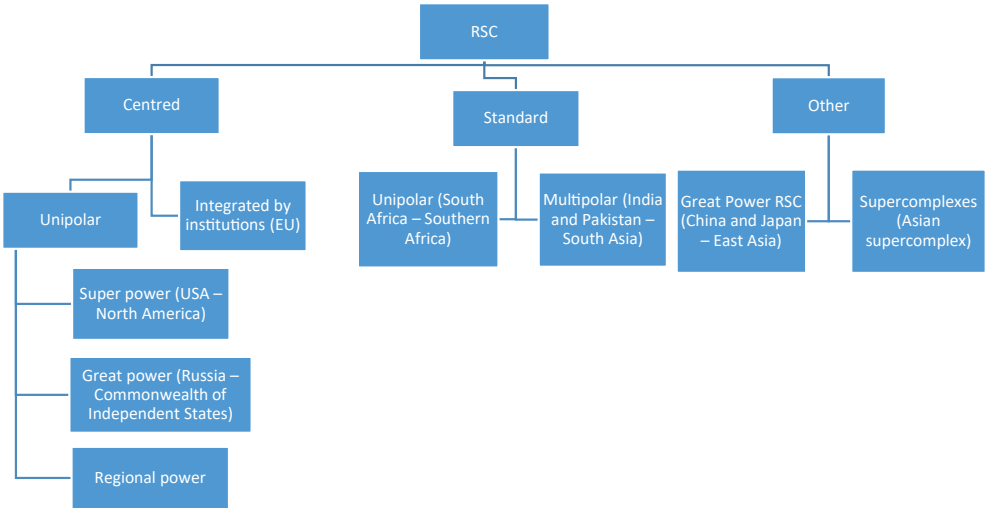


Figure 1: Types of regional security complexes

Source: Compiled by the author.[20]

[18] Csaba Vida, 'A regionális biztonsági komplexum elmélete és alkalmazása Közép-Európára', *Hadtudomány* 7, no 1 (2007), 30–40.

[19] Buzan and Waever, *Regions and Powers*, 54–61.

[20] In the Figure I used the examples of Buzan and Waever, *Regions and Powers – The Structure of International Security*. We must notice, that based on their work, there are many other interpretations of the regions and complexes. For example, the Middle Eastern RSC can be divided into three sub-complexes (Levant, Gulf, Maghreb) or in the Mediterranean region, the Euro-Mediterranean RSC is definable. Éva Remek, 'Az Európai Unió és a Közel-Kelet I.', *Nemzet és Biztonság* no 5 (2017), 4–30.

In the global security system, we can find some other special type of the RSC which cannot be categorised into the standard or centred types of RSC. One of the special types is the great power RSC, in which there are at least two global players, the example of this is East Asia with Japan and China. Finally, the other special case is the supercomplex. In a supercomplex, we can find one or more great powers and very complicated security dynamics that has led to a weak interregional level but the superregional took its place. The presented types of RSC can be seen in Figure 1.

After the categories of the regional security complexes, we also have to mention two cases, when the region cannot be put into the mentioned types. The first is the absence of RSC.[21] There are two situations when RSC cannot be formed or do not form. The first case is overlay, which means that the members of the region cannot form the RSC because the influence of a great power or superpower in the region is too high for the members to operate their own security relations. A good example for this situation is the Cold War Europe influenced by the two superpowers.

The second case of absence is the unstructured RSC. In this case, on the one hand, the countries are not able to project their will on regional level, because they are fragile or failed states with low capabilities. On the other hand, the countries of the regions can be divided from each other geographically (for example, separated islands) and because of this, strong security links cannot be formed. Buzan and Waever said that the Sub-Saharan Africa and the Pacific are good examples for the absence of RSC.

After this short summary of the Regional Security Complex Theory based on *Regions and Powers* by Barry Buzan and Ole Waever, I will examine the Sahel region from the perspective of the RSCT. The questions are how does the Sahel fit in the RSC theory, are there any links between the countries of the region to form some kind of complex, what region can we exactly call Sahel?

The Regional Security Complex Theory and Africa

Before I concentrate on the Sahel region based on the RSCT, we have to take a look on the whole continent. In the following, I present how the Post-Cold War African security system was defined in *Regions and Powers*. According to the structure of RSC built by Buzan and Waever, Africa is divided into two parts. The region of Northern Africa is part of the Middle Eastern RSC, while we have to examine Sub-Saharan Africa as the other part of the continent. In this article, the main focus is on the Sub-Saharan region. (In the following, I will mention Sub-Saharan Africa only as Africa.)

With the European state phenomenon and the idea of the Westphalian state, we can declare that African countries are very young entities with so many difficulties. After their decolonisation, a significant part of African countries could not operate as a well-functioning state. One reason of that was that the new leaders of these countries were not able to use the ideas of 'European' or 'Western' style states. Most of the new African states failed their governmental role as well as their exercising power. With this unstable background and the lack of sovereign power, these states have become unfit to play on the international

[21] Buzan and Waever, *Regions and Powers*, 61.

level, operate on regional or continental stages. Many countries fell towards personalised regimes, dictatorships or fell prey in the hands of warlords.

I typified the African continent as an ever-changing entity. In *Regions and Powers* Buzan and Waever presented Africa in the middle of transition after the end of the bipolar global security system. Nearly thirty years have passed since that change and just like the global security environment, the African security has changed a lot too. To investigate today's Africa through the lens of the RSCT, we have to compare the features of African states of the 1990s and nowadays.

The concept of the Weberian state has some vital elements, such as legitimacy and sovereignty. First of all, the power of the state must be based on the general acceptance by the society of the state, its decisions, its administrational system, the monopoly of the state on the necessary fields for example on violence. Legitimacy has three different types, traditional, charismatic and legal-based. Sovereignty is a necessary, inevitable element (*conditio sine qua non*) of a state. It has two sides, the outer sovereignty which means that the state is independent from other countries, the power of the state is not limited by other countries. The other part is internal sovereignty, which requires that within the boundaries of the state there is not any other state-like power and the state is the only one acting like this.[22]

The creation and the development of the countries of Africa are very different compared to the countries of any other continent. The most important thing we have to mention is that most countries of the post-colonial Africa were not born as a result of some natural process but were created by the former colonisers and great powers. Because of the local specificities, the Westphalian model works in a very different way in Africa. The boundaries drawn by the foreign powers could not have the role of state borders; the ethnic social and political boundaries are more significant. The development of the region was influenced by different ideologies of the end of the twentieth century. The pan-African idea, the 'safety net' that the Organisation of African Union (and later the African Union) meant, and the network of the regional institutions all have a part in the process in which African states did not follow the Westphalian security system with military rivalry and interstate wars. The strong and dense network of the international and regional institutions backed by the UN, other international organisations and different powers made it impossible for the African countries to have the necessary strong impetus to start a military-political competition which is a natural feature of the anarchic international system. For this reason, the security dynamics have developed less dynamically as in other regions.[23]

Comparing the Weberian idea and the post-colonial Africa, legitimacy and sovereignty are at least questionable. The impact of the former colonisers in the creation of the countries undermined the legitimacy and the outer part of sovereignty. In addition, the strong local, ethnic, often traditional and cross-border connections, the military groups, warlords, radical or terrorist groups all make it impossible to create the inner sovereign power by the state.

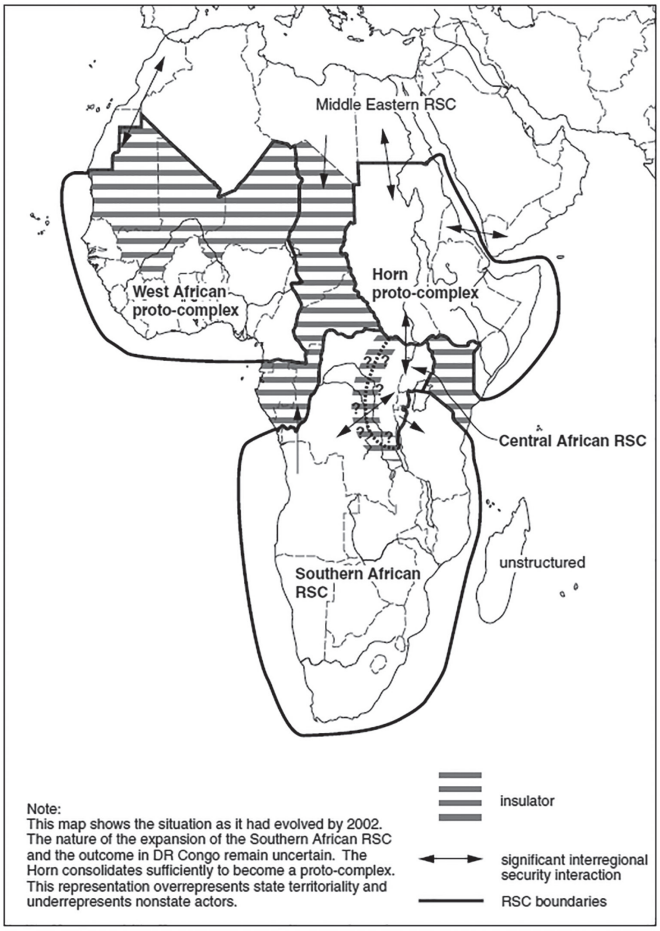
In the presented security environment, Buzan and Waever have defined the following parts of the African security: Southern African RSC, Central African RSC, West African proto-complex and Horn Proto-complex. The post-Cold War status has showed an evolving

---

22 Gábor Pál (ed.), *Politológia – Betekintés a politika világába* (Budapest: Dialóg Campus Kiadó, 2018).

23 Buzan and Waever, *Regions and Powers*, 221–222.

continent, in the middle of great changes. As we can see on Map 2, the authors could define only two concrete RSCs, and a huge part of the continent had an insulator role or formed a proto-complex.

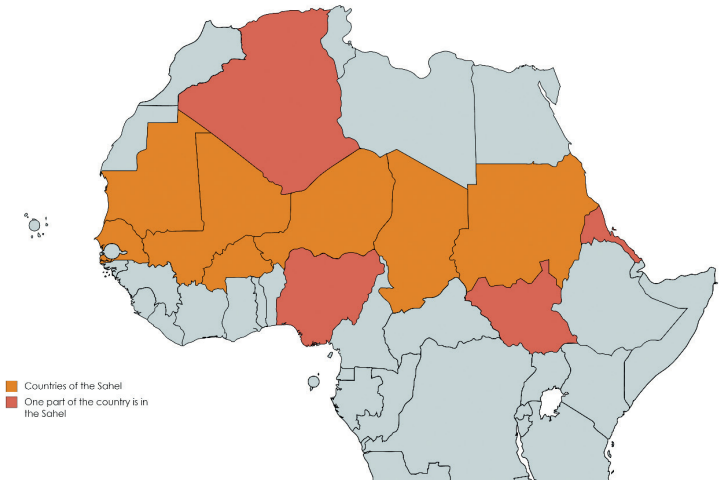


Map 2: The security complexes of Africa

Source: Buzan and Waever, *Regions and Powers*, 231.

To implement the RSCT on the Sahel region, we have to examine which region is exactly the Sahel. The different international actors, the various disciplines have different concepts about the Sahel. Geography uses a wide definition which says that the Sahel is a semiarid region of western and north-central Africa extending from Senegal eastward to Sudan.[24] The Sahel is a 5,000-kilometre belt of land below the Sahara Desert, it stretches from Africa's Atlantic coast to the Red Sea, says the UNDP.[25]

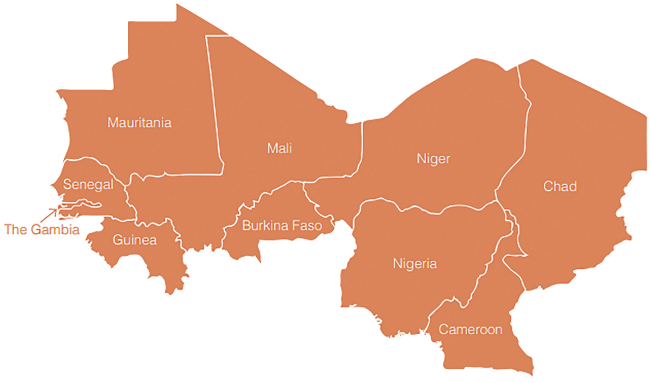
[24] Encyclopaedia Britannica, 'Sahel'.
[25] UNDP, 'Sahel – A region of opportunities'.



Map 3: The Sahel region in a geographic approach

Source: Compiled by the author.

In contrast, the political approach, the different strategies of the international organisations use a very different definition of the region. I have already mentioned that the UN presented the Sahel as a belt across Africa from East to West. In 2013, they described the region as: 'The Sahel stretches from Mauritania to Eritrea, including Burkina Faso, Chad, Mali, the Niger, Nigeria, Senegal and the Sudan, a belt dividing the Sahara desert and the savannahs to the south.'[26] In the UN Support Plan for the Sahel, another group of states is mentioned, which contains only the western countries of the zone (Map 4): Senegal, the Gambia, Mauritania, Mali, Burkina Faso, Guinea, Niger, Nigeria, Cameroon and Chad.



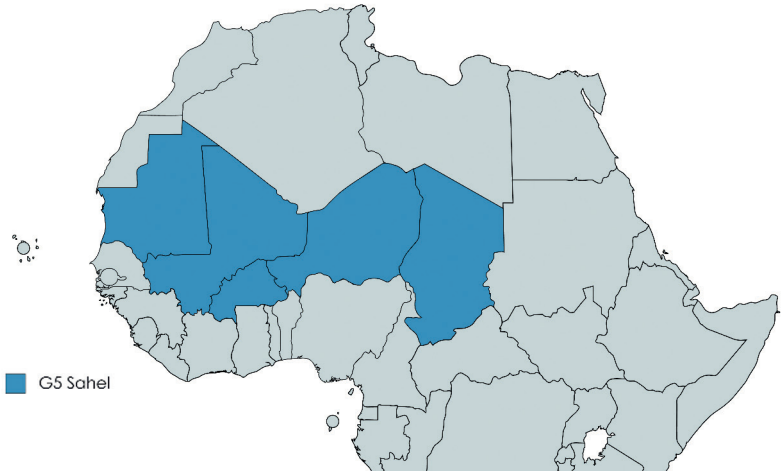
Map 4: The Sahel in the UN Support Plan

Source: United Nations, 'UN Support Plan for the Sahel', May 2018.

[26] UN Security Council, 'Report of the Secretary-General on the situation in the Sahel region', *United Nations*, 14 June 2013.

In another document, the UN has reduced the number of the states, and only focused on five countries: Burkina Faso, Mali, Niger, Nigeria and Mauritania.[27]

The European Union also has a special strategy for the region. At the beginning, the EU started to cooperate with Mali, Mauritania and Niger, as the countries of the Sahel. In 2014, they extended the list with Burkina Faso and Chad. These five countries created the framework for the cooperation named G5 Sahel (Map 5).[28]



Map 5: The G5 Sahel

Source: Compiled by the author.

The government of Norway also presented a programme to support the Sahel region. In the Strategy for Norway's efforts in the Sahel region 2018–2020, the Sahel refers to Mali, Niger, Mauritania, Chad and Burkina Faso, and to parts of north-eastern Nigeria.[29] The Norwegian strategy also mentions Algeria, Morocco, Libya and Cameroon as countries with shared characteristics with the Sahel.

These were only a few examples but the differences between definitions and the targeted areas are clear. The question is which Sahel could be the basis of a Sahel complex?

Sahel as a complex

Africa and the Sahel region have changed a lot in the previous 20–30 years. The post-Cold War dynamics has transformed, developed, new players and new challenges have appeared. Nowadays, we can see the vulnerable and fragile states, civil wars, radicalisation, famine, human trafficking. The Weberian idea could not come true in these states. However, the number of the non-state actors has increased both on the positive (for example, new

[27] UN Economic Commission for Africa, 'Conflict in the Sahel region'.
[28] Secrétariat Permanent du G5 Sahel.
[29] Ministry of Foreign Affairs, 'Strategy for Norway's efforts in the Sahel region 2018–2020', September 10, 2018.

international organisations, foundations, NGOs) and the negative side (for example, radical and terrorist groups). I have already mentioned the UN and the EU as an example but the African Union, the ECOWAS, the G5 Sahel have also a very important role in the region. All of the different development funds, programmes, action planes strengthen the cohesion between the countries of the region and build the cross-border links, and the regional thinking. In parallel, the radicals, different rebel groups, terrorist organisations (for example, AQIM,[30] GSIM,[31] Boko Haram[32] and so on) and especially the root causes[33] of the strengthening of these groups weaken the legitimacy of the states and also question their sovereignty. We also have to admit that we can find countries in Africa, in the Sahel or near the Sahel, who could achieve significant economic growth in the past few years. For example, Ethiopia, Ivory Coast and Senegal are part of the 15 fastest-growing economies in the world in the present and in the 5-year projections, too.[34] Every country has different opportunities, resources and abilities, and we cannot expect the same development from the countries of the Sahel, but the three mentioned states can be the good example for the countries of the region.

Previously, I used the following definition to the regional security complex: 'A set of units whose major processes of securitisation, desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another.' Does any one of the Sahel definitions fit for this concept? I also presented four essential variables of the RSC: boundary, anarchic structure, polarity and social construction. How are these realised in the Sahel?

The Sahel in the geographic approach, based on *Regions and Powers*, belongs to the West African proto-complex, the Horn proto-complex and most countries of the area are insulators. The geographic definition determines a large area, with too many countries. These countries have too many differences (ambitions, priorities, challenges, opportunities) and also the security regime in the western, eastern and central part of the Sahel is very different to form an RSC.

If we exclude the geographic view as the basis of the Sahel security complex, we can examine the area presented in the UN Support Plan. In this zone, we cannot find the structured security links required to form an RSC. This group is still too varied, and the security background of the countries are too different to use the Sahel security complex in this area. Similarly, despite the fact that the West African proto-complex includes

---

30 AQIM: Al-Qaeda in the Islamic Maghreb. The former GSPC (Groupe Salafiste pour la Prédication et le Combat) joined the Al-Qaeda in 2007. It has become one of the most influential terrorist groups of the Sahara and Sahel region. Gábor Búr, 'Az AQIM, az iszlám Maghreb al-Kaida szervezete', in *Afrikai terrorista- és szakadárszervezetek*, ed. by Álmos Péter Kiss (Budapest: HM Zrínyi Nonprofit Kft., 2015).

31 GSIM: Group for the Support of Islam and Muslims (Jama'at Nasr al-Islam wal Muslimin [JNIM]). In 2017 three terrorist groups, Ansar al-Din, al-Murabitoon and al-Qaeda in the Islamic Maghreb's (AQIM) Sahara branch unified and formed GSIM. They have fought against France, the 'historical enemy of the Muslim word'. Their main zone of activity is Mali, Niger and Burkina Faso. Center for Strategic & International Studies, 'Jama'at Nasr al-Islam wal Muslimin (JNIM)', 2018.

32 Boko Haram: The Group of the People of Sunnah for Preaching and Jihad (Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād) commonly known as Boko Haram. In 2015, Boko Haram's leader pledged allegiance to the Islamic State of Iraq and the Levant, one of the four deadliest terrorist groups in 2017. Institute for Economics & Peace, 'Global Terrorism Index 2018'.

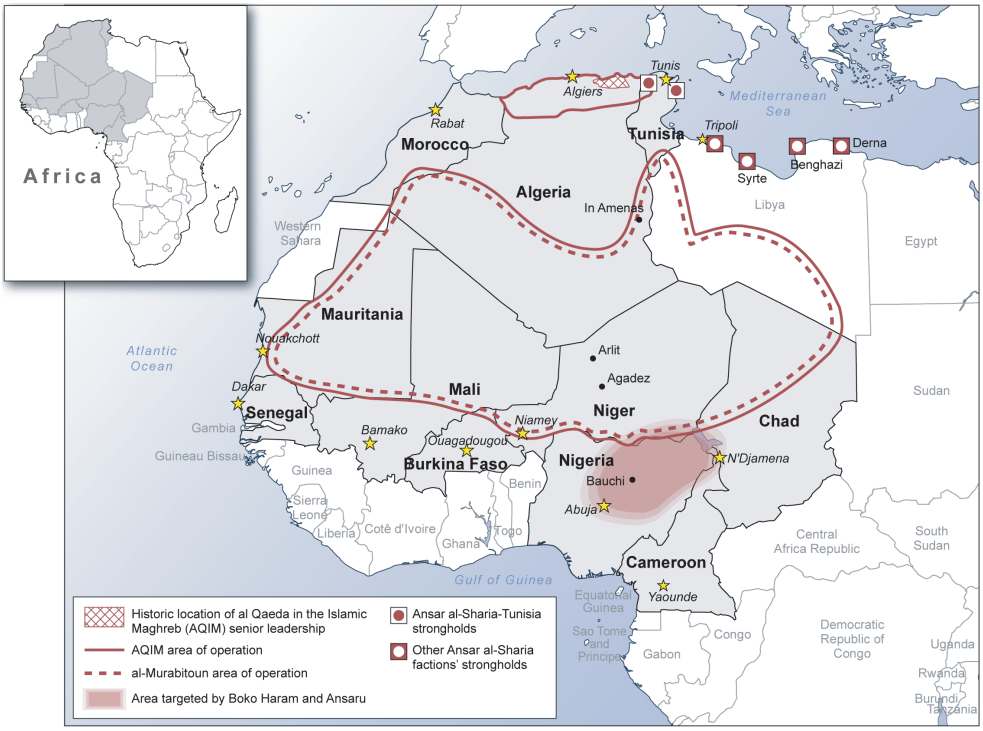
33 Márton Varga, 'Társadalmi biztonság a terrorizmus árnyékában', *Hadtudomány* nos 1–2 (2017), 127–137.

34 Oliver Reynolds, 'The World's Fastest Growing Economies', *Focus Economics*, 16 February 2021.

a significant part of the Sahel, this complex means much more security challenges, links and connections than the Sahel itself.

Finally, the question is whether the G5 Sahel meets the requirements to become some kind of entity by the RSCT. Countries of the G5 Sahel have similar historic, economic, political and security background. This group means a much narrower unit than the other mentioned grouping. In the G5, we can find landlocked countries, except Mauritania. Their territory is defined by not just the Sahel, but the Sahara also. This way, they have very similar economic and commercial opportunities. Their common historical background, as former French colonies, also determine their communities.

The extra factor, which connects these countries is the common enemy. An enemy under the state level and not on the local but the regional level. The enemy are the international terrorist groups, especially the AQIM (Map 6) that has played a decisive role in the region. The radical and terrorist groups in this region can be a strong challenger to the states on the peripheral areas. The states missed to fulfil their duties and created the opportunity for the extremists to integrate themselves into the society.[35]



Map 6: Key Terrorist Groups in Northwest Africa and Their Regions of Operation, 2009-2014

Source: United States Government Accountability Office, 'Combating Terrorism. U.S. Efforts in Northwest Africa Would Be Strengthened by Enhanced Program Management', June 2014.

[35] Varga, 'Társadalmi biztonság a terrorizmus árnyékában'.

Previously, I have presented four essential elements of an RSC. How do these elements work in the Sahel? The four elements:

1. Boundary, which differentiates the RSC from its neighbours: The geographical definition gives the basis, the cooperation of the G5 Sahel defines the exact borders of the regional unit.
2. Anarchic structure, which means that the RSC must be composed of two or more autonomous units: In the G5 Sahel, we can find five sovereign states and numerous other actors under and above the state level.
3. Polarity, which covers the distribution of power among the units: The main competition is not between the countries, but the actors of the state level and the non-state level.
4. Social construction, which covers the patterns of amity and enmity among the units: Because of the complex challenges of the region, the states are doomed to friendships and cooperation, while the enmity is among the state and the anti-state groups.[36]

As we can see, not all the required elements can be found in the Sahel region, consequently, the Sahel region itself cannot be a separate complex. In *Regions and Powers*, the countries of the Sahel region were mostly signed as insulators. In the past decades, the region has gone through many decisive events, there were political, economic, societal changes which influenced the security dynamics in the area. As I presented, there are numerous different definitions of the Sahel region, but the common security challenges among the members of the G5 Sahel made them a new entity in the system of the regional security complex. The G5 Sahel has to be defined as a sub-complex in the West African complex. The G5 sub-complex has its own security dynamics that differentiates it from the West African complex and from the other complexes. It has its own organisation that provides the institutional framework for the region.

Summary

The continent of Africa has a huge amount of difficulties but also opportunities. The ongoing changes are noticeable in every little piece of the African countries' life. The Sahel region has a special role in these processes while there can be found wide interdependent crises in the region. These problems challenge not only the neighbouring countries and the larger international community, but also the theoreticians who are trying to describe the transformations of the security progress with different theories.

In this article, I presented a possible way to describe the Sahel region with the Regional Security Complex Theory. As the conclusion of my examination, the Sahel region can be defined as a regional security sub-complex, which has five member states, Mauritania, Mali, Niger, Burkina Faso and Chad, all of them are part of the G5 Sahel cooperation.

As we can see, Africa mutated significantly since *Regions and Powers* presented it as a continent mostly with different proto-complexes and a huge number of insulator states. I have also showed several definitions of the Sahel region. Consequently, my interpretation

[36] Buzan and Waever, *Regions and Powers*, 53.

of the Sahel region describes only the present status. That is why the Sahel sub-complex cannot be a closed group of states.

We also have to admit, that this article has focused on the Regional Security Complex Theory which is based on the state as the main component of a region. As I presented, that kind of state-centred approach has many difficulties in Africa, since this continent developed so very differently than, for example, the European or Asian countries. Based on the experiences, African countries are open to the cooperation within international organisations. This way Africa is more like the South African complex than European. The question is what will be the result in Africa?

The formation of the African countries, the development of the states are very different than the Europeans. In the areas where the tribal or regional connections are stronger than the citizenship, the meaning of the legitimacy and sovereignty and the state-based Weberian concept fails. It is clear, that we have to use these theories more flexible or we need new concepts, as the number of the non-state actors increases, and the number of inner state and cross-border challenges becoming more pronounced.

References

Búr, Gábor, 'Az AQIM, az iszlám Maghreb al-Kaida szervezete', in *Afrikai terrorista- és szakadárszervezetek*, ed. by Álmos Péter Kiss. Budapest: HM Zrínyi Nonprofit Kft., 2015.

Buzan, Barry, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Coventry: University of Warwick, Department of International Studies, 1983, 105–114.

Buzan, Barry and Ole Waever, *Regions and Powers – The Structure of International Security*. Cambridge: Cambridge University Press, 2003. DOI: https://doi.org/10.1017/CBO9780511491252

Center for Strategic & International Studies, 'Jama'at Nasr al-Islam wal Muslimin (JNIM)', 2018. Online: www.csis.org/programs/transnational-threats-project/terrorism-backgrounders/jamaat-nasr-al-islam-wal-muslimin

Encyclopaedia Britannica, 'Sahel'. Online: www.britannica.com/place/Sahel

Háda, Béla and Péter Tálas (eds), *Regionális biztonsági tanulmányok*. Budapest: Nemzeti Közszolgálati Egyetem Nemzetközi Intézet, 2014.

Institute for Economics & Peace, 'Global Terrorism Index 2018'. Online: http://visionofhumanity.org/app/uploads/2018/12/Global-Terrorism-Index-2018-1.pdf

Ministry of Foreign Affairs 'Strategy for Norway's efforts in the Sahel region 2018–2020', 10 September 2018. Online: www.regjeringen.no/en/dokumenter/sahel_strategy/id2610507/

Pál, Gábor (ed.), *Politológia – Betekintés a politika világába*. Budapest: Dialóg Campus Kiadó, 2018.

Remek, Éva, 'Az Európai Unió és a Közel-Kelet I.'. *Nemzet és Biztonság* no 5 (2017), 4–30.

Reynolds, Oliver, 'The World's Fastest Growing Economies'. *Focus Economics*, 16 February 2021. Online: www.focus-economics.com/blog/fastest-growing-economies-in-the-world

Secrétariat Permanent du G5 Sahel. Online: www.g5sahel.org/

UN Economic Commission for Africa, 'Conflict in the Sahel region and the developmental consequences', *United Nations*, December 2016. Online: https://repository.uneca.org/bitstream/handle/10855/23474/b11580410.pdf?sequence=3

UN Security Council, 'Report of the Secretary-General on the situation in the Sahel region', *United Nations*, 14 June 2013. Online: https://unowas.unmissions.org/sites/default/files/s_2013_354_sahel_strategy_en_0.pdf

United Nations, 'UN Support Plan for the Sahel', May 2018. Online: www.un.org/africarenewal/sites/www.un.org.africarenewal/files/English%20Summary%20Report_0.pdf

United States Government Accountability Office, 'Combating Terrorism. U.S. Efforts in Northwest Africa Would Be Strengthened by Enhanced Program Management', June 2014. Online: www.gao.gov/assets/670/664337.pdf

UNDP, 'Sahel – A region of opportunities'. Online: https://feature.undp.org/sahel/

Varga, Márton, 'Társadalmi biztonság a terrorizmus árnyékában'. *Hadtudomány* nos 1–2 (2017), 127–137.

Vida, Csaba, 'A regionális biztonsági komplexum elmélete és alkalmazása Közép-Európára', *Hadtudomány* 7, no 1 (2007), 30–40.

Wikipedia, 'Map of the Sahel'. Online: https://upload.wikimedia.org/wikipedia/commons/thumb/6/69/Map_of_the_Sahel.png/550px-Map_of_the_Sahel.png

AARMS Vol. 19, No. 2 (2020) 65–78.

10.32565/aarms.2020.2.5

Peacekeepers' Autonomy and Military Authority

Mihály BODA[1]

This article considers the problem of conciliation of military authority and peacekeepers' autonomy. At first glance there is a tension between authority and autonomy in many areas of human life like religion, political life, national soldiering and even peacekeeping missions. The core of this tension is the practical contradiction between authority, which implies reason for controlling the behaviour of others, and the autonomy of the others, which involves reason for self-governing. This article proposes a distinction in peacekeepers' autonomy between professional and moral autonomy, and suggests a way of explaining away the tension. The essential part of the solution is the claim that peacekeepers' professional autonomy involves 'building the moral community' between the formerly hostile sides of a conflict within the confines of international military hierarchy. From this claim I draw the conclusions that the concept of military authority is part of the concept of peacekeepers' professional autonomy, and that due to the content of peacekeepers' professional autonomy, peacekeepers' special moral autonomy is extended as compared to civilian moral autonomy.

Keywords: *ethics of peacekeeping, moral autonomy, military authority*

The conundrum

Soldiers have, or are supposed to have, important moral or morally relevant character traits. Traditionally, such traits include courage, honour, loyalty, discipline, etc.[2] Many of these are commonly referred to as 'warrior' or 'martial' traits.[3] By today, wars and military operations have changed a great deal and soldiers face new challenges. One of these challenges comes from soldiers taking part in peacekeeping operations.[4] Soldiers involved in these operations are expected to have a range of new moral, or morally relevant, abilities;

1 PhD, Associate Professor, University of Public Service; e-mail: boda.mihaly@uni-nke.hu; ORCID: https://orcid.org/0000-0003-3037-3644

2 Cf. Peter Olsthoorn, *Military Ethics and Virtues* (London and New York: Routledge, 2011).

3 David H Levine, *The Morality of Peacekeeping* (Edinburgh: Edinburgh University Press, 2014), 57.

4 In this paper I take peacekeepers as they are soldiers in national armies, too; however, peacekeepers can also come from private forces. See Christopher Spearin, 'Between Public Peacekeepers and Private Forces: Can there be a Third Way?' *International Peacekeeping* 12, no 2 (2005), 240–252; Alex J Bellamy and Paul D Williams, *Understanding Peacekeeping* (Cambridge: Polity Press, 2010), Chapter 4.

for example a special kind of moral fitness;[5] virtues like attentiveness, restraint, creativity[6] and moral autonomy.[7]

In a seminal paper, Paolo Tripodi claimed that soldiers taking part in peacekeeping operations needed special training to develop a special character trait, the one we call moral autonomy. Tripodi says 'a major component of a peacekeeper's identity and mindset should be a strong moral autonomy. Peacekeepers should be prepared to choose a course of action that is in line and coherent with the peacekeeper's role'.[8] And he continues: 'I contend that it is necessary to create a peacekeeper's ethical code. This code should reflect the importance of human life as its central value so that each action taken by a peacekeeper reflects this value. To foster this code, it is necessary to move past law enforcement training and into the area of ethical decision-making.'[9] To foster the ethical code, Tripodi also purports the importance of human rights education.

Tripodi believes that moral autonomy is vital for soldiers because he thinks it is essential that soldiers take the decisions that are morally right in unanticipated situations. He argues that one of the multiple factors which led to the massacre of civilians in Rwanda in 1994 and Srebrenica in 1995 was the training characteristics of peacekeepers, and that for two reasons. For one, soldiers involved in these human rights abuses had been taught mainly how not to violate human rights rather than how to protect them in an active fashion. For the other, the military training they had received resulted in a kind of 'robot psychology'[10] and impaired their moral autonomy. If Tripodi is right, then in fact some human rights catastrophes could be prevented by claiming moral autonomy for soldiers and training them to make morally relevant decisions.

Thinking further along those lines, some additional suggestions can be proposed to complement Tripodi's own. The problem he identifies lies in the tension between peacekeepers' autonomy and military authority, which is an example for the antagonism between autonomy and authority in general. A tension between autonomy and authority exists because to have autonomy means to have reason to be independent and to govern oneself, while to have authority means to have reason to restrict the independence of others and to rule others. Consequently, if someone has authority over another, then, this latter can hardly be said to be an autonomous person, because somebody else makes decisions for them.

The same problem has been uncovered and examined in many areas of life, in areas other than peacekeeping operations. About religion, for example, James Rachels argued that 'even while admitting the existence of such an awesome being [the all-powerful, all-wise, etc. God] we might still question whether we should recognise him as having an unlimited claim on our obedience. … In fact, there is a long tradition in moral philosophy, from Plato to Kant, according to which such a recognition could never be made by a moral agent. According to this tradition, to be a moral agent is to be an autonomous or self-directed

---

5 R Richardson, D Verweij and D Winslow, 'Moral Fitness for Peace Operations', *Journal of Political and Military Sociology* 32, no 1 (2004), 99–113.

6 Levine, *The Morality of Peacekeeping*, 59–66.

7 Paolo Tripodi, 'Peacekeepers, Moral Autonomy and the Use of Force', *Journal of Military Ethics* 5, no 3 (2006), 214–232.

8 Tripodi, 'Peacekeepers, Moral Autonomy and the Use of Force', 219.

9 Ibid. 220.

10 Ibid. 219.

agent'.[11] The same problem arises – in a somewhat different form though – in politics and law. Robert Paul Wolff argued that:

> Authority is the right to command, and correlatively, the right to be obeyed. … Every man who possesses both free will and reason has an obligation to take responsibility for his actions. Since the responsible man arrives at moral decisions which he expresses to himself in the form of imperatives, we may say that he gives laws to himself, or is self-legislating. In short, he is autonomous. … The defining mark of the state is authority, the right to rule. The primary obligation of man is autonomy, the refusal to be ruled. It would seem, then, that there can be no resolution of the conflict between the autonomy of the individual and the putative authority of the state. Insofar as a man fulfills his obligation to make himself the author of his decisions, he will resist the state's claim to have authority over him. That is to say, he will deny that he has a duty to obey the laws of the state simply because they are the laws.[12]

The question this paper is focussing on is whether peacekeepers' autonomy and military authority rule each other out and are mutually exclusive. In what follows, I am going to attempt to show how they can coexist. To support that, I intend to first present the relationship between these apparently opposing terms; then, I will argue that peacekeepers have a special kind of professional autonomy, a special competence which differs from soldiers' professional autonomy but which accommodates military authority; and finally I will conclude that the professional autonomy of peacekeepers has special implication for moral autonomy of them.

Military authority and autonomy

About military authority and autonomy in general

I claimed elsewhere[13] that military authority in essence describes the relation between military officers, for example soldiers, or peacekeepers; it refers to the moral power to command and control others, and the discipline to obey the commands. Military authority presupposes a hierarchy between officers. In hierarchy, there is a superior, the commander, who commands their subordinates. A commander with military authority gives commands to subordinates, which makes it possible for subordinates to discharge their duty.

Soldiers' and peacekeepers' autonomy is some sort of competence to act, and consists in at least two distinct types of autonomy: professional autonomy on the one hand, and moral autonomy on the other. Professional autonomy is a special competence to do things; things required by a profession interpreted as a social role; and so it is not accessible for every human being.[14] Members of a profession have such autonomy because they are empowered

---

11 James Rachels, 'God and Human Attitudes', *Religious Studies* 7, no 4 (1971), 325-337. 334.

12 Robert Paul Wolff, *In Defense of Anarchism* (Berkeley and Los Angeles, CA: University of California Press, 1988), 4, 14, 18.

13 Boda Mihály, 'Soldiers' Autonomy and Military Authority', in *Military Ethics and Leadership*, ed. by Peter Olsthoorn (Leiden: Brill Nijhoff, 2017), 150–167.

14 Ernest Greenwood, 'Attributes of a Profession', *Social Work* 2, no 2 (1946), 46.

by legislation or some other rule. Soldiers' and peacekeepers' professional competences are similar to competences of other professionals, like for instance judges or priests. A judge can make deliberations regarding a case at court and a priest can say mass thanks to their respective special empowerments.

In contrast to professional autonomy, moral autonomy does not derive from the law or other rules but from one's human mental ability, that is, from human reason and will. With the help of reason and will, people can reflect on their own acts as well as on their mental capacities, including reason and will,[15] and so they are able to make decisions which promote the very aim of human reason and will. That aim is to promote the interests of every being that has reason and will.[16] Hence, moral autonomy has two moral effects on its bearer: that is, it makes them morally valuable and morally sensitive. To have moral value means having interests shared by all beings equipped with moral autonomy; to have moral sensitivity means to respect beings that have moral value. Beings that have moral value and moral sensitivity are (according to our recent knowledge) human beings.

Military authority and soldiers' autonomy

A fundamental question regarding the problem of military autonomy is whether military authority rules out soldiers' autonomy as such. People and their autonomy are influenced by military authority if and when they become soldiers. Therefore, I proposed previously to examine soldiers' professional autonomy and the changes in people's human rights after they have entered the military.[17]

At the heart of soldiers' professional autonomy lies their special power to act ('to kill') in a certain way: to apply and manage violence in order to defend state and society.[18] In general, they do that as members of national or allied/ supranational military units, commanded by their superiors, so by embedded in relationships of military authority. That means that soldiers' essential professional autonomy and professional competence could be defined as the applying and managing of violence within the confines of (national or international) military hierarchy, and we could conclude that this autonomy requires military authority. Hence, military authority does not seem to rule out soldiers' autonomy completely: their professional autonomy remains.

As concerning the moral autonomy of soldiers, it is first necessary to understand the implications of the basic moral autonomy of non-soldiers, civilians. A person, before becoming a soldier, has moral value shared by all other human beings equipped with moral autonomy and have moral sensitivity to respect beings that have moral value. They are respected by others and respects others due to the common interests. Respecting the common interests and moral values implies to observe the rules and discharge the obligations that are meant to protect that interest. Those values are called human rights and the underlying

---

15 Cf. Immanuel Kant, *Groundwork of the Metaphysics of Moral* (Cambridge: Cambridge University Press, 1998), 24.

16 Cf. Ibid. 38.

17 Boda, 'Soldiers' Autonomy and Military Authority'.

18 Samuel P Huntington, *The Soldier and the State* (Cambridge, MA and London, England: The Belknap Press of Harvard University Press, 1988), 11.

obligations are moral obligations. A fundamental human right is the right to live and to not being killed; and, likewise, a fundamental moral obligation is 'to let live and not to kill anyone!'. These fundamental rights and obligations belong to every human being before they are enlisted in the army.

By becoming a soldier, a person acquires a new freedom: that is, the freedom to kill enemy soldiers;[19] at the same time, they renounce their own right to not being killed by enemy soldiers.[20] But that is only conditional and temporary, because killing is something morally permissible only on the condition that a war has been unleashed; and because soldiers do not have to stay soldiers forever. In peacetime, soldiers have the same human rights as civilians, and it is in their power to renounce that newly-acquired freedom to kill just as they can re-acquire the unconditional right to not being killed.

In the process of becoming soldiers, soldiers acquire a new and limited form of moral autonomy. Soldiers' moral autonomy is the result of their renouncing a human right and acquiring a freedom in exchange. The limitation of their moral autonomy is precisely the result of the acquisition of a new freedom and the renunciation of a fundamental human right. Because of their special freedom, they cannot completely respect other human beings (for they sometimes must kill enemy soldiers), and because of their special renounced right, they do not have complete moral value (for sometimes, they are permitted to be killed). But at the same time, soldiers hold on to all their other human rights, for example, the one to not being killed at peacetime and by any other than the enemy; and they continue to lack other freedoms, for example, to kill civilians on the enemy's side. So, even though limited, soldiers' moral autonomy is not ruled out by military authority.

Peacekeepers' autonomy and military authority

Apparently, not only is the relationship between military authority and soldiers' autonomy problematic, but also that between military authority and peacekeepers' autonomy. In what follows, I will examine the professional autonomy side and the moral autonomy side of this problem.

Conceptual elements of peacekeepers' professional autonomy: defending civilians, building moral community and international military hierarchy

I have claimed that soldiers' professional autonomy is not ruled out by military authority because soldiers discharge their professional duty with the help of military authority. Peacekeepers' military authority is similar to soldiers' and it can go hand in hand with professional autonomy for the same reason as the former: because military authority is a conceptual part of peacekeepers' professional autonomy. However, peacekeepers' professional autonomy is different from that of soldiers.

---

19 Michael Walzer, *Just and Unjust Wars* (New York: Basic Books, 2006), 36.

20 Ibid. 136.

Alex Bellamy and Paul D Williams understand peacekeepers' professional autonomy in a very broad sense. According to them, irrespectively of whether or not we talk about an intervention based on consent, or an intervention in a conflict between two states or in a conflict within one and the same state, every peace operation pertains to peacekeepers' competence.[21] The authors distinguish seven types of peace operations, which differ from one another in their intended ends. From that derive seven types of duties for peacekeepers. The seven different kinds of peace operations are:

- Preventive deployment: operation 'in order to prevent violent conflict from emerging or a specific threat to a civilian population from materialising'
- Traditional peacekeeping: support for 'peacemaking between states' in case of a ceasefire agreement
- Wider peacekeeping: support for peacemaking between states 'in the context of ongoing conflict'
- Peace enforcement: imposing of 'the will of the UN Security Council', without the consent of the host state
- Assisting transitions: multidimensional operation taking place 'after both ceasefire and a political settlement'
- Transitional administrations: multidimensional operation taking place after ceasefire and coming along with some 'sovereign authority over a particular territory', and
- Peace support operations: establishing of 'liberal democratic political systems and societies within states'[22]

My own understanding of peacekeepers' professional autonomy is somewhat narrower than that. I accept only five of the different types of peace operations out of the seven listed by the above authors; the remaining two I propose to be considered as 'peace enforcement' operations. In peacekeeping operations, only peacekeepers take part in the mission to keep the peace. In peace enforcement operations, national and/or international (allied) soldiers are involved with the aim of enforcing peace.[23]

Peacekeepers are soldiers of a nation but they do not have the same special competence or the same rights and obligations as soldiers of national armed forces normally have. The similarity lies in the fact that peacekeepers rely on commands from their superiors and are part of a military hierarchy. The peacekeepers' job, however, is different. Soldiers are empowered to apply and manage violence in a way peacekeepers are not, and – as opposed to peacekeepers – they receive commands within the context of a national military hierarchy.

Peacekeepers also have features in common with international/allied soldiers. International soldiers take part in some international alliance missions, like NATO missions or peace enforcement operations, which are commanded in the context of an international hierarchy. An important similarity between international soldiers and peacekeepers is, therefore, that they do receive commands not within the confines of a national hierarchy.[24] An important difference is that international soldiers are essentially soldiers anyway, who are empowered to apply and manage violence in a way peacekeepers are not.

---

21 Bellamy and Williams, *Understanding Peacekeeping*, 4–5.
22 Ibid. 7–9.
23 Levine, *The Morality of Peacekeeping*, 6.
24 Ibid. 9–10.

In trying to put our fingers on what peacekeepers' professional autonomy actually is, we must find out about what exactly professional peacekeepers are expected to do. Peacekeepers' professional autonomy is a complex competency: for sure, it includes as conceptual elements of the defence for civilians, the building of moral community and of the international military hierarchy.

Defending civilians

Peacekeepers like soldiers are supposed to apply and manage violence but differently. Soldiers apply and manage violence strategically while by nature, peacekeepers' task is tactical.[25] When soldiers apply and manage violence strategically, they use force to defeat the enemy. In contrast to that, peacekeepers are not allowed to use violence in general, except when defending civilians or themselves. While this distinction may not be so manifest in all cases, it is indeed very important. In 1993, in Mogadishu, the capital of Somalia, a peacekeeping mission turned into a combat operation. Ever since then, the term 'crossing the Mogadishu line' has had a very clear and distinct meaning.

The tactical application and management of violence may be understood as a sort of policing.[26] Tony Pfaff says peacekeepers are allowed to use lethal violence in a restricted way, exactly like police officers. Both use violence in peacetime, against citizens who violate the rights of other citizens; and the reason for that is that the violation of a person's rights is a disruption of the peace. In such a situation the use of violence would be another disruption of the peace; therefore, peacekeepers and police officers are only allowed to use 'the least force possible'. In contrast to policing, soldiers' activities are not to defend individuals' rights but to secure those of a state.[27] And the situation where they are allowed to use 'the most force permissible' is war.

Given that peacekeepers are not allowed to resort to violence except when defending others or themselves, they have no enemy.[28] To have an enemy is 'to be in relation of enmity' with someone, which provides one with a reason to strategically apply and manage violence against them. Enmity may occur, for example, between different sides within a population where peacekeepers are needed; but not between one or more sides of the population on the one hand and peacekeepers on the other.

But what kind of relation exists between peacekeepers and the different sides of the former conflict? In light of the above, that relation is identical to the relation between police officers and criminals. Peacekeepers are expected to deal with war criminals from the local communities. Peacekeepers seek out war criminals with the intention to arrest them just as police officers seek our ordinary criminals. Although, a different, and – from the moral perspective – more interesting relation also exists between peacekeepers and the local population, which can be explored by looking at the other side of peacekeepers' professional autonomy.

---

25 Ibid. 7.

26 Tony Pfaff, *Peacekeeping and the Just War Tradition* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000), 13–20.

27 Walzer, *Just and Unjust Wars*, 51–63.

28 Levine, *The Morality of Peacekeeping*, 21–33.

Building of moral community

Peacekeepers' task of tactically applying and managing violence is only part of their duty. Peacekeepers' other task has to do with the claim that 'peacekeepers have no enemy'. Peacekeepers enter a territory in order to promote peace there – negative or positive peace.[29] 'Promoting negative peace' means an attempt to maintain social conditions among which the formerly hostile sides can live side by side by impeding the use of direct physical violence. Negative peace implies the absence of direct physical violence: it is peaceful on the level of actions but not on the level of intentions. And intentional violence is strongly connected with structural and cultural violence. Structural violence is without an actor *per se* who would commit the violent act,[30] and cultural violence is an aspect of a culture which can be used to justify or legitimate structural or other sorts of violence.[31] Examples for structural violence include social structures like multicommunication systems or vehicles of distribution, and the examples for cultural violence are stars, crosses, flags, anthems, military parades or the portrait of leaders. Negative peace, as it allows intentional violence to survive, is a very fragile setting for a society and it can be maintained by the defensive use of force and materialises through the aforementioned activities of peacekeepers.

By promoting positive peace, peacekeepers can create a world where the formerly hostile sides can live in moral harmony. A precondition for positive peace is not only the absence of direct physical violence but also the presence of the more or less harmonious intentions. To create such conditions the mindset of people must be changed; that is, peacekeepers must change how the local people think about other groups and improve their understanding of others through learning;[32] or, more widely speaking, by building a special community from the formerly hostile sides of a population. According to David H Levine, peacekeepers' most important task is to build a moral community in the territory where they are promoting the peace.[33]

Building a simple community involves giving reasons to prospective members to believe in the community and act in a special way. The people will begin to share those reasons. Such groups of people will become sensitive to and accountable for those shared reasons and hence they are willing to collaborate with each other for the shared reasons, and respect each other because they collaborate.

Building a moral community presupposes that we supply moral reasons to a group of people in order for them to accept all people in the world, and especially all members of the former enemy, and think about them like one of 'us', a fellow human being. The moral community provides for collaboration, so the members may actively contribute to each other's projects. But they can collaborate with each other passively, that is, by not making any contribution to each other's objectives but not hindering the others either, or active, when they help each other to achieve their goals. Although in both cases, each member of the community is very important and earns more respect as an autonomous person, active collaboration is morally deeper than the passive one. This is so because the passive

29 Johan Galtung, 'An Editorial', *Journal of Peace Research* 1, no 1 (1964), 2.
30 Johan Galtung, 'Violence, Peace, and Peace Research', *Journal of Peace Research* 6, no 3 (1969), 170.
31 Johan Galtung, 'Cultural Violence', *Journal of Peace Research* 27, no 3 (1990), 291.
32 Galtung, 'An Editorial', 3.
33 Cf. Levine, *The Morality of Peacekeeping*, 43–56.

relationship is morally more superficial then the active and helping collaboration, which establishes more autonomy for the other members of the group.[34]

The task of building a moral community results in a special relationship between peacekeepers and the locals in that peacekeepers attempt to integrate local people into the moral community which they are meant to build. Let us take a closer look at the process of integration to find out more about that relationship.

To become a member of the moral community, the would be members need to acquire theoretical knowledge about human rights and the implications thereof. They, of course, can attend human rights courses, but that alone ensures compliance with abstract norms only. For that reason a second, more practical, phase becomes necessary. At that stage, they must learn how to act in collaboration with others in accordance with the relevant standards. There are at least three different ways of getting there. Levine suggests that people learn through 'habituation to compliance' or the 'creation of enforcement/punishment/accountability practices'.[35] Habituation, however, is a process that relies only on unconscious repetition; and creation in this context means the fostering of an institutional threat for those who are not sensitive to moral reasons; these involves deterrence and punishment to enforce moral reasons. While one or more of these suggestions (including acquiring theoretical knowledge as well) are clearly useful, these methods seem to be missing one essential point. According to the 18–19th century German philosopher, Johann Gottlieb Fichte, in order for one to learn the moral duties or become a member of moral community, they need to realise the practical importance of human rights themselves, that is, autonomously; not only through theoretical knowledge, habituation or coercion. This is the implication of the final purpose of teaching practical morality, which is 'to protect and to promote the formal freedom' – the moral autonomy – 'of our fellow human beings'.[36]

So there is yet another, alternative third way of teaching practical morality to people: notably, by setting an example by doing what is morally right. Setting an example is important as it teaches good morals and involves teaching respect, which cannot be compelled nor created artificially. Respect towards others is not abstract, and it cannot be taught by habituation or using punishment. However, it can be inspired in others, that is, if someone sets a good example, it naturally can generate respect.[37]

Before acquiring both the theory and the practice of human rights, no one can be a member of a moral community, and so the depository of human rights in the sense that they cannot make moral claims. The aim of the teaching and learning process is precisely that, that is, to elevate people to personhood and so create the possibility for them to make moral claims. Once that creation is completed, a moral community has been built.

---

34 Cf. Christine Korsgaard, 'Creating the Kingdom of Ends: Reciprocity and Responsibility in Personal Relations' in *Creating the Kingdom of End* (Cambridge: Cambridge University Press, 2000), 192–193.

35 Levine, *The Morality of Peacekeeping*, 54.

36 Johann Gottlieb Fichte, *System of Ethics* (Cambridge: Cambridge University Press, 2005), 299–301.

37 Cf. Ibid. 298–299, 301–302.

International military hierarchy

Finally, peacekeepers' professional autonomy has to do with the military authority relation through which they discharge their duties. This is because peacekeepers are themselves partly soldiers, and therefore to discharge their duties they must be part of military authority. They could do their job alone, but then they would not be professionally autonomous peacekeepers but, for example, volunteers. That means that peacekeepers keep the peace with the help of a hierarchy which is similar to soldiers' military hierarchy in nature.

The hierarchy of peacekeepers, however, differs in at least one aspect from the hierarchy of soldiers. Soldiers of a national army are commanded by the officers of that army and by the leaders of the nation. In contrast to that, peacekeepers are commanded, at least at high level, by the officers of the international military contingent they belong to, and by the decision-makers of the international community. Peacekeeping operations are generally understood to be carried out by UN member states and to be organised and authorised by the Security Council of the United Nations and the Military Staff Committee, which consists of the Chiefs of Staff of the permanent members of the Security Council.[38] The Security Council deploys peacekeeping forces on behest of the Military Staff Committee. It is the Military Staff Committee which then devises the strategy of peacekeeping operations.

All in all, a special form of military hierarchy is a conceptual part of peacekeepers' professional autonomy. One consequence of this is that, similarly to soldiers' professional autonomy and military authority, one sort of peacekeepers' autonomy (that is, their professional autonomy) can be accommodated with military authority as professional autonomy includes it as its conceptual part.

Peacekeepers' moral autonomy and military authority: Extended moral autonomy

I claimed that soldiers have limited moral autonomy; the kind of autonomy which is not ruled out by military authority since soldiers – temporarily and conditionally – renounced the human right of 'not to be killed' and acquired the power to kill enemy soldiers, but they shall continue to have all other human rights and lack all other freedoms. This is true for both sides of a war due to the enmity relation of the belligerents.

Similarly to soldiers, peacekeepers temporarily and conditionally renounce the human right of 'not to be killed' and acquire the power to kill enemy soldiers, but because they are peacekeepers and do not have enemies this potential does not materialise. Their moral autonomy cannot therefore be limited in the sense soldiers' moral autonomy can. What characterizes peacekeepers' moral autonomy? Is it akin to people's moral autonomy, that is, the same as the most fundamental, unlimited moral autonomy? Is it ruled out by or can it subsist alongside military authority?

As mentioned earlier, a person's moral autonomy has two moral effects on its bearer. On the one hand, moral autonomy makes its bearer morally valuable; on the other, it has its own inherent aim which makes morally autonomous persons morally sensitive to beings

[38] Charter of the United Nations, Chapter VII, Articles 43–48.

with a moral value, that is, to other people. This moral sensitivity means being depository of human rights and partly consists in having 'fundamental answerability' to every other trustee of human rights interests.[39] Acting only because one is fundamentally answerable to others is a behaviour by which people pay respect to the independence of others, and for this reason implies not to interfere with the actions of others. This form of responsibility is required from every member of the moral community.

Beyond fundamental answerability, moral sensitivity can involve, and in case of peacekeepers, should involve another form of responsibility, the (active) helping collaboration with others, that is, caring behaviour. In virtue of their exemplary behaviour, peacekeepers are expected to care for others in order to be able to build a moral community as required of them.

According to Levine, caring means listening to the desires and needs of others and acting in their interest without being specifically requested to do so, in an entirely active fashion.[40] Although this sort of caring behaviour is fundamental: it can be found among members of a family, for example, it seems to be too demanding in the context of the relationship between peacekeepers and the locals. Caring behaviour should mainly consist in doing what's morally right and setting a morally good example for the locals by it.

Fundamental answerability and caring in the sense of setting a good example are two forms of moral responsibility which make the difference between peacekeepers' moral autonomy and people's moral autonomy. The difference lies in that while peacekeepers' behaviour has a more or less active moral impact on others, people's behaviour in general has a rather passive impact (even though both may have an impact on others). This difference can be stressed further.

It can be claimed that taking care for others by setting a good example in order to build a moral community is a duty for peacekeepers while it is merely supererogatory for people in general. According to Gregory Mellema, '[t]he concept of supererogation is standardly defined in the literature in a way roughly similar to the following: The performance of an act qualifies supererogatory if and only if: (1) The agent has no moral duty or obligation to perform it; (2) The performance of the act is morally praiseworthy; and (3) The omission of the act is not morally blameworthy'.[41] On the basis of the definition, we can say that every person – peacekeeper or otherwise – is admitted to have the duty to 'respect the human rights of others to not being killed'. Peacekeepers, however, because of their professional autonomy, have at least another duty, that is, that of 'building a moral community'. The man of the street does not have that second duty, and if they perform an act which helps advance the building of a moral community that is viewed as supererogatory. Such an act deserves credit if carried out, while it is not reproachable if omitted.

This distinction is plausible in general, and also regarding peacekeepers' professional and moral autonomy. According to Fichte, someone setting a good example in moral matters is not a behaviour they would not pursue at other times; it is a person's normal behaviour and basic moral attitude that counts. Hence, if we accept that people must observe the

---

39 Stephen Darwall, 'The Moral Obligation: Form and Substance' *Proceedings of the Aristotelian Society* 110, April (2010), 31–33.

40 Cf. Levine, *The Morality of Peacekeeping*, 59–66.

41 Gregory Mellema, *Beyond the Call of Duty: Supererogation, Obligation, and Offense* (New York: State University of New York Press, 1991), 17.

rules of moral autonomy – which Fichte thinks they must – then every person (not just peacekeepers) can be expected to set a good example for others.[42] Fichte, however, later ads that ordinary people, through a 'social contract', confer the duty to 'fashion everyone morally'[43] to a special social institution, that is, to the moral teachers; which, for Fichte, is the Church. Supposing this social institution did not exist, everybody would have the duty to 'fashion everyone morally'. But as the social institution of moral teachers actually exists, in one way or another, such moral teachers have to do (or at least try to do) what's morally right in all cases, and by this, they must set a good example for others.[44]

From this perspective, peacekeeping is an international social institution. 'Building a moral community abroad' would, of course, be everyone's duty if it was not for the international institution. However, people confer – through an international social contract – their duty to 'build a moral community abroad' directly on an international social institution and – indirectly – on the members of that institution, that is, peacekeepers. So as long as peacekeepers are not only soldiers but peacekeepers as well, it is their professional and moral duty to build a moral community abroad. This also means that peacekeepers must shoulder an additional duty, which they receive in two steps. That duty is first conferred by people on an international institution, which in turn confers it on peacekeepers as part of their professional duty.

This gives peacekeepers a moral duty ordinary people do not have; therefore peacekeepers' moral autonomy is extended in relation to that of ordinary people (similarly to the moral autonomy of moral teachers being extended in relation to that of ordinary people). In other words, the extended moral autonomy of peacekeepers derives from the fact that they have more duty than ordinary people, and this is possible because ordinary people confer their duty to 'build a moral community abroad' on an international social institution and the members thereof.

So is peacekeepers' moral autonomy excluded by military authority after all? I have said that building a moral community is a part of peacekeepers' professional autonomy and, moreover, for this reason, peacekeepers enjoy specially extended moral autonomy. These are, however, supported by the hierarchy of peacekeepers, which is a form of military authority. So we can conclude that peacekeepers' moral autonomy is not at all ruled out by military authority. On the contrary, as military authority is part of peacekeepers' professional autonomy and it enables peacekeepers to have an extended moral autonomy, military authority actually supports the moral autonomy of peacekeepers.

Conclusion

Paolo Tripodi reminds us how the moral autonomy of peacekeepers is essential in forestalling human rights catastrophes such as the genocides that took place in Rwanda and Srebrenica. In this paper, I looked into the professional and moral autonomy of peacekeepers in relation to military authority to answer the question whether peacekeepers' autonomy – professional

42 Fichte, *System of Ethics*, 298–299, 301–302.
43 Ibid. 329.
44 Ibid. 329–330.

and moral – is ruled out by military authority to better understand peacekeepers' behaviour, that is, their options and choices in difficult situations. The professional autonomy of peacekeepers is threefold: it pertains to defending civilians against violence (keeping negative peace); building the moral community (keeping positive peace); and their role in an international military hierarchy. Their role as builders of the moral community calls for and informs their moral autonomy, which they rely on in relation to people. The conclusion follows that neither their professional nor their moral autonomy is ruled out by the effect of military authority: their moral autonomy is in fact supported by it.

References

Bellamy, Alex J and Paul D Williams, *Understanding Peacekeeping*. Cambridge: Polity Press, 2010.

Boda, Mihály: 'Soldiers' Autonomy and Military Authority', in *Military Ethics and Leadership, ed.* by Peter Olsthoorn. Leiden: Brill Nijhoff, 2017, 150–167. DOI: https://doi.org/10.1163/9789004339590_008

Charter of the United Nations. Online: https://www.un.org/en/about-us/un-charter

Darwall, Stephen, 'The Moral Obligation: Form and Substance'. *Proceedings of the Aristotelian Society* 110, April (2010), 31–46. DOI: https://doi.org/10.1111/j.1467-9264.2010.00278.x

Fichte, Johann Gottlieb, *System of Ethics*. Cambridge: Cambridge University Press, 2005. DOI: https://doi.org/10.1017/CBO9780511806612

Galtung, Johan, 'An Editorial' *Journal of Peace Research* 1, no 1 (1964), 1–4.

Galtung, Johan, 'Violence, Peace, and Peace Research'. *Journal of Peace Research* 6, no 3 (1969), 167–191. DOI: https://doi.org/10.1177/002234336900600301

Galtung, Johan, 'Cultural Violence'. *Journal of Peace Research* 27, no 3 (1990), 291–305. DOI: https://doi.org/10.1177/0022343390027003005

Greenwood, Ernest, 'Attributes of a Profession'. *Social Work* 2, no 2 (1957), 45–55.

Huntington, Samuel P, *The Soldier and the State*. Cambridge, MA and London, England: The Belknap Press of Harvard University Press, 1998.

Rachels, James, 'God and Human Attitudes'. *Religious Studies* 7, no 4 (1971), 325–337. DOI: https://doi.org/10.1017/S0034412500000391

Levine, David H, *The Morality of Peacekeeping*. Edinburgh: Edinburgh University Press, 2014.

Kant, Immaneul, *Groundwork of the Metaphysics of Moral*. Cambridge: Cambridge University Press, 1998. DOI: https://doi.org/10.1017/CBO9780511809590

Korsgaard, Christine, 'Creating the Kingdom of Ends: Reciprocity and Responsibility in Personal Relations', in *Creating the Kingdom of End*. Cambridge: Cambridge University Press, 2000, 188–221. DOI: https://doi.org/10.1017/CBO9781139174503.008

Mellema, Gregory, *Beyond the Call of Duty: Supererogation, Obligation, and Offense*. New York: State University of New York Press, 1991.

Olsthoorn, Peter, *Military Ethics and Virtues*. London and New York: Routledge, 2011. DOI: https://doi.org/10.4324/9780203840825

Pfaff, Tony, *Peacekeeping and the Just War Tradition*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000.

Richardson, R, D Verweij and D Winslow, 'Moral Fitness for Peace Operations'. *Journal of Political and Military Sociology* 32, no 1 (2004), 99–113.

Spearin, Christopher, 'Between Public Peacekeepers and Private Forces: Can there be a Third Way?' *International Peacekeeping* 12, no 2 (2005), 240–252. DOI: https://doi.org/10.1080/13533310500066529

Tripodi, Paolo, 'Peacekeepers, Moral Autonomy and the Use of Force'. *Journal of Military Ethics* 5, no 3 (2006), 214–232. DOI: https://doi.org/10.1080/15027570600913338

Walzer, Michael, *Just and Unjust Wars*. New York: Basic Books, 2006.

Wolff, Robert Paul, *In Defense of Anarchism*. Berkeley and Los Angeles, CA: University of California Press, 1998.

AARMS Vol. 19, No. 2 (2020) 79–91.

10.32565/aarms.2020.2.6

Leadership Responsibilities in Information Security Awareness Development

Balázs KÁRÁSZ[1] – Csaba KOLLÁR[2]

This paper aims to introduce the main aspects arising in the organisational context related to leadership roles when information security awareness is being engineered and developed according to purposes set within. Achieving these development purposes is connected to the commanding function of leadership, while being influenced by key human risk factors such as: leadership commitment and example setting, leadership quality, the state of being motivated and above all, the ability of responsible decision-making on a professional basis. In order to improve the effectiveness of putting the implementation into practice, a methodological toolset needs to be elaborated for the disposal of the leader, thanks to which, besides taking on a transactional leadership style and a cyclic program management, the continuous monitoring and tailoring to the organisation of the development purposes all become facilitated.

Keywords: *information security, security awareness, manager communication, leadership commitment, leadership skillset*

Introduction and research details

Due to current threats on information society, as well as the growing need of dynamical development in safety culture, it became pronouncedly important for organisations to protect information as an intangible asset of high value, as well as the information systems and information infrastructures affected. Despite applying all sorts of countermeasures that have a technical approach, human risk factors highly influence their effectiveness in practice. Therefore, the psychological side also needs to be assessed, which, in the organisational context, can be intervened by employees in key positions, including leadership and management level, but also non-leadership levels of technical departments.

[1] PhD student, University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering, e-mail: karaszb@gmail.com; ORCID: https://orcid.org/0000-0003-2065-4928

[2] PhD, Lecturer, University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering, e-mail: kollar.csaba@uni-nke.hu; ORCID: https://orcid.org/0000-0002-0981-2385

Scientific research problem

Based on the above-mentioned issues, the following question arises: how can organisational information security awareness be, and how could leaders effectively manage human risks when reacting to cyber threats at leadership level by applying civil methods of HR and risk management, as well as security awareness development?

Research objective

The objective of this research is to determine the roles of leadership within the concept on how organisational information security awareness can be outlined and defined, through analysing the available literature on the functions of leadership. As a second step, the research aims to emphasise major responsibilities of leaders, which can be effectuated as reactions to the expected effects of human risk factors. The expected results are targeted to further researches in military context.

Research methods

The authors used theoretical and empirical research techniques, partly with the method of synthesis. Related scientific literature from Hungary, as well as abroad, from professionals of both technical and management background are widely mapped and elaborated, in terms of review papers, monographs, conference publications, laws and internet sources.

Literature review

In this section, the authors enlist concepts on the role and functions of leadership in general, besides introducing how the awareness on leadership level influences the information security awareness within organisational processes. The authors found that literature from the past decades can still be considered the fundaments of the theoretic review of the topic. Concerning the professional proposals discussed in the *Conclusion and outlook* section, more up-to-date publications are cited, which support the necessity of forward-pointing in the practical implementation of the theory.

Organisational information security awareness

The conceptual foundation for organisational information security awareness has been established already 20 years ago, in order to emphasise the role of motivation within security awareness education programs.[3] In his widely cited paper, Siponen claims that

[3] Mikko T Siponen, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security* 8, no 1 (2000), 31–41.

the creation of an information security awareness program requires a systematic approach, dividing awareness into framework and content parts, where the framework should be developed in a systematic and structural manner, with the help of appropriate standards (reference in section *Standardisation of security management*). If end-user internalisation of the security guidelines is the objective, the content part of the awareness program must also come under serious consideration. It is argued that all approaches affecting the behaviour of the user (increasing awareness and so on) should satisfy the requirements of behavioural theories and provide answers for employees acting as end-users in the organisation, letting them observe the reasons for following security guidelines. In this respect, a wide variety of persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions have been established so far. The use of a persuasion strategy is a necessary condition for giving any strategy for increasing awareness a solid basis and for achieving user commitment.

Functions of leadership

Up to current times, data has evolved as the biggest asset of any organisation, since each one of them has to deal with data. A substantial part of data is also personal, belonging therefore to the affected person at the same time. It is crucial to mention the importance of the responsibility of the organisation managing personal data to elaborate the suitable data protection measures and security regulatory system, as well as the sustainable compliance to the related regulations. In favour of full data privacy and information security, it is not enough to introduce internal rules, technological controls, follow-up logs and do back testing, all these measures must be supported by corporate culture itself, enabling the company to continue and apply practices of data management based on awareness.

This aspect originates from an effective setup and continuous improvement of the personnel development system. Such systems assign a declared role to training and career guidance, and when discussing both knowledge management and career planning, functions of leadership play the most significant role.[4] It includes various methods, forms of learning, amongst others lecturing, negotiation, printed material, digital solutions, behaviour challenging methods and techniques of practice and feedback.

A personnel development system, including training of experts and specialists in addition to the training of leaders, can also act as an answer to the recent requirements of the personality of the leader and how they fill their part, such as empathy, encouragement, recognition and inspiration. According to the classic school of Henri Fayol, the functions of leadership can be summarised as follows: planning, organising, commanding, coordinating and controlling.[5] Moreover, organisational communication has got similar functions[6] such

[4] Mártonné Karoliny and József Poór (eds), *Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások* (Budapest: Wolters Kluwer, 2015), 365–383.

[5] József Roóz and Balázs Heidrich (eds), *Vállalati gazdaságtan és menedzsment alapjai* (Budapest: Budapesti Gazdasági Főiskola, 2013); Henri Fayol, *General and Industrial Management* (Martino Publishing, 2013), 142.

[6] Károly Balaton, Gyula Bakacsi, Miklós Dobák and Antal Máriás, *Vezetés-Szervezés II.* (Budapest: Aula, 1991), 106.

as emotional (social needs), motivational (mediated by communication), informative (in favour of integrity and accuracy) and controlling (based on the organisation structure).

Leadership awareness

When performing the enhancement of the information security awareness, the strengthening of engagement should be brought through first at leadership level and only secondly at employee level. This can also be facilitated conceptually by being embedded into a complex development strategy. According to the basic risk management methodology of investigating precedents and detection of patterns and trends, if translated to operational context, this would mean that targeted courses should focus on case studies and the analysis of artificial cyberattacks and social engineering attacks organised in realistic environment. This is also the fundamental research result of Wilson and Hash[7] in whose paper, concepts of awareness, training and education are defined in order to outline principles to build up a security awareness training program. According to the direction they show, when designing related education material, the most important factor to consider is the utilisation rate of the program and material from the point of view of implementation possibilities and the significant role of follow-up.

In the context of security, knowing the most possible ways of carrying out attacks of either physical or cyber nature can substantially reduce information leakage and unauthorised use, while in parallel, it can increase the stability of State institutions and the safety of actors in society and economy.[8] After a thoroughly structured introduction to security risks found in the thesis of Chestnut,[9] the emphasis is put on the real impact of the mistakes happened or made. According to various methodologies browsed and analysed to discover administrative and management responsibilities with direct impact on human risk factors influencing the information security level, economically grounded proposals are formulated to mitigate risks. These proposals have one common inference to be drawn, which is an emphasised importance of back testing and controlled supervision.

Information security engineering

In this section, the authors collect technical aspects of security management including related standardised concepts, physical/human and information security risks and countermeasures, underlining the role of leadership commitment.

---

7 Mark Wilson and Joan Hash, *Building an Information Technology Security Awareness and Training Program* (Washington, D.C.: National Institute of Standards and Technology, U.S. Government Printing Office, 2003).

8 Veronika Deák, 'Biztonságtudatosság az információs környezetben', *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

9 Jacqueline Annette Chestnut, *Assessing the Impact of Human Error in Information Security Incidents* (Mississippi, MI: Bell & Howell Information and Learning Company, 2000).

Standardisation of security management

In favour of establishing a general framework for ways of information security engineering, a possible solution is to implement an information security management system (further referred to as ISMS) within the organisation based on a certified standard. ISO 27000 is a collection of internationally acknowledged and applied standards, which introduces basic directions, according to which, operating an ISMS ensures the manageable safety and security.

Information security (not to be mistaken for IT security – being a subcategory of information security in the context used by this paper) must be interpreted only in the way of the effectuation of *confidentiality, integrity, and availability* (further referred to as C.I.A. triad) together and under all circumstances according to the following reasoning:

1. Confidentiality: no one without authorisation can access any part of data or information (often regulated by extensive access management), contrary to *availability*.
2. Integrity: the data or information is genuinely authentic and undeniable, while also no changes are performed on its original state (also proven by *confidentiality*).
3. Availability: in case of properly functioning information security, the (*intact*) data and information can be accessed by those disposing of authorisation at any time.

According to recent summary data, Hungary is no 17 out of 170 countries in having obtained the most ISO IEC 27 001 certifications in number as of 31 December 2018.[10]

The PDCA model is used wide-spread and applied in ISO standard-families, including the group ISO 27000 dedicated to information security. Furthermore, the model can be used in the development of information security awareness of leaders and even executives, although not in its original form. It serves, however, as a suitable fundament to be completed by further elements – especially envisaging purposes – and this way becoming an effective consultancy and coaching method at the disposal of business coaches working on executive areas.[11]

Security risk management

ISMSs need to be established in the organisation including a comprehensive mapping, identification, assessment, analysis, management, monitoring and review of risks, in harmony with the PDCA cycle used widely in all management system related standards. Physical security issues and risks deriving from information technology background should not be handled separately. Some examples are collected here to show the importance of the risk integrity when discussing about cyber protection at workplace:

- Welcoming external persons: guests are often left alone or without surveillance in office areas or are entering meeting rooms when confidential documents from previous meetings are not yet put away. Also combined with either the interruption of the

[10] Certification & Conformity, 'The ISO Survey 2018'.

[11] Csaba Kollár, 'Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével', *Magyar Coachszemle* 5, no 3 (2016).

entrance security system, losing the access card or lending them to guests (that is, unauthorised access is made possible to even protected areas).
- Leak of information: informal discussions in the canteen, in the elevator or not adapting adequately to the clean desk and clean display policy can lead to unauthorised persons overhearing confidential information. Suspicious calls via telephone can also be categorised here in some cases.
- Unauthorised access: originating from either social engineering (psychological manipulation) or inherent and unintentionally present human risk factors such as inadvertence, authentication data is leaked and used by unauthorised persons to access the information system for personal use.
- Protection against malicious software: both sources (for example emails, websites, downloaded programs) and file names can be suspicious, but without regularly updating antivirus programs or by attaching data media of unknown origin unawareness can mean a serious threat to confidential information.
- Data breach: when considering the worst scenarios, the stored data can be destroyed, seriously damaged, or locked down by blackmail viruses. Without a successful external attack, data breach can be suffered by the company if an information device is lost, upon which corporate data can be accessed.

Seeing the above-mentioned examples, it can be clearly understood that the common origin of these can be found in the human behaviour,[12] out of which, sanctioning can only cover intentional or unintentional but eliminable actions or happenings according to the following overview of several exemplary cases:
- Loss or damage caused to physical device (such as mobile phone): beyond the book value of the device, damages should be estimated according to the C.I.A. triad of the stored or accessed dataset – especially when information is compromised.
- Default in reporting an incident: either technically, connected to the systems, devices used to access corporate information (for instance noticed failure message or unusual operation method), or connected to physical and human security – damages caused by the late or defaulted report should be estimated.
- Not intended (that is, not work-related) use of information infrastructure: unsubstantiated personal use (music, movie, game download), use of illegal software, changing centrally controlled settings can all be continuously monitored by log, email check and so on. Damages are to be assessed according to the Criminal Code, too.
- Ignoration of information security regulation measures: damages should be assessed by taking into consideration material, reputation, operation expenses, as well as legal consequences, client dissatisfaction and business continuity issues.

Furthermore, the enforcement of various sanctions also plays a significant role in key leadership responsibilities managing information security issues, which is placed into organisational context in section *Using specific leadership skills*.

[12] Balázs Kárász, 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata', *Biztonságtudományi Szemle* 2, no 2 (2020).

Leadership commitment

In harmony with Clause 5 of ISO 27001 standard (and appearing in the High-Level Structure of ISO standards): 'Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.' (ISO, 2013) Concerning all security management professional areas, the crucial question is – beyond its transparency – how leadership commitment can be demonstrated. Security therefore should be engineered at top-level within an organisation, just as we see that sanctioning and regulation measures can also be implemented by management.[13] A possible step forward is the subordination of the responsible department(s) unto the managing director/chief executive officer, as it can be seen at organisational structures of, for example, several large enterprises operating critical infrastructures.

When discussing about lower employee levels, awareness here originates and is principally based on the awareness level of the management. Development programs such as training, personal coaching and consulting that aim the improvement of security awareness should therefore include all hierarchic levels.[14] Commitment can be grounded by turning the focus of top management development to risks expressed in quantified ways as well as client relationships (in terms of the commitment towards handling personal data of customers), while the shareholder value should also be emphasised. If the leader makes decisions observing accurately collected and processed information, besides being highly committed to security measures, even responsibility related to the moment of decision can be decreased significantly.

Leadership responsibilities in information security

Key leadership skills in shaping security management include both technical (including business and professional) competences and interpersonal skills (mostly communication-related). In this section, the authors also put emphasis on competences influencing the enhancement of organisational security awareness, which are related principally to leaders.

Using technical and business skills

Visibility is the first attribute that must be ensured in an organisation in the sense that if an attack surface or its part is not visible, no measures will be able to maintain security. Therefore, all assets and all attack vectors must be mapped and accurately understood in order to mitigate breach risk. Also, the exact timing of a cyberattack is hardly known, which is the reason for applying methods, suitable tools, processes and models predicting risks according to breach scenarios. This will create a modern risk approach to cybersecurity, which has three main characteristics in being *predictive, proactive, and preventive.* Not

[13] Balázs Kárász and Imre Négyesi, 'Information Security Responsibilities of Critical Infrastructures in the Aspect of Human Risk Factors', *Hadtudományi Szemle* 13, no 3 (2020).

[14] Kárász, 'Az információbiztonság'.

to forget the third aspect, that is, recognising all kinds of threats (including password issues, misconfigurations, phishing, ransomware, encryption issues, and so on) against which protection should be established. Proven that visibility, prediction and full-scope recognition of threats are in function, appropriate response can be carried out overall.

Regarding a full functioning alert system, prioritisation of vulnerabilities becomes a must, based on the extent of business criticalness of all elements affected, such as assets, threats, controls and exposure, in order to be able to focus on tasks of high priority. When facing problems, it is response time that will influence the impact of the threat; therefore, among possible ways of finding the solution, natural language search across the personal network is at hand.

All in all, strong cyber hygiene should be built and practiced by the leader of technical responsibility. For example, multifactor authentication is an efficient way to reinforce security posture, which mitigates cyberattacks connected to compromised user credentials.[15] Investing in technologies that enable strong password creation is highly recommended, since systems can be easily defended against brute force attack techniques with the help of them. Also, the elaboration of a continuously controlled and efficiently functioning access management is inevitable. When determining the regulations for each user within the organisation, the 'principle of least-privileged access' should prevail, for instance a project engineer does not need access to an organisation's financial data and a finance manager does not need to access the organisation's production code repository. Building a strong identity and access management system begins with having a single trustworthy reference of all users and their roles within an organisation.[16] These are considered the fundaments of human security management.

Using interpersonal and communication skills

Leadership can be defined as the process to influence (that is, motivate) others to follow rules and procedures (including compliance to standards) to achieve objectives, whereas leadership style refers to the characteristics of the leader to monitor and control their followers.[17] Here it can be seen that interpersonal skills are key to efficient communication and reaching well-defined objectives within the organisations.

Taking a closer look on cyber risks, in order to manage them, not exclusively the leaders of security-related departments but all leaders in the organisation must also leverage colleagues. The best way to encourage employees to participate in security programs is to use gamification and make them win incentives, rewards and awards for completing security related tasks. Gamification is a process where game mechanisms are integrated into platforms and programs, which traditionally would not consist of such elements,[18] or it can be defined from the perspective of motivation, where gamification utilises game elements in order to encourage users and communities by commitment to do activities that they are not necessarily willing to take up under different circumstances. From our point

[15] Kárász and Négyesi, 'Information Security Responsibilities'.
[16] World Economic Forum, *The Cybersecurity Guide for Leaders in Today's Digital World* (Geneva, 2019), 22.
[17] James MacGregor Burns, *Leadership* (New York: Harper and Row, 1978), 530.
[18] Christopher Swan, 'Gamification: A New Way to Shape Behavior', *Communication World* 29, no 3 (2012).

of view, gamification therefore is a useful tool to build commitment to security measures at all levels of the organisation.

The other aspect to be mentioned among communication skills is reporting to the board as a security/IT professional leader. Here lies a crucial point to break through when communicating business-level risks in a quantified way, in terms of metrics, indicators and everything translated to cash. When convincing them of a necessary cyber protection investment, leaders must quantify the security posture of the organisation to the board or top management to get their buy-in for the initiatives and focus on the trade-off. Leaders should possess and develop for themselves a strong business acumen to translate the technical risks into business strategy risks, so that a non-technical audience can understand the potential threats to business operations.

Using specific leadership skills

When discussing skills that belong exclusively to leaders either by personality or by responsibility, the problems should be divided into two aspects, just as we did above, the first being the category of leaders being responsible for a security department. In this case, as we already agreed, the leader should avoid technical approach and language and start thinking like a business leader by ensuring transparent communication and building trust in the organisation. With the help of the leader paying attention and making efforts to develop critical thinking, creativity and problem-solving skills within the organisation, not only the cybersecurity team but the entire personnel can benefit from it thanks to their mindset being challenged and finally changed. Beyond all technical (hard) and interpersonal (soft) qualities – even with the lack of them which can be easily completed by learning – every leader in the organisation has to make efforts in aligning to and complying with security regulations. One side of this coin is already mentioned as the concept of leadership commitment. It is an attribute which can be visible and easily demonstrated, for example, in legal and regulatory context.

The other side of possessing an affinity in example setting as a leader cannot be put away, since as a non-technical leader, it supports the authenticity of commitment, while as a technical leader, a culture of cybersecurity can be created on this basis. Either perceived in the aspect of interpersonal relations, that is, drawing the attention of employees to the importance of complying with security regulations, or manifested connected to technical knowledge, for instance knowing the most modern way of protecting information infrastructure, authentication credentials and so on, the leader has to achieve the goal that the employees will follow these habits by their own understanding. Especially when discussing about the access to domains handling sensitive data, leaders are exposed from the point of view of their example setting, in order to make themselves able to align with security guidelines. Moreover, the leader exclusively disposes of the power to enforce the compliance with regulations of the employees with sanctions. Not to be forgot, we have to mention the special characteristic of example setting, being especially important in security areas, where, on the contrary, it is not the exclusive responsibility of the leader, but equally of all colleagues throughout the department.

To have a more global outlook on the above-mentioned questions, fostering both internal and external partnership (from the view of the organisation) is an important recommendation, since threats and information security innovations share a dynamic nature, and therefore a better global systematic architecture should be built on cyber protection.[19] The network behind all similar kinds of potential initiatives is based on the cooperation and acquaintances that leaders can support. This way, more effective platforms can be created to facilitate information and knowledge sharing within and across industrial segments.

Transactional and transformational leadership

According to the study of Humaidi and Balakrishnan,[20] which focuses on the following two styles of leadership described partly by Burns[21] and Bass:[22] transformational and transactional leadership, we can suppose that these two well-described styles differ fundamentally and can therefore have significant impact on shaping both information security engineering culture and awareness within an organisation. Leaders who are engaged with their team members and motivate them are said to have the characteristics of a transformational leader, while on the other hand, a transactional leader is somebody who as a leader operates within the existing system or culture and strictly controls how policies are implemented in the organisation.

Many leadership studies already have pointed out that both of the leadership styles influence work performance overall significantly. The three constructs of awareness that serve as a second dimension of the study are threat severity (as an externally determined factor), susceptibility (which can be considered an interior human risk factor) and security-countermeasure awareness (a retaining factor affecting human behaviour). Although the above and following statements are focused on security/IT professional or department leaders, we must take into consideration – as stated before – that all measures to the benefit of operating an effective information security should be expanded to circles beyond security and IT leaders and include every leader of the organisation, plus, through them, all employees.

Synthesising the two key skills of section *Using specific leadership skills*, example setting and commitment, with the above described leadership styles, this paper intends to add that example setting on leadership level makes up an inseparable part of transactional leadership, while commitment, regarding its basic characteristics, is an attribute mainly of the transformational leadership style. This becomes even more meaningful if we take into consideration the quantitative research results published in the cited paper,[23] which show that transactional leadership has significant direct and indirect impact on the user's policy compliance behaviour through threat severity awareness and in parallel, security-

---

19 World Economic Forum, *The Cybersecurity Guide*, 22.

20 Norshima Humaidi and Vimala Balakrishnan, 'Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness', *International Journal of Information and Education Technology* 5, no 4 (2015), 311–318.

21 Burns, *Leadership*.

22 Bernard M Bass, *Leadership and Performance beyond Expectation* (New York: The Free Press, 1985), 256.

23 Humaidi and Balakrishnan, 'Leadership Styles and Information Security'.

countermeasure awareness, while transformational leadership turned out to have no indirect effect on the user's behaviour.

The reason behind the transactional leadership being more resultful compared to transformational leadership, especially when related to information security compliance behaviour, may be found in higher transparency in terms of clearly showing rewards and punishments. When transactional leadership is exercised strongly by applying rewards depending on following regulations properly and punishment of not complying employees, situations can come across, with the help of which, higher awareness level is formed, and therefore, information security compliance behaviour may also be ameliorated.

Conclusion and outlook

We attempt to find the shared section of all above-mentioned aspects of leadership functions and styles, security awareness, commitment and example setting, key skills – in order to locate leadership example setting within the concept of organisational information security awareness.

Organising security awareness programs alone does not result in realising security awareness itself, since it is inevitable to entirely process the information needed for design, achieve full leadership commitment and example setting, as well as undertaking corrections after the realisation of the program according to the related feedbacks, in order to implement an effective and successful personnel development system. The development of information security awareness of leaders and executives is one of the most crucially important fields of consultancy and coaching services of the beginning of the 21st century, especially taking into consideration that the leadership attitude towards security is not an autotelic responsibility, but has a significant impact on the financial situation and safety of the organisation. The improvement of the company nowadays cannot be separated from the information security awareness of the employees, including executives as well, which also has to involve the recognition and successful defence against social engineering attacks.[24]

Example setting cannot be interpreted as a leadership attribute or skill standing alone, since it can be accomplished in the field of responsibly taking main leadership tasks and communication. In leadership positions within any organisation, the following qualities have to be in balance to effectuate example setting: goal setting, decision-making, change management, delegation, assessment, control, feedback, problem management in terms of correction application, conflict handling, negotiation techniques, hierarchy acumen and creativity.[25] Out of all these aspects, control is necessary to be considered the only function that cannot be delegated, since it originates from the responsibility and position of the leader. In the context of the network of human risk factors in information security, specific leadership skills play a substantial role in shaping relations, that is, reactions of employees to human and IT-based social engineering attacks.[26] Most likely of all, example setting represents the outlined role of the control function of leadership in the effectuation of high

[24] Kollár, 'Az információbiztonság-tudatosság fejlesztése'.
[25] Daniel Eppling and Laurent Magnien, *Leadership in Action – What Great Managers Really Do*, 222.
[26] Kárász, 'Az információbiztonság'.

level information security awareness, since its 'target audience' cannot be limited to direct subordinates, but extended to indirect subordinates, colleagues on same or lower hierarchic level, as well as a higher level leader, thus potentially, the entire organisation.

In order to make it possible to realise an effective control function in leadership, independence of security departments needs to be assured, since when operating as a local department, it did not dispose of enough power to enforce the necessary guidelines or steps.[27] This is the reason for our proposal towards organisations that security departments should be centralised – even as a service provider within large organisations – and assigned under direct control of top management. This organisational structure can effectively function based on leadership commitment at top levels, which will escalate then to all hierarchic levels in the organisation.

Summary

This research collected the most recent international literature concepts as well as standards concerning the role and responsibilities of leadership in the field of information security awareness development. Beyond the technical capabilities, personality and a wide scope of skills of the leader have a significant impact on shaping human behaviour, that is, the awareness throughout the entire organisation. The research also successfully defined the concept of organisational security awareness, and all results build up a useful basis for continuing research in the topic of measuring effectiveness of development steps and processes, also suggested to be considered in military engineering context. The results will be used to widen the network of human risk factors in information security by the aspect of specific leadership skills and responsibilities.

References

Balaton, Károly, Gyula Bakacsi, Miklós Dobák and Antal Máriás (eds), *Vezetés-Szervezés II*. Budapest: Aula, 1991.

Bass, Bernard M, *Leadership and Performance beyond Expectation*. New York: The Free Press, 1985.

Burns, James MacGregor, *Leadership*. New York: Harper and Row, 1978.

Certification & Conformity, 'The ISO Survey 2018'. Online: www.iso.org/the-iso-survey.html

Chestnut, Jacqueline Annette, *Assessing the Impact of Human Error in Information Security Incidents*. Mississippi, MI: Bell & Howell Information and Learning Company, 2000.

Deák, Veronika, 'Biztonságtudatosság az információs környezetben'. *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

Eppling, Daniel and Laurent Magnien, *Leadership in Action – What Great Managers Really Do*.

Fayol, Henri, *General and Industrial Management*. Martino Publishing, 2013.

[27] Viktor Spilák and Zsolt Tibor Kosztyán, 'Szervezeti kultúra, vezetői szerepek, az információbiztonság és a felhőalapú megoldások kapcsolata', *Vezetéstudomány* 50, no 7–8 (2019), 70–87.

Humaidi, Norshima and Vimala Balakrishnan, 'Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness'. *International Journal of Information and Education Technology* 5, no 4 (2015), 311–318. DOI: https://doi.org/10.7763/IJIET.2015.V5.522

Kárász, Balázs, 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata'. *Biztonságtudományi Szemle* 2, no 2 (2020), 57–68.

Kárász, Balázs and Imre Négyesi, 'Information Security Responsibilities of Critical (Information) Infrastructures in the Aspect of Human Risk Factors'. *Hadtudományi Szemle* 13, no 3 (2020). DOI: https://doi.org/10.32563/hsz.2020.3.6

Karoliny Mártonné and József Poór (eds.), *Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások*. Budapest: Wolters Kluwer, 2015, 365–383.

Kollár, Csaba, 'Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével'. *Magyar Coachszemle* 5, no 3 (2016).

Roóz, József and Balázs Heidrich (eds), *Vállalati gazdaságtan és menedzsment alapjai*. Budapest: Budapesti Gazdasági Főiskola, 2013.

Siponen, Mikko T, 'A conceptual foundation for organizational information security awareness'. *Information Management & Computer Security* 8, no 1 (2000), 31–41. DOI: https://doi.org/10.1108/09685220010371394

Spilák, Viktor and Zsolt Tibor Kosztyán, 'Szervezeti kultúra, vezetői szerepek, az információbiztonság és a felhőalapú megoldások kapcsolata'. *Vezetéstudomány* 50, no 7–8 (2019), 70–87. DOI: https://doi.org/10.14267/VEZTUD.2019.07.07

Swan, Christopher, 'Gamification: A New Way to Shape Behavior'. *Communication World* 29, no 3 (2012).

Wilson, Mark and Joan Hash, *Building an Information Technology Security Awareness and Training Program*. Washington, D.C.: National Institute of Standards and Technology, U.S. Government Printing Office, 2003. DOI: https://doi.org/10.6028/NIST.SP.800-50

World Economic Forum, *The Cybersecurity Guide for Leaders in Today's Digital World*. Geneva, 2019. Online: www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf

Praesent ad accumsan velit
John Doe

I Lorem ipsum dolor sit amet: Consectetur adipiscing elit

Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.[1] Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi aliquip ex commodo consequat . . .

A Duis aute irure dolor in reprehenderit[2]

In voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum . . .

(i) Sed ut perspiciatis unde omnis

Iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae sunt . . .

a) Nemo enim ipsam voluptatem

Quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt . . .

b) Integer condimentum mauris ut lacus facilisis iaculis

Praesent sed fermentum neque. Proin porta sagittis tortor sit amet luctus. Suspendisse ut gravida sem. Quisque vestibulum et neque condimentum, vitae efficitur dolor pretium . . .

(ii) Neque porro quisquam est

Qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem . . .

B Suspendisse vulputate consectetur nunc vitae suscipit

Quisque efficitur vestibulum pellentesque. Phasellus tempor massa purus, vitae viverra orci ultricies at. Morbi nibh nisi, molestie id rutrum eu, efficitur ut arcu . . .

II Nunc nec ex interdum, blandit lacus imperdiet, bibendum ex

Nullam lobortis, nulla sed accumsan ornare, est arcu scelerisque nisi, sed malesuada mi turpis in purus. Morbi scelerisque dui fringilla volutpat ultricies . . .

[1] Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur?
[2] Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Quotations
Punctuation follows the closing quotation mark, unless the whole sentence is a quotation. The footnote marker comes last. If you add emphasis to a quotation, put '(emphasis added)' into the footnote.
Incorporate quotations of up to five lines into the text, within single quotation marks. Quotations longer than five lines should be in indented paragraphs; leave additional line spacing above and below indented quotes. For quotations within short quotations, use double quotation marks.

Citation
Either directly or indirectly citing any source, put the reference in footnote. Do not use endnotes.

David Hume, in the section Of the Origin of Our Ideas of *A Treatise of Human Nature*, wrote that

> All the perceptions of the human mind resolve themselves into two distinct kinds, which I shall call *impressions* and *ideas*. The difference betwixt these consists in the degrees of force and liveliness, with which they strike upon the mind, and make their way into our thought or consciousness. Those perceptions, which enter with most force and violence, we may name impressions: and under this name I comprehend all our sensations, passions and emotions, as they make their first appearance in the soul.[1]

Shortly after this definition, starting to prove the precedency of our impressions or ideas,[2] he put that 'our ideas are images of our impressions, so we can form *secondary ideas*, which are *images* of the primary'.[2] Arguing that […]

[1] David Hume, *A Treatise of Human Nature* (London: John Noon, 1739), 1.
[2] Ibid. 6 (emphasis added).

Books:

First note:
[1] John Dewey, *Logic: The Theory of Inquiry* (New York: Henry Holt, 1938).
[2] Jean-Pierre Changeux and Paul Ricoeur, *Ce qui nous fait penser – la nature et la règle* (Paris: Odile Jacob, 1998), 14–34.
[3] Klaus Wettig (ed.), *»Ich wohne nicht in stehenden Gewässern«. Der politische Günter Grass* (Göttingen: Steidl, 2018), 120–21.
[4] Christoph E Düllmann et alii (eds), *Nuclear Physics A: Special Issue on Superheavy Elements* (Oxford: Elsevier 2015), 13, 23, 79–101.

Subsequent notes:
[11] Dewey, *Logic*, 123.
[12] Changeux and Ricoeur, *Ce qui nous fait penser*.
[13] Düllmann, *Nuclear Physics A*, 74–76.

Chapters and other parts of edited books:

First note:
[1] Clinton Tolley, 'Hegel's Conception of Thinking in His Logics', in *Logic from Kant to Russell: Laying the Foundations for Analytic Philosophy*, ed. by Sandra Lapointe (New York: Routledge, 2019).

Subsequent notes:
[7] Tolley, 'Hegel's Conception of Thinking', 84.

Journal articles:

First note:
[1] Louis D Brandeis and Samuel D Warren, 'The Right to Privacy', *Harvard Law Review* 4, no 5 (1890), 193–220.
[2] Karl Schlieker, 'Lufttaxis gewinnen an Flughöhe', *Allgemeine Zeitung,* November 29, 2019.

Subsequent notes:
[4] Brandeis and Warren, 'The Right to Privacy', 201.
[5] Schlieker, 'Lufttaxis'.

Online works:

First note:
[1] Sophia Chen, 'Physicists Take Their Closest Look Yet at an Antimatter Atom', *Wired*, February 19, 2020, https://www.wired.com/story/physicists-take-their-closest-look-yet-at-an-antimatter-atom.

Subsequent notes:
[2] Chen, 'Physicists'.

If a paper you are linking to has an associated Digital Object Identifier (DOI), please use the http://dx.doi.org/ address to link to it instead of the publisher's address.

Cases: Citing cases in the body text, at first, use the '*Doe v Wade*' form, later on, an unambiguous short version is enough ('in *Wade*'). In footnotes, when it is first mentioned, give the name of the case in full – thereafter it may be shortened, but provide a cross-citation in brackets to the footnote in which the full citation can be found. Do not forget to give the law report and page or paragraph number.

[1] *Virginia v Black* 538 US 343 (2003).
. . .
[14] *Virginia* (n 1) 345.

Citing sources of law, use full forms in the body text (for example, Article 8 and Section 9(1)(a) of Human Rights Act 1998), and abbreviations in footnotes (Human Rights Act 1998, art. 8 and s. 9(1)(a)).

R v Secretary of State for the Home Department [2000] AC 115
Connolly v Director of Public Prosecutions [2007] EWHC 237
Hill v Great Tey Primary School [2013] ICR 691
Smith Kline & French Laboratories (Australia) Ltd v Secretary to the Department of Community Services and
London Artists Ltd v Littler [1969] 2 All ER 193
Rofe v Smith's Newspapers Ltd [1924] 25 SR (NSW) 4
Australian Broadcasting Corp. v O'Neill [2006] HCA 46
Abrams v. United States 250 US 616 (1919)
Lingens v Austria (1986) 8 EHRR 407
Health (1990) 22 FCR 73
Burnett v National Enquirer, Inc. 144 Cal. App. 3d 991 (1983)

Schenck v United States 249 US 47, 52 (1919)
R (on the application of ProLife Alliance) v British Broadcasting Corporation [2003] UKHL 23, [91]

Case C-154/19 *Kypriaki Kentriki Archi v GA* (ECLI:EU:C:2019:888)

Von Hannover v Germany no 59320/00
Von Hannover v Germany (No 2) nos 40660/08 and 60641/08

Arrêt n°1113 du 19 décembre 2019 (18-25.113)
BVerfGE 120
Cass. civ. 13 aprile 2000, n. 4790

Footnotes

Footnotes can be a form of citation or can provide relevant additional information. Indicate footnotes with a superscript number which should appear after the relevant punctuation in the text – for the clarity, it can also be put directly after the word or phrase to which it relates. If a subsequent citation immediately follows, use 'Ibid.' Separate citations with semi-colons. Pinpoints to pages come at the end of the citation. If the page numbers have the same hundreds or thousands digit, do not repeat it when listing the final page in the range. Close footnotes with a full stop. Italicise titles of books – all other titles should be within single quotation marks and in roman. Capitalise the first letter in all major words in a title. Footnotes must contain all available data of the cited sources. Do not insert 'at', 'page', 'p' or 'pp', and avoid 'ff'. Use 'Press' referring to university publishing houses (for example, Edinburgh University Press).

[1] Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (New York: St. Martin's, 1985); Henry Petroski, *Design Paradigms: Case Histories of Error and Judgment in Engineering* (Cambridge: Cambridge University Press, 1994); Tom Jackson (ed.), *Engineering: An Illustrated History from Ancient Craft to Modern Technology* (New York: Shelter Harbor, 2016).
[2] Simon Winchester, *The Perfectionists: How Precision Engineers Created the Modern World* (New York: Harper Perennial, 2019).
[3] Ibid. 74.
[4] Petroski, *Design Paradigms*, 122–34.
[5] Petroski, *To Engineer Is Human*, 27.
[6] Winchester, *The Perfectionists*, 76.

Italicising

For laying emphasis on a word or some words, use italics. Avoid over-emphasis. Italicise foreign words and phrases as well, but not quotations and words that are in common usage in English. Referring to foreign terms, next to the English translation, provide the original expression in brackets.

The being-in-the-world (*in der Welt-Sein*) . . .
The expression 'general rule' (*à la règle générale*) . . .
Everyday autarky (*αὐτάρκεια*) in this context means . . .

Listing
Lists with less than five items preferably should be in paragraph format, and marked with numbers ((1); (2); (3); (4)). If necessary, use vertical lists with en dashes instead of bullets. Put a period at the end of items in a vertical list only if the items are complete sentences. Otherwise, omit terminal periods, even for the last item, and do not capitalise the first words.

Punctuation and abbreviation
Use as little punctuation as possible. Abbreviations and initials in authors' names do not take full stops. Nevertheless, mentioning for the first time, full names should be used at first.

Cass R Sunstein, in his paper The Power of the Normal, analyses the stigmatisation by categorisation as well. He, like Erving Goffmann, uses these words . . .
Sunstein argues that . . .

The European Union (EU) is an international organisation comprising 27 European countries. Originally, the EU confined to western Europe . . .

Contractions ending with the same letter as the original word do not take terminal full stops (Mr, edn), but abbreviations where the last letter of the word is not included do (ch., ed.) – except the abbreviated forms of 'versus' and 'note'. The abbreviations 'etc.', 'i.e.' and 'e.g.' should be replaced by 'and so on', 'that is' and 'for example'.

article, articles	art., arts
chapter, chapters	ch., chs
number, numbers	no, nos
paragraph, paragraphs	para., paras
part, parts	pt, pts
section, sections	s., ss

Commas should be omitted before the final 'and' and 'or' in lists unless they help understanding.
Introducing a span or range with words, do not use the en dash. Use en dash reporting contest scores or results, and between words representing conflict, connection or direction.
Omissions should be indicated by ellipsis, in which each dot should be separated from its neighbour by a non-breaking space (. . .). If the omission comes at the end of a sentence, use a full stop and an ellipsis.

Winston Churchill in his historic speech, 'We Shall Fight on the Beaches', said that

> That was the prospect a week ago. . . . The King of the Belgians had called upon us to come to his aid. Had not this Ruler and his Government severed themselves from the Allies, who rescued their country from extinction in the late war, . . . the French and British Armies might well at the outset have saved not only Belgium but perhaps even Poland.

Symbols
Instead of using % symbol, write 'per cent'.
Use & symbol only if it is a legacy, for example, in titles and names (*William & Mary Quarterly*, Simon & Schuster).

Contents