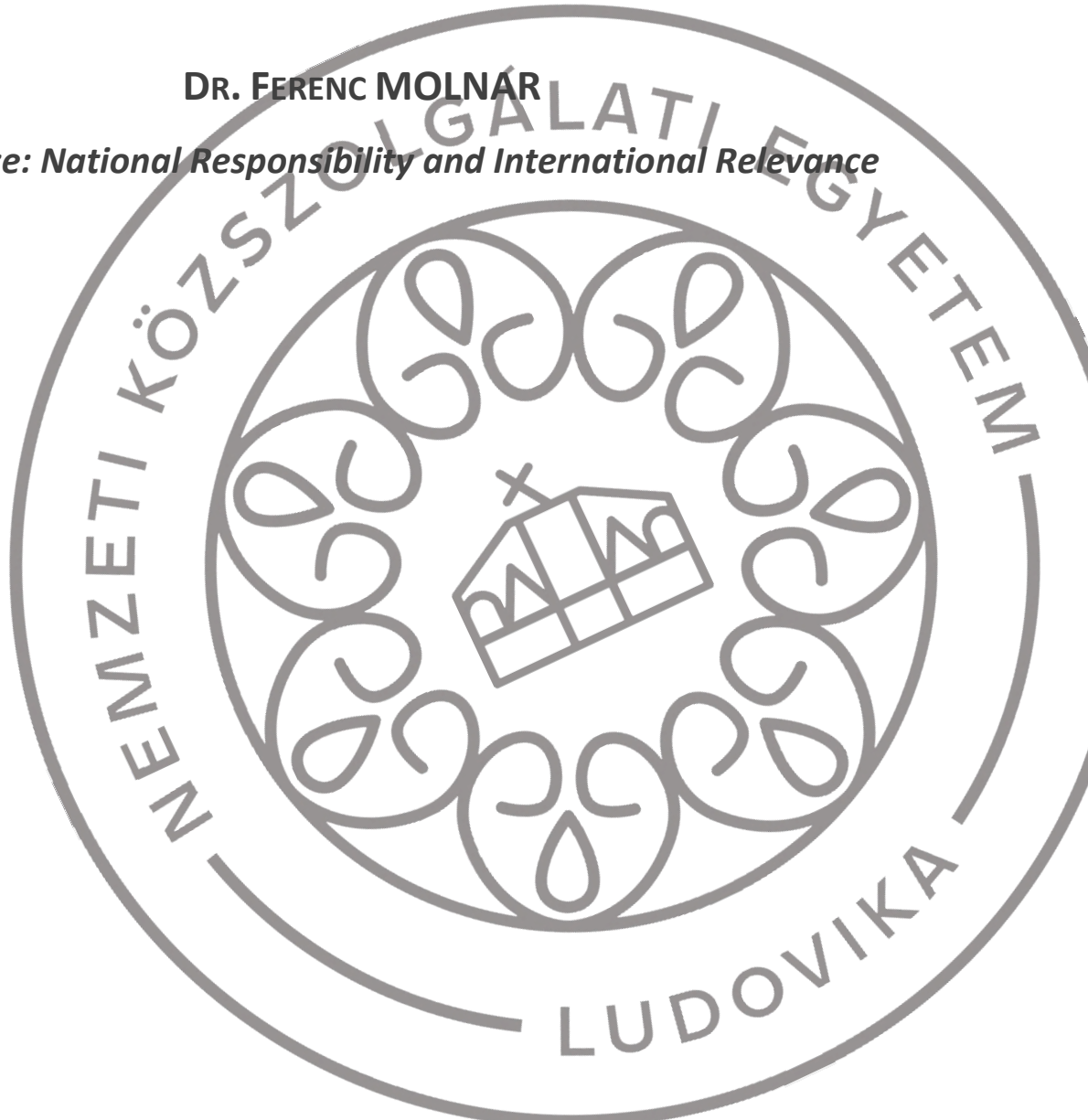
NEMZETI KÖZSZOLGÁLATI EGYETEM
VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY

VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2023/12.

DR. FERENC MOLNÁR

Resilience: National Responsibility and International Relevance



Rólunk

A műhelytanulmány (working paper) műfaja lehetőséget biztosít arra, hogy a még vállaltan nem teljesen kész munkák szélesebb körben elérhetővé váljanak. Ezzel egyrészt gyorsabban juthatnak el a kutatási részeredmények a szakértői közönséghez, másrészt a közzététel a végleges tanulmány ismertségét is növelheti, végül a megjelenés egyfajta védettséget is jelent, és bizonyítékot, hogy a később publikálandó szövegben szereplő gondolatokat a working paper közzétételekor a szerző már megfogalmazta.

A Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok célja, hogy a Nemzeti Közszolgálati Egyetem Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely küldetéséhez kapcsolódó területek kutatási eredményeit a formális publikációt megelőzően biztosítsa, segítve a láthatóságot, a friss kutatási eredmények gyors közzétételét, megosztását és a tudományos vitát.

A beküldéssel a szerzők vállalják, hogy a mű megírásakor az akadémiai őszinteség szabályai és a tudományosság általánosan elfogadott mércéje szerint jártak el. A sorozatban való megjelenésnek nem feltétele a szakmai lektorálás.

A műfaji jellegből adódóan a leadott szövegekre vonatkozó terjedelmi korlát és egységes megjelenési forma nincs, a szerzőtől várjuk az absztraktot és a megjelentetni kívánt művet oldalszámozással, egységes hivatkozásokkal.

A szerző a beküldéssel hozzájárul, hogy a művét korlátlan ideig a sorozatban elérhetővé tegyük, továbbá vállalja, hogy a working paper alapján megírt végleges szöveg megjelenési helyéről a szerkesztőséget legkésőbb a megjelenéssel egy időben értesíti.

A kiadvány ötletét az MTA Jogtudományi Intézet Law Working Papers sorozatának sikeréből merítettük.

Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2023/12

Szerző:
Dr. Molnár Ferenc dandártábornok

Kiadja
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője
Dr. Kádár Pál PhD dandártábornok

ISSN szám
2786-2283

A kézirat lezárva: 2023. november 15.

Elérhetőség:
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely
1441 Budapest, Pf.: 60
Cím: 1083 Bp., Ludovika tér 2.
Központi szám: 36 (1) 432-9000

DR. FERENC MOLNÁR

Resilience: National Responsibility and International Relevance[1]

Introduction

Throughout the ancient time, the middle ages and modern times, the history of Europe is largely about wars and conquering much of the world. World War I and II are horrific memories for our societies. Those wars initiated major European efforts to develop regulated forms of competition among nations other than war. Relations of the European Union countries regulated by law and their security is guaranteed through an institutionalized system, so that they do not pose a threat to each other. Their defence against external armed threats is essentially guaranteed by NATO, with the United States of America as the dominant military force. However, over the last decade, NATO allies and the EU have had to conclude that it is urgent to strengthen their defence.

The post-Cold War euphoria eclipsed the knowledge of security related principles, including the importance of the balance of power. Moreover, the priority of the United States is increasingly Asia and not Europe, where the future of world development lays and the peer competitor is. Although the he Russo-Ukrainian war proved that the US is still engaged in Europe but there is no doubt that European comprehensive security and defence developments are needed. There are many reasons for this: most notably, the vast majority of European countries significantly reduced their defence capability including their forces after the Cold War while concentrated on crisis management away from their borders; the return of inter-state war in the form of hybrid warfare in Europe. It is both a total war between states (Russian-Ukrainian war), military and non-military (e.g. economic, energy, IT, diplomatic), and a combination of covert and overt means (disinformation, fake news, use of irregular and terrorist groups).

As the hybrid warfare is more eminent, the boundaries between war and peace are blurred, so that societies and states can be destabilised without armed conflict. As a consequence, NATO

[1] Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

allies and EU states will have to make increasing efforts to develop their resilience in comprehensive way – including political, governance, economic and social resilience. These developments in turn imply legal and regulatory, structural, operational and cultural dimensions. Consequently, effective whole of government and international coordination[2] are needed probably more than ever.

Nowadays, the improvement of resilience is an integral part of NATO's defence and deterrence policy with primary focus on military means in order to divert an adversary from offensive intentions as its incapability to achieve desired objectives is proved. The EU is also making efforts on resilience in wider range of areas while partnering with NATO. This paper aims to briefly illustrate how resilience has become a catchword and to contribute to a better understanding the importance of international collaboration in that field. It points out that resilience is essentially a national responsibility, but effective national resilience can only be achieved within NATO and the EU. Consequently, collective commitments are key for the cohesion of allied nations, NATO's deterrence, the delivery of its core tasks and its cooperation with the EU are of paramount important for the resilience of the Western world.

Emerging Significance of Resilience and International Cooperation

In terms of reconsidering security and defence, the Russian annexation of Crimea (2014) was a defining moment for NATO and the European Union. It was the first time changing internationally recognised independent state borders by force in Europe after the second World War, however, not through traditional war. Russians used military force, by threatening both the civilian population and local authorities, and by circumventing international law. The then seemingly successful implementation of hybrid warfare in practice marked the beginning of a new era. In the same year, Russia supported national separatism in eastern Ukraine by political, military, economic and communications means. Russia's action against Ukraine triggered closer cooperation between NATO and the European Union and fundamental changed the way these

[2] Hungary adopted the Act XCIII of 2021 as the first legislation dealing with the coordination of security and defence issues as a prerequisite for creating effective resilience.

organisations think about defence. This was clearly articulated at the 2014 NATO Summit in Wales:

"Russia's aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at peace. Growing instability in our southern neighborhood, from the Middle East to North Africa, as well as transnational and multi-dimensional threats, are also challenging our security. These can all have long-term consequences for peace and security in the Euro-Atlantic region and stability across the globe."[3]

The Summit's final declaration underlines that Russian aggression against Ukraine had changed NATO's approach to European security. NATO's Foreign Ministers' meeting after the Summit in 2015, attended by the EU High Representative for Foreign Affairs and Security Policy, set out a strategy for defence against hybrid warfare and closer cooperation with the EU and partners.[4] As regards the future development of cooperation, resilience is presented as an area for development requiring complementary action by NATO, the EU and their partners. The "triumph" of resilience as a phrase of was completed in 2016 in both the EU and NATO narratives. The European Union's Global Strategy for Foreign and Security Policy emphasised the resilience of states and societies within Europe and in the neighbourhood, and the fact that the development and deployment of civilian-only instruments is increasingly inadequate to the realities of a changing world.[5] Resilience was also a key concept in the final declaration of the NATO Heads of States and Governments meeting of the North Atlantic Council in Warsaw.[6] Both NATO and EU documents, public dialogues emphasised the need of cooperation and coordination. Nevertheless, Covid-19 pandemic shed light to real actions.

Dealing with the spread of the Covid-19 virus would clearly have required international cooperation from the outset, but in the context of strategic rivalry, it has led to unilateral

[3] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 05 September, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm (01.08.2023.)

[4] NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini sajtónyilatkozata, 2015. 12.02. https://www.nato.int/cps/en/natohq/opinions_125361.htm (01.08.2023.)

[5] Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign And Security Policy https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0_0.pdf (02.08.2023.)

[6] Warsaw Summit Communiqué https://www.nato.int/cps/en/natohq/official_texts_133169.htm (02.08.2023.)

reactions, above all from China and the United States. The Chinese leadership focused on maintaining its central power and strengthening its international position in the unexpected situation. The US leadership, on the other hand, focused on competing with China at the expense of international cooperation – even in case of the Alliance. The UN World Health Organization became the arena for US-China rivalry at the very time when international cooperation was most needed.[7]

The rapidly changing international environment at the outbreak of the pandemic also placed significant strains on the operations of NATO allies. The response of the Allied countries to the health shock was first at national level, and then the undoubted need for international cooperation led to continuous and increasingly complex coordination. In each case, national efforts to deal with the pandemic also meant the rapid deployment of security and defence organisations, including almost immediately the armed forces. The complex international and national civil-military coordination has greatly contributed to the recognition of the importance of resilience. Managing the pandemic made it increasingly clear that the international order, security and defence had fundamentally new characteristics. The rapidly emerging new security environment required significant and rapid adaptation by NATO allied nations and the EU, both at strategic and operational level.

The pandemic proved that the world had changed significantly through globalisation:

- countries and companies are much more interdependent, making them more vulnerable in many respects (e.g. supply chains);

- technological developments have opened up completely new dimensions in the fields of politics, public administration, public services, economics and warfare (e.g. artificial intelligence);

- a very different kind of resilience from the pre-Cold War needs to be developed today because of cross-border risks, interdependence and the decentralisation of systems within countries (e.g. the role of the private sector).

[7] Robert B. Zoellick, Before the Next Shock - How America Can Build a More Adaptive Global Economy, *Foreign Affairs,* March/April 2022.
https://www-foreignaffairs-com.cdn.ampproject.org/c/s/www.foreignaffairs.com/articles/world/2022-02-22/next-shock?amp (05.08.2023.)

Since the period of the pandemic outbreak, reconsidering resilience has let to researches, national and international conceptualisations. If any conclusion can be drawn from those, that is the following: resilience is multi-sectorial (political, economic, defence, etc.) and number of interrelated terms linked to that, in particular, resistance, recovery, adaptation and transformation. Nevertheless, novel developments such as outsourced services, accelerating scientific and technological developments worth to be highlighted which influence our current state of resilience and war too.

Actors of the market, and eminently the private sector, are key players in the provision of critical infrastructure and essential services. Many of those infrastructural elements and services which were nationally owned for decades (especially in Central and Eastern Europe) then mostly privatised during the 1990s. Even in the case of the Armed Forces significant services (e.g.: logistic, telecommunication) were outsourced during the period dominated by international peace support missions. It resulted in extensive dependence on commercial market actors of the armed forces in general and especially many of those in operations.

In many areas, civilian resources and critical infrastructures that are key to defence are owned and operated by the private sector. For example:

- about 90% of military transport for major military operations is provided by civilian assets leased or requested from the commercial sector;
- More than 70% of satellite communications used for defence purposes are provided by the commercial sector;
- some 90% of transatlantic Internet traffic, including military communication, is carried on submarine fibre-optic cable networks owned and maintained by civilian companies;
- around 75% of the national support for NATO operations is provided by local commercial infrastructure and services.[8]

In case of the pandemic, the challenges caused of outsourced production was bluntly pointed out by LTG Rittimann:

"NATO and its members should seriously consider repatriating the manufacturing facilities for masks, respirators, and medicine, all of which have been outsourced to countries outside the Alliance for economic benefit. When manufacturing is out of one's control, it is not possible to

[8] Resilience, civil preparedness and Article 3
https://www.nato.int/cps/fr/natohq/topics_132722.htm?selectedLocale=en

decide when to increase production or who gets priority. These are matters which go beyond NATO's mandate, but are nonetheless important."[9]

The reconsideration of how to regulate and incorporate private sector to national and international resilience and defence are key and an ongoing process. On the technological side nothing proves better the significance this problematic than the war in Ukraine in which core technological services are provided by private actors. No doubt that the Russia war against Ukraine provides plenty of lessons concerning different aspects of resilience, here one should be emphasized by citing the Ukrainian spy chief concerning the difference Starlink was making in the war:

"They have played and continue to play a significant role, because so many systems use the antennas, use the Starlink systems themselves, for communications, for drone transmissions, especially in terms of a remote command post and so on." [10]

The above described major involvement of big companies have special significance in the international systemic rivalry.

Although political, communicational aspects of interstate competition and so resilience are not new at all, a particular aspect of resilience worth to be emphasised because of its relative novelty, rapid evolution and significant effects, eminently the cognitive war. According to NATO Allied Command Transformation it can be defined as "the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage." Cognitive Warfare needs to be highlighted due to its nature of remaining under the threshold of traditional war, rapidly evolving scientific researches. Results are quickly applied by states and non-state actors such as social media companies.[11] This aspect of war closely related to misinformation, disinformation.

The production and dissemination of news that mislead and manipulate societies and have serious consequences for the political, economic and, where appropriate, national defence,

[9] LTG Olivier Rittimann, NATO and the COVID-19 emergency: actions and lessons, NDC Policy Brief No. 15. September 2020, p. 4.

[10] Josh Pennington and Sean Lyngaas, Starlink in use on 'all front lines,' Ukraine spy chief says, but wasn't active 'for time' over Crimea, https://edition.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html (2023.09.13.)

[11] The evolution of the relevance of social media in the context of war see: P.W. Singer and E.T. Brookings, Like War, the Weaponization of Social Media. Boston (MA): Houghton Mifflin Harcourt, 2018

presupposes, in addition to the technical conditions, a receptive society. Actually, this is essentially how the social science literature describes today's advanced digital societies. *"Post-truth"* was chosen by Oxford Dictionaries as the international adjective of 2016 (the year when Donald Trump was elected as the President of the USA and Grate Britain decided to leave the EU), with 2,000% more post-truth adjectives used than in 2015. A post-truth society denotes a society where objective facts have less influence on shaping public opinion than appeals to emotion and personal conviction. In other words, it could be argued - with a slight exaggeration, of course - that societies have become "fact resistant". The plausibility of the question of truth has raised fundamental questions of expertise and thus also for developed democracies. While some authors see the omnipotence of the ordinary person through social media as a dream of populists and the death of democracy;[12] others see it as an opportunity for democratic societies to rethink and strengthen their resilience.[13] Meanwhile the novel (digital) ways of misinformation, disinformation and cognitive war emerged, NATO and EU started to reemphasize security and defence in a more complex way.

The pandemic accelerated many international processes that had already begun. These include, first and foremost, global economic and strategic realignment; rivalries between political systems; restrictions on democratic freedoms; and technological progress. The pandemic has made it clear that we are living in a period of transnational threats that do not respect borders and of great power rivalry, and that these two phenomena are reinforcing each other. Above all, Russia war on Ukraine, the Azerbaijan attack against Armenia, and most recently, the large scale terrorist attack on Israel proved that national borders are challenged even by long haven't seen brutal physical forces.

[12] Tom Nichols, How America Lost Faith in Expertise And Why That's a Giant Problem, In: Foreign Affairs, March/April, 2017

[13] Timotthy Clark, Robert Johnson, The World Information War, Western Resilience, Campagning and Cognitive Effects, Routledge 2021.

National Responsibility with International Commitment

Allied nations declared during the Warsaw Summit 2016, that *"Resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance's core tasks."*[14] It also points out that there are three key core functions: ensuring continuity of governance and essential services to the population, as well as ensuring continued civilian support to national and NATO military forces. Resilience therefore requires a broad, comprehensive effort for involving government (ministries), the armed forces, the economy (state and market actors), citizens, civil society and international organisations.

It is well understood that European and allied nations' legal, regulatory and organisational processes are in line with the above described complexity, however, those qualities and effectiveness may vary. Coordinated whole-of-government actions are essential, as the threats and challenges are very diverse and no single ministry or nation can address them. The solidarity of society in the field of defence involves various forms of participation in physical protection, but also requires awareness-raising, education and training, as new digital technologies are sophistically applied in misinforming, influencing populations of countries with unprecedented effectiveness. Furthermore, there is a desperate need for concerted, international actions in the broadest sense – regulations, education,[15] training and practices. Although NATO, EU and other partners are working together on many fields in relations to resilience, here one perspective, cyber-enabled disinformation, is emphasised with an aim to underline national responsibility with international commitment, what is essential to have effective resilience.

In order to develop effective resilience to cyber-enabled disinformation, two directions should be identified: physical and cognitive resilience. Effective resilience can be developed as the result of complex steps in these two directions. Physical resilience can be achieved in cyberspace and through cyberspace-related operations. For example, preventing the spread of information,

[14] Commitment to enhance resilience, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm

[15] In the context of education, the NATO Defense College 51st Conference of Commandants is a good example, where the education of resilience in professional military education institutions were deeply discussed in 2022. https://ndc.nato.int/outreach/outreach.php?icode=46

damaging IT networks, removing news from social media. Detection and analysis of disinformation falls under this heading, as it has been partially automated through the use of artificial intelligence.[16] The development of cognitive resilience is based on preventing the acceptance of disinformation and on trust in public institutions.[17] Above all, it can be developed through education, the development and dissemination of best practices, awareness-raising and practical advice. Broad education is essential because practically all citizens are involved in the influencing processes, so the protection of national values and interests, social resilience can be greatly enhanced by conscious online activities (dynamic activities in addition to awareness of the risks).

This physical and cognitive resilience is most commonly achieved in the context of three closely interconnected sectors: public institutions, the market sector and civil society. It is within this framework that the related strategies, policies, regulations, structures and processes can be developed and put in place. The effective operation of all these can lead to the development of the essential cognitive components, namely trust in political and public institutions, social cohesion and the will of citizens to take action.

Effective resilience against disinformation spread through cyber operations is essentially a national responsibility, but can only be understood in an international context, as the risks and threats are transnational and the development of related knowledge and technology (e.g. AI) is unthinkable in isolation. Both NATO and the European Union have taken and are taking significant steps to improve resilience, and countering disinformation is an important part of this. There is regular political dialogue and professional cooperation between NATO and the EU. Their commitment to cooperation and areas of cooperation were set out in joint declarations in 2016, 2018 and 2023[18]

[16] Juršėnas, A., Karlauskas, K., Ledinauskas, E., Maskeliūnas, G., Rondomanskas, D., Ruseckas, J. The Role of AI in the Battle Against Disinformation (2022). Riga: NATO Strategic Communications Centre of Excellence https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Role-of-AI-DIGITAL.pdf?zoom=page-fit

[17] C. Bjola and K. Padadakis, Digital Propaganda, Counterpublics, and Disruption of the Public Sphere, in: Timotthy Clark, Robert Johnson, The World Information War, Western Resilience, Campagning and Cognitive Effects, Routledge 2021. p. 195

[18] Joint declaration on EU-NATO Cooperation by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, 2016. https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf; Joint declaration on EU-

Their respective processes are twofold. The first is the intensive use of strategic communication tools, the second is an approach based on innovation and technological development. The importance of strategic communication is underlined in NATO latest Summit Communiqué:

" We will continue to address disinformation and misinformation, including through positive and effective strategic communications. We will also continue to support our partners as they strengthen their resilience in the face of hybrid challenges." [19]

NATO is making intensive use of strategic communication tools to achieve its political objectives. It will seek to coordinate its capabilities and activities in support of specific policies, operations and other activities. Also from the military side, disinformation management is seen as a multidisciplinary activity, coordinated from the information operations side, based on a continuous assessment of the information environment, in which the psychological operations specialists play a leading role, complemented by the public relations specialists.

At the same time, relying on the autonomous regulation of the Allied countries and on common values, the organisation plays an important supporting role in the development of tools and methods and in the coordination of the numerous public and market players. Relevant for our topic, NATO institutions and organisations such as NATO's Transformation Command, NATO's Science and Technology Organisation, the North Atlantic Defence Innovation Accelerator (DIANA) play a leading role in the development of concepts and training for cognitive warfare at the Alliance level. This line of activities implies extensive research in cybernetics, psychology, neuroscience and other natural and social sciences. Participation in research, access to resources and exploitation of results are of high value to NATO members and partners.[20]

The EU is also taking significant steps to combat disinformation. In addition to their strategic communication, they are making a particular effort to involve market and civil society actors alongside public and governmental actors, based on a common set of values and principles. A

NATO Cooperation, 10 July, 2018. https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf; Joint Declaration on EU-NATO Cooperation, 2021. https://www.nato.int/cps/en/natohq/official_texts_210549.htm

[19] Vilnius Summit Communiqué, Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023 https://www.nato.int/cps/en/natohq/official_texts_217320.htm

[20] See: François du Cluze, Cognitive Warefare, ACT Innovation Hub, 2021, https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf

code of practice for a more coherent and predictable approach has been developed (2018) and reinforced (2022)[21] to ensure a more coherent and predictable approach by all actors.

Summary

Today, in a world that is multipolar, no country, and neither NATO nor the EU, can guarantee its security and defence on its own. Historically, it is not unprecedented to have a bipolar or multipolar world order, but the world has never been so complex, real-time and interconnected. Climate change, accelerating technological development and the rivalry between political systems do not respect national borders.

Developing resilience has gradually gained ground in the developed part of the world, and then rapid actions were required due to Russia's war against Ukraine, the Covid-19 pandemic and China's decisive economic and military rise. Over the past decade, it has become clear that a comprehensive reinterpretation, coordination and regulation of the security and defence sector at national level has become urgent. Cyber-enabled disinformation and cognitive war are eminent fields in which resilience requires national assessment, planning and actions in the frame of international commitment. Eminent fields in a sense that those aim to harm (under the threshold of war) the very cohesion of societies and national institutions, which are existentially important for nations.

The effectiveness of national developments depends crucially on alignment and coordination with international alliance and partner systems. This is an exceptionally difficult task, as Russia and China aim to change the current rules-based world order favoured by the Western world. This order will certainly change, as the post-World War II systems are becoming increasingly dysfunctional. However, the extent to which the balance of power and thus the rules change is of existentially important for NATO, the EU.

[21] EU strengthens its code of practice to tackle online disinformation, https://www.euronews.com/my-europe/2022/06/16/eu-strengthens-its-code-of-practice-to-tackle-online-disinformation