Hybrid Warfare Reference Curriculum Volume II

Edited by
Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS

Hybrid Warfare Reference Curriculum
Volume II

Hybrid Warfare Reference Curriculum Volume II

Elective Seminars

Edited by
Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS
Budapest, 2025

Disclaimer: This book was developed in the framework of the Hybrid Warfare Project (ID.: 2021-1-HU01-KA220-HED-000032179) that has received funding from the Erasmus+ Programme. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Editors
Zoltán Jobbágy – Edina Zsigmond

Peer reviewed by
András Rácz

Published by the Ludovika University of Public Service
Ludovika University Press
Responsible for publishing: Gergely Deli, Rector

Address: HU-1083 Budapest, Ludovika tér 2.
Contact: kiadvanyok@uni-nke.hu

Managing editor: Katalin Pordány
Copy editor: Zsuzsánna Gergely
Layout editor: Angéla Fehér

Printed and bound in Hungary.

DOI: https://doi.org/10.36250/01236_00

ISBN 978-963-653-106-5 (print)
ISBN 978-963-653-107-2 (ePDF)
ISBN 978-963-653-108-9 (ePub)

Contents

Introduction

It is a commonplace to state that the form of war is constantly evolving. In the contemporary conflict environment, in addition to large-scale, conventional conflicts, many hybrid actors and proxy groups also wage war in an asymmetric, low intensity and irregular manner by exploiting ambiguity, strategic surprise and deception to accomplish their objectives. This conflict environment is volatile, uncertain, complex and ambiguous, in short, VUCA. This environment requires that educational and research institutions disseminate knowledge to help students perform complex tasks and duties in an efficient and effective manner. Curriculum development within higher education is a performance improvement tool that helps both lecturers and students to gain cutting-edge knowledge to perform up to a certain standard or obtain the expected level of performance. This is even more important as security challenges come in many disguises. The concerns European societies face are of unknown magnitude and the need for proper understanding and adequate policy responses is paramount. Supporting improved awareness, strengthening resilience and building the required capacity are all part of this effort. The Russo–Ukrainian war just underlines the need for such capacities and capabilities. Security challenges and threats, in whatever disguise they may come, have the potential to undermine the security of the European Union (EU) and the very values that underpin and inspire its societies. The EU must be committed to address these challenges with all available means. Citizens need to have a clear understanding of the risks and threats affecting the security, resilience and sustainability of their environment, including the smaller and larger communities to which they belong. The term hybrid warfare first appeared in 2005. The underlying concept subsequently evolved to cover a multitude of actors, strategies and actions. Overcoming a uniquely military-centred point of view is at the core of hybrid warfare as it takes advantage of the disunity within organisations of political entities and of the absence of a hegemon in international relations. The *Hybrid Warfare Reference Curriculum* was created within the framework of a Cooperation Partnership project of the Erasmus+ Programme. Financed by the European Union, in 2021 four European and an Israeli higher education institute and a U.K. think tank embarked on a journey to create a cutting-edge education and training material on the hybrid warfare topic. A curriculum with relevance hard to underestimate – especially after the war started in 2022 in Ukraine – but missing from European universities' study

DOI: https://doi.org/10.36250/01236_01

programmes. The present curriculum takes into account the diversity of actions forming part of hybrid warfare, uniting a variety of disciplines. Founding on the academic and geographic diversity of the project partnership, the *Education and Training on Hybrid Warfare Project* recognises the responsibility of higher education institutions in contributing to stable societies. The partners' aim is to provide a conceptual framework for a better understanding of current and most likely future conflicts to a variety of key national stakeholders, ranging from government to the civic society and with a specific focus on youth. This requires a comprehensive academic and professional curriculum aimed at enhancing situational and contextual awareness and in particular, the anticipated consequences of such conflicts. The project accords with the clear requirement of the security studies institutions to become more familiar with the complexities associated with hybrid warfare and to initiate a consolidated familiarisation with a refined appreciation of the disparate risks associated with hybrid warfare. In terms of foreign and defence policy postures and capabilities, it is essential for EU members to foster a culture of common appreciation, allowing for a wider understanding and dissemination of knowledge and to support the crafting of common responses to hybrid warfare. The failure to address issues ranging from definitions and lexicon to the mechanics of force or policy posture can be detrimental to EU members' ability to work collaboratively, especially in periods of high tension and crisis. The intention behind the development of the project was to provide common study material for civilian, police and military higher education institutions to address a significant number of issues associated with the policy and operations of most forms of hybrid warfare. Through the newly developed curriculum and teaching methodology students shall gain:

- a better appreciation of how hybrid warfare impacts today's modern military forces, in terms of doctrine, force structure, armaments, operations, command and control and training
- an insight into the non-military aspects of hybrid warfare, ranging from information and cyberattacks on critical network infrastructure to the nexus of public health and national security in response to the malicious use of life sciences and artificial intelligence
- a more nuanced understanding of how some hybrid warfare acts intend to destabilise communities and society, from the instigation of alternative news narratives to inciting community violence and criminality

– a deeper understanding of the decision-making process generated by hybrid warfare across a myriad of sectors to benefit from risk analysis, crisis management case studies, and simulation exercises to reinforce the contextual and situational awareness

The developed hybrid warfare reference curriculum, its supporting methodology and massive open online course will allow blended (physical and virtual) learning methods for accredited university classes, but also allows for mass online learning, thus reaching a much wider audience. The reference curriculum shall form the basis for either the partial or entire re-design and update of courses within the curriculum of military, police and civilian students of higher education institutions. The reference curriculum as a document reflects the combined knowledge of a multinational team of academics and policy experts drawn from European and Israeli universities and think tanks. The reference curriculum comes as the result of close cooperation between the project partners to motivate others interested in the subject. The reference curriculum also serves as an initial document for individuals or organisations looking to develop a curriculum dedicated to combating hybrid challenges, or to amend their existing curricula accordingly. The content of the hybrid warfare reference curriculum is not intended to be adopted in lockstep, but rather to fit particular needs and aspirations. Its function is to increase intellectual interoperability and foster in-depth and specific academic knowledge and professionalism in an interdisciplinary manner. It can also support interested partners in enhancing their capacities to develop their national skills and improve suitable strategies to counter or wage this sort of warfare. The reference curriculum also serves as a fundamental document to address educational institution requirements and provide helpful guidelines for relevant courses on security and defence. The reference curriculum, among others, provides an overview of underlying ideologies, motivations and methods, as well as contemporary practices and projections of future potential. As such it contributes to European and Transatlantic cooperation in security-related issues through education by offering students, professors, researchers, policy experts and the interested public a new international and interdisciplinary platform of study, and also a foundation for cutting-edge, practice-oriented knowledge. The curriculum also serves as a basis for those who intend to implement tailored versions of the curriculum for their distance learning or residential courses.

It contributes to a student-centric environment too, as it can help train students to better understand the complex challenges posed by hybrid warfare and to respond better to it. The reference curriculum promotes critical thinking and a thorough understanding of European core values and interests. This important pedagogical objective is fostered through participatory structures and transformative education. To reach the goals set above and to exploit the synergies created by the participating institutions, the reference curriculum may be regarded as the basis of a modular system resulting in various single or joint degree courses at a later stage. The reference curriculum contributes to a series of online and blended modules with a focus on selected security and defence issues, involving a participative and extensive simulation exercise/wargame moderated by a trained staff. All recipients of the curriculum, irrespective of their previous background and knowledge, shall benefit from a range of delivery methods including:

- a cutting-edge, interdisciplinary curriculum
- a combination of presentations, tutorials, case study analysis simulation exercises and table-top exercises
- a massive open online course on hybrid warfare to reach a much wider audience

Thus, global issues, especially security ones are increasingly the subject of policy-level deliberations, both nationally and internationally. Transnational cooperation in science deals with these issues. Cooperation in the form of various partnerships is of special importance, because they possess much of the expertise, data and resources that are needed to find effective solutions. The reference curriculum makes clear that hybrid warfare stands for issues and options that deserve the attention of scientists and researchers as they seek to design, initiate and manage collaborative research programmes and projects that include both scientific and development goals. Links between science policy and the mechanisms to address issues raised already exist in EU countries. Motivations and opportunities to support scientific collaboration in the form of partnerships to strengthen research capacity have assigned a higher priority to global issues, put more emphasis on collaborative research, and have moved beyond traditional knowledge transfer. The reference curriculum just reflects the fact that scientists and policy makers increasingly turn towards desirable and even crucial partners who can provide a wide range of expertise, resources and other benefits. Some are identifying ways to organise projects that encourage the full participation of researchers who are actively building and enhancing

research capacity to create and utilise the new knowledge that is essential for their development to address local and regional manifestations of global-scale challenges of which hybrid warfare is but one. Recognising the importance of the global security challenges and trends and seeking to maximise the benefits of cooperation through linking science policy with science capabilities thus contemplating new cooperative ventures to improve existing efforts. Moreover, we are living in a time when different generations may see the world dramatically differently. Therefore, the experience of the 20th century must reach out to the enthusiasm of the 21st century and make a strong bond. The reference curriculum can forge the bond in the mind and soul of the young generation, of whom university students play an important role as they will form the future cohort of intellectuals and decision-makers that will need to take care of various policy and military responses to hybrid threats in the near future. The reference curriculum offers a comprehensive and interdisciplinary approach in the broadest sense that encompasses definitions and descriptions, addresses the hard and soft aspects of hybrid warfare, and names disciplines and subjects to make hybrid warfare studies accessible for lecturers and students alike. The project stands for a change in the institutional portfolio of the authoring partner institutions since it produces new knowledge that they institutionalise and disseminate through various social practices over time. Thus, the reference curriculum brings something new and creative to the partners involved and to the wider EU community. The partnership powers high quality and fosters innovation by exploring and considering a new concept such as hybrid warfare, and by delivering new content and methods with much value to lecturers, researchers and students. The present book can be seen as a descriptive, reflective and explanatory study of hybrid warfare seen from many different angles. It is descriptive in a sense that it describes hybrid warfare as a complex phenomenon posing serious threats to the stability of any political unity. It is also reflective since by approaching hybrid warfare as an intrinsically complex and multi-layered phenomenon, consistency and coherence is provided by the use of the respective scientific literature and very often Clausewitz's epic volume *On War.* It is explanatory since inconsistencies are discovered, the authors identify and explain the contributory factors in detail. The reference curriculum aims at developing a coherent framework that offers a novel approach to hybrid warfare by detailing the underlying attributes from a multiple point of view. Since the curriculum exceeds the framework of a semester class in volume, the team of authors agreed to divide the chapters into compulsory lectures (Volume I), elective seminars (Volume II), and elective

lectures (Volume III), from which lecturers may choose the topics most relevant for their classes. The present, second volume offers a selection of topics suggested for elective seminars on the subject matter, providing its readers with practical knowledge for understanding the hybrid phenomenon and its practices. This textbook highlights the different tools and approaches on hybrid warfare, and provides for case studies and methodology as well. Russia – a *par excellence* user and inventor of hybrid warfare means and tools, even if using different definitions – is appearing in many of this book's chapters. Russia's practices are thoroughly examined – going back to the Cold War and up until the present war in Ukraine, the role of proxy wars are introduced and analysed throughout history but focusing on today. This volume gives an overview about chemical, biological and nuclear warfare and the questions of biosecurity. The book introduces the establishment and functioning of the European Centre of Excellence for Countering Hybrid Threats and puts emphasis on the methodology analysing the most representative conceptual models for understanding the framework of hybrid threats, and the adversary's strategies, operations and tactics. Today, citizens are organised worldwide through virtual networks that consume, produce and spread information at an incomprehensible speed. The fragility and underlying dangers inherent in this phenomenon are also examined in this volume, pointing out the "blurring boundaries between the real and the virtual" and the possibility for mass manipulation and other forms of digital hybrid warfare. Most of the chapters provide for excellent basis for thought-provoking debates and group exercises entailing creative and innovative thinking. The Hybrid Warfare Project Team from the Ludovika University of Public Service in Budapest, Hungary, the "Nicolae Bălcescu" Land Forces Academy in Sibiu, Romania, the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš, Slovakia, the University of Torino, Italy, the Bar-Ilan University in Ramat Gan, Israel and the Centre for the Study of New Security Challenges in Edinburgh, United Kingdom wishes interesting and useful readings for all students, lecturers and independent learners.

Zoltán Jobbágy – Edina Zsigmond
editors

Vojtech Jurčák – Ján Marek[1]

Russian Practices

Opinions on defining the term "hybrid war" are not uniform. To a large extent, they have an empirical basis, hence the diversity of definitions. The authors use a semantic approach to define the term. The term "hybrid war" itself is composed of two words such as war and hybrid. Dominant in relation to this phrase is the noun "war", the adjective "hybrid" determines what type of war it is. In the English language, according to the Dictionary of Military Terms, the word *war* "means an armed conflict between nations",[2] or "may also mean conflict between social groups within the state, world war, civil war, guerrilla war, atomic war, thirty-year war, Trojan war", etc. According to the Encyclopedia Britannica[3] *war* is defined as "wars, battles, and other domestic or international conflicts, whether armed or diplomatic, are often the outcome of a dispute over natural resources or a struggle for power, influence, and wealth. Major conflicts between nations, peoples, and political groups can end up shifting the cultural and political geography of the world and can also effect change, whether international or not, in societal values and the balance of power". In defining the term *war,* the definition of Carl von Clausewitz, a Prussian general, an important military strategist, theoretician and historian, professor of the military academy, representative of the Prussian–German military school is generally accepted, who in his work *On War* defined war as "an act of violence to force an adversary to submit to our will".[4] Violence (we stress physical violence) is the dominant theme of this concept, and represents a means to achieve the goal by defeating or disarming the enemy. As Clausewitz further states in his work, war between nations always starts from a certain political situation and is always triggered by a certain political motive. It is not just a political act, but a real instrument of politics, "war as a continuation of political relations and their implementation

[1] Armed Forces Academy of General Milan Rastislav Štefánik.
[2] U.S. Department of Defense 2010.
[3] Encyclopedia Britannica s. a.
[4] Brühl 2016.

DOI: https://doi.org/10.36250/01236_02

by other means".[5] Therefore, even in case of a hybrid war, it must be based on the analysis of the current political context and the motives of the actors who are waging this kind of warfare against sovereign states. The word "hybrid" is a word of Greek origin and means crossbreed or mixed race, or bastard. The adjective hybrid is derived from it, meaning crossed, mixed. In the English language, the word "hybrid" means "something that is created by mixing two very different things".[6] From the above said and their semantic context, the authors conclude that a "hybrid war is an act of violence, carried out with significantly different means or methods, with the aim of forcing the adversary to submit to our wills or, as a continuation of policy by significantly different means, while carrying out the policy openly and covertly, through various activities of state and non-state actors, military and non-military means, conventional and asymmetric forms of waging war, even without its declaration". NATO defines hybrid warfare as: "The use of military and non-military as well as covert and overt means (including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces) to blur the lines between war and peace, sow doubt in the minds of target population, and destabilize and undermine societies."[7]

Gray zone conflict

The gray zone is an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counteractions by other nation states. Inside the gray zone, aggressors use hybrid tactics to achieve their strategic objectives. While hybrid threats have historically been associated with irregular and conventional warfare, their use in the gray zone leads to a dichotomy between two types of hybrid threats that can mainly be attributed to the need for ambiguity and non-attribution in the gray zone. The two types of hybrid threats are "open-warfare hybrid threats" and "gray-zone hybrid threats". A case in point is Russia's military actions in eastern Ukraine, part of what the Kremlin calls its "New Generation Warfare".[8]

5 Brühl 2016.
6 U.S. Department of Defense 2022.
7 NATO 2023.
8 Chambers 2016.

Aleksandr A. Bartosh defines the gray zone as a wide area of action (operational environment), which we can perceive as the battlefield of a hybrid war, which covers the territory of one or more states against which a campaign of hybrid war is conducted.[9] In the European Union, only two member states have a defined gray zone in their strategic documents – Hungary and Romania. In the Hungarian security strategy, the issue of the gray zone is characterised concretely and extensively as asymmetric and hybrid ways of waging war, where emerging or resurgent states or non-state actors use a wide range of military or non-military means to advance their interests, often in a covert form are gaining more and more weight. This way of waging war blurs the otherwise clearly defined boundaries between peace and war, leading to transitional situation below the threshold of armed conflict – gray zone that do not meet the definition of war and are difficult to assess. The lack of an adequate defence capacity cannot only make it difficult for the target of the attack to react quickly and decisively or to prepare preventive measures, but it can even make it completely impossible.[10] Russia considers the Venezuelan presidential crisis, the ongoing Libyan conflict, the Syrian civil war and the crisis in Belarus (the crisis in Belarus is mainly a crisis of the regime, when President Lukashenko, instead of dialogue with his own people, relied on violence and repression, thereby depriving himself of legitimacy) as examples of hybrid warfare.[11] The Russian military actively focuses on preparing for future conflicts and on enhancing the capabilities it considers essential for victory in hybrid warfare. Russian strategic thinking identifies "hybrid wars" as the main line of future military development, not as a temporary phenomenon. The Russian military maintains theoretical space for the idea of traditional conventional warfare and does not argue that all conflicts are now "hybrid" in nature. Instead, it argues that conventional war is an inherited type of conflict that is increasingly unlikely in the 21st century due to technological change and strategic power. The Kremlin further argues that Russia should shape its military and national security tools for hybrid warfare not only because it is becoming more common, but also because it is now more practical, economical and effective than traditional conventional warfare.[12] The Kremlin rejects the differences between different types of conflicts and synthesises these types of

[9] Bartosh 2021.
[10] The Government of Hungary 2020.
[11] Clark 2020: 11.
[12] Clark 2020: 12.

conflicts within a unified concept of hybrid war. He rejects the conflict in the gray zone as well and considers it part of a hybrid war. Russia's hybrid warfare framework specifically includes the use of conventional military operations. Russia rejects the Western division into proxy operations and disinformation on the one hand and conventional conflict on the other. The Russian concept of hybrid warfare is incompatible with the idea of fighting in a "Grey zone", which is related to a relatively clear line where conflict means "war", but below which there is an ambivalent state of "war" or competition.[13] After the aggressor has made a strategic decision to use hybrid aggression, its preparation begins and takes place in peacetime. The nation or state against which it will be used is mostly without indications of any conflict. The preparation mainly includes intelligence activities to find out the weak and vulnerable places of the enemy for the later correct choice and use of components and elements of hybrid warfare. If we accept that the beginning of hybrid aggression begins in peace and that the purpose of hybrid aggression is not total war, then it mainly takes place in the beginning of the already mentioned gray zone. It is precisely in conflicts that take place within the gray zone that it is not possible to talk about peace, but the situation of the strategic environment does not even show formal signs of war, rather it seems to be a series leading to the escalation of the conflict. An aggressor who has decided to use a hybrid form of war minimises the space and scope of his operations to a place (within the axis of the conflict spectrum) where he is covered by sufficient ambiguity that he is a participant in the conflict, so that he can avoid bearing the consequences as an aggressor. All this without the open use of its own conventional armed forces. The result is a mixed and unclear management of operations and combat activity. It is precisely this feature that characterises contemporary modern conflicts and wars.

From the Russian perspective, the entire "Grey zone" is potentially part of a hybrid war, which additionally involves the use of military forces above the upper threshold of the "Grey zone", which the West and China would consider a conventional war.[14] Therefore, the West must fundamentally reorient its strategic thinking about Russia. It assumes that the Kremlin is currently fighting a hybrid war against the West and is using the experience gained from the battle in preparing for the next war. Thus, the West must avoid imposing its own conceptual boundaries on the developing Russian theory, which expressly rejects

[13] Clark 2020: 12.
[14] Clark 2020.

it. It must recognise the key differences between hybrid warfare and "Grey zone" conflict and incorporate conventional military operations into the perception of hybrid warfare. Only then can the Western community propose an appropriate approach to combat the real threat posed by Russia.[15]

Different approaches

Hybrid war is a coherently defined term for a typology of war as a set of means for conducting state policy for Russian military thinking and has an explicit and concrete meaning. The Russian military defines "hybrid war" as a strategic-level effort to shape the governance and geostrategic orientation of a target state in which all actions, up to and including the use of conventional military forces in regional conflicts, are subordinate to an information campaign[16] and considers (as we have already mentioned above) the Venezuelan presidential crisis, the ongoing Libyan conflict, the Syrian civil war and the current crisis in Belarus as examples of hybrid war. The confusion of the term in the English language led to its complete rejection or to the proposal of its own definition.[17] The discussion in the Western community points out that the term hybrid war is generally and primarily used in connection with the means of war, while for the Kremlin it refers to a category of war. The West will not understand Russian security policy, let alone Russian military policy, without a clear understanding of the Russian concept of hybrid warfare. The Western debate on the nature of the Russian military threat often divides the issue of hybrid warfare into two parts. One part is the threat of conventional war against NATO, but this kind of threat is unlikely, moreover, it is economically disadvantageous. The second consists of information aimed at subversive Russian actions or the deployment of "green men" as the maximum limit of kinetic operations. Such a divided concept does not describe the Russian view of "hybrid war", since it includes only conventional manoeuvre warfare and activities that American theorists associate with the term "Grey zone".[18] Although several studies report that the Kremlin uses "hybrid means" in every conventional war, it is quite the opposite,

[15] Clark 2020.
[16] Clark 2020: 11.
[17] Klijn–Yüksel 2019.
[18] Dalton et al. 2019.

the Kremlin conducts conventional military operations in the space that the West considers "competitive".[19] This misunderstood conception of the Russian threat leads Western policymakers to focus on the components of the Russian military threat separately, despite the fact that they are actually part of a cohesive whole.[20] A strategy of confronting Russia based on answers to incomplete parts of a set of problems is doomed to failure. Limiting the concept of hybrid warfare to activities below the threshold of conventional conflict leads Western analysis of the Kremlin to focus too much on the conventional threat posed by the Russian military to NATO armies. The false dichotomy of dividing hybrid and conventional means leads the West to conclude that conventional forces will be used and that it is necessary to adapt to the conventional use of conventional forces. Therefore, Western analysis does not pay enough attention to the capabilities and intentions of conventional units of the Russian armed forces to conduct hybrid operations directly and not only through subversive actors or other elements of the Russian state. Studies conducted have attempted to examine the relationship between hybrid efforts and conventional forces, how NATO conventional forces can counter a Russian hybrid effort led by Russian proxy forces such as in Ukraine. The goal of hybrid warfare is often to succeed without the involvement of conventional troops. Such studies do not address how NATO should respond in such an event and fail to adequately consider how to identify and respond to Russian conventional forces engaged in hybrid warfare. These studies informed NATO on the interaction between kinetic conflicts and the information space and limited the problem in ways that missed the mark.[21] The 2018 U.S. National Defense Strategy (NDS) asserts that Russia is disrupting the military balance of the "Competitive Military Advantage" of the U.S. and recommends upgrading the capabilities of the conventional military.[22] This recommendation is not bad, but it is insufficient. It does not eliminate Russian

[19] The competition space, also known as the competition continuum, is a framework the United States increasingly employs to reject the artificial distinction between armed conflict and peace without significant military competition that the United States has traditionally followed. Discussions of the competition space reject a dichotomy between war and peace, and instead describe ongoing international competition conducted through a mixture of cooperation, competition below armed conflict and armed conflict. See Joint Chiefs of Staff 2019.

[20] Mueller III 2019.

[21] Asymmetric Warfare Group 2016.

[22] U.S. Department of Defense 2018.

efforts to circumvent and directly challenge NATO's capabilities. One of the results of the studies is the finding that Russia's conventional threats are overestimated and hybrid warfare threats are underestimated, including an excessive focus on nuclear power or strategic deterrence.[23] Keeping NATO conventional forces in Eastern Europe is necessary and important to deter any potential Russian conventional threat. Russia could certainly use conventional forces against its western neighbours if the U.S. and its allies did not maintain adequately equipped and trained forces to help those allies defend themselves. In addition, these conventional forces can serve as a basis for directly attacking Russian hybrid operations.[24] The assumption that maintaining conventional NATO forces on the alliance's eastern border will prevent Russian hybrid operations seems unrealistic. Russian theory and doctrine increasingly assume that Russia cannot or should not engage in conflict against a conventional NATO force, but that it can achieve its goals – including against NATO states – through a hybrid effort that nevertheless includes elements of conventional warfare.[25] The NDS prioritises averting a major conventional conflict between the great powers. Russia is also trying to avoid a major conventional war between the great powers, so it is using a hybrid way of waging war that would achieve its goals. The NDS thus creates a hidden risk that Russia can achieve its political goals through hybrid warfare, to the great detriment of the U.S. and its allies, even if the U.S. formally achieves the goal of deterring war between the great powers. Russia has no intention of waging a conventional superpower war. If the U.S. focuses on deterrence to prevent Moscow from achieving its objectives below the threshold of conventional war, then the U.S. may suffer a strategic defeat even if its defence strategy technically succeeds.[26] Studies of the Russian military threat to Europe are necessary but insufficient because they do not capture the global scope of the Kremlin's use of conventional assets as part of hybrid warfare.[27] Several valuable case studies of Russian hybrid warfare focus exclusively on conflicts in the former Soviet Union, neglecting the Kremlin's global goals and the concept of

[23] Rose 2018.
[24] Connable et al. 2020.
[25] Sokolsky 2017.
[26] Sokolsky 2017.
[27] Sokolsky 2017.

hybrid warfare.[28] Russia represents a major conventional military threat to the West. Russia has also posed a huge challenge to the U.S. and its international efforts to fight the Islamic State in Syria because of the limited conventional military force it has incorporated into its hybrid warfare. The concept of Russian hybrid warfare thus allows Moscow to pose military challenges to the U.S. and its allies in areas beyond conventional military forces. Western decision-makers and military personnel must study Putin's Russia with a full understanding of Russian intentions and not just Russian capabilities. Intelligence analysis of Russian military capabilities without analysis of Russian intentions is valuable but often misleading.[29] Western analyses of Russian military learning and development can often correctly identify Russian capabilities and weaknesses, but fail to predict how Russia will use its increasingly modernised forces in ways consistent with the Kremlin's intent and view of hybrid warfare.[30] Discussion of Russia's experience gained in Syria and Ukraine is often strictly focused only on how Russia will apply this experience in the fight against conventional NATO forces, rather than understanding that this experience is part of Russia's theory of hybrid warfare.[31] Western decision-makers must change their conceptual understanding of Russian hybrid warfare from a term that identifies a set of means to a definition of a type of war. Several analysts in the Western community have accurately assessed the Kremlin's changing means of achieving its goals, most of which fall below the level of conventional warfare.[32] Several major studies have highlighted the key lines of the Kremlin's hybrid warfare efforts and proposed recommendations for countering them. The existing literature on Russian hybrid warfare is inconsistent with the Russian understanding of the term and uses "asset pool" rather than "type of war". This is not to say that the U.S. and its allies should not continue to develop their own frameworks, but the U.S. cannot eliminate important Russian terms due to faulty Western definitions. The U.S. and its allies must understand the Kremlin's concept of hybrid warfare and successfully counter the means involved in those wars – otherwise the West risks winning one battle but losing a war it does not know it is fighting. The thinking required to confront Russian hybrid warfare in current and future

[28] Connable et al. 2020.
[29] Defense Intelligence Agency 2017.
[30] Blank 2019.
[31] Majumdar 2018.
[32] Connable et al. 2020.

conflicts is critical. Western studies have analysed the key attributes of the Russian military threat but have so far failed to synthesise them with the views of the Russian military. The West cannot successfully counter the Russian threat without a holistic understanding of the Russian military.[33]

The Russian approach

This section analyses the Russian military debate on hybrid warfare and Russia's assessment of the future of warfare from the perspective of the National Security Strategy of the Russian Federation. The analysis of the Russian perspective on hybrid warfare is of great importance for further research on the topic, not only because of the great military power of the Russian Federation (RUS), but also because of its Russian–Georgian conflict in 2008 and later in the sudden annexation of the Crimean Peninsula in the spring 2014. Chief of the General Staff of the Armed Forces of the RUS and First Deputy Minister of Defence – Army General Valery Vasilievich Gerasimov is considered the founder of the Russian concept of hybrid warfare. According to Gerasimov "hybrid war is a war of a new generation, in which traditional military methods and procedures are replaced by hybrid ones, that is, a wide range of political, economic, informational, international, humanitarian and other tools". General Gerasimov goes on to say that "in the 21st century, a tendency begins to prevail, when the boundaries between war and peace are blurred. Wars are not declared, and if they are started, they do not follow the usual pattern. Experiences from conflict connected with the so-called "colour revolutions" in North Africa and the Middle East point to the fact that a prosperous state can become in a few months, or even days, an arena of military struggle, a victim of foreign intervention, and reach a state of humanitarian disaster, chaos, and civil war".[34] "In none of the countries" continues the general, "where the so-called Arab Spring is not an officially declared war, but the social, economic, and political consequences for individual states and societies are comparable to the consequences of a real war. Weapons are no longer needed to achieve political and strategic goals, there are more effective tools. To achieve the set goals, it is often more appropriate to use political, economic, informational, humanitarian, and other non-military measures, including the protest potential

[33] Connable et al. 2020.
[34] Gerasimov 2016.

of the target country's population". As an example, Gerasimov cites the use of humanitarian organisations or private security companies. According to him, examples are operations in Syria, Ukraine, or Libya, where hired private military companies worked closely with armed opposition units, or Greenpeace's activities in the Arctic. The Chief of General Staff and the Russian Government are convinced that the West finances both the opposition and other organisations in Ukraine and Russia. "All this is supplemented by cover military action of an information nature or special forces. The open use of force under the pretext of "peacekeeping and crisis management" only happens at the end of the conflict to "achieve the ultimate goals". In this context, Gerasimov goes on to ask: "Of course, it would be easiest to say that the events of the Arab Spring were not a war, and therefore we soldiers should not investigate them. But maybe it is quite the opposite, aren't these events a typical war of the 21st century?" And at the same time he adds: "The very rules of war have changed. The role of non-military methods of achieving political and strategic goals has increased, and in many cases their effectiveness exceeds the power of weapons. Military forces are often used under the guise of peacekeeping operations to achieve reconciliation between hostile parties." Frontal battles of large groups of soldiers at the strategic and operational level are gradually receding into the background, the general states. Influence on the adversary at a distance gradually becomes the main strategy to achieve the objectives of the operation. Its objects are destroyed throughout the depth of its territory. The distinctions between strategic and tactical levels and defensive operations are being blurred. Very accurate weapons are widely used. Weapons operating based on a new physical principle and robotic systems are built as part of the armament. Symmetric military activity is widely used, which makes it possible to level the superiority of the adversary in armed combat. At the same time, members of the special forces and forces of internal opposition are used to create a permanent front on the entire territory of the hostile state. Information influence is also used, the forms and methods of which are constantly being improved. Current events are reflected in the military doctrines of various countries. General Gerasimov presented the view (mentioned above) that the enemy can be defeated by a combination of political, economic, technological, informational and ecological operations. His statement is in line with the vision of war, which does not take place on the physical battlefield, but, as the Russian theorist states, it takes place in the so-called psychological sphere. According to him, future wars will not be fought in the classic way, on the battlefield, but mainly in people's minds. This is also why Russia

currently places great emphasis on the field of information and psychological operations. Information and psychological operations will no longer play the role of only supporting auxiliary activities, as before, because a well-prepared and conducted information and psychological war can, according to this concept, in many cases replace traditional ways of conducting war without the need to deploy many military units and equipment. In recent conflicts, according to General Gerasimov, new methods and ways of conducting military operations have appeared, the development, improvement and application of which will continue and will bring fundamental changes in the character of future armed conflicts. The biggest changes between traditional and non-traditional military methods (ways) are shown in Figure 1. As part of clarifying the Russian view of hybrid war, respectively new generation wars, it is also necessary to mention the work of Colonel Sergey G. Chekinov and Lieutenant General Sergey A. Bogdanov. The importance of their work mainly lies in the fact that, although they emphasise the use of the most modern military and non-military technologies, the war of the new generation should take place primarily in the psychological and informational dimension. The enemy's public institutions will be drawn into the war in a subversive way, while these conflicts, in which asymmetric procedures are to be largely used to undermine the enemy's superiority, should be preceded by intensive intelligence and reconnaissance activities. Chekinov and Bogdanov divided the course of war of the new generation into the following phases:[35]

1. Non-military asymmetric warfare including informational, psychological, ideological and economic measures as part of a plan to create favourable political, economic and military conditions for the next phases of the war.
2. Special operations aimed at deceiving political and military officials through coordinated measures along diplomatic channels, mass regulations and directives.
3. Intimidating, lying and bringing government and military officials to force them abandon their official duties.
4. Destabilising propaganda, which is supposed to increase the dissatisfaction of the population, which will be intensified by the arrival of militant groups and the escalation of subversive activities.
5. Establishment of non-fly zones over the country to be attacked, declaration of blockade and extensive use of private military companies in close cooperation with armed opposition forces.

[35] Chekinov–Bogdanov 2017.

6. Initiation of military actions, which were preceded by extensive reconnaissance and diversionary activity, i.e. all types, forms and methods of operations, including special forces operations, space operations, radio and electronic operations, diplomatic intelligence, intelligence and industrial espionage.
7. Operations conducted through targeted information, electronic warfare, air and space operation, continuous aerial intimidation in conjunction with the use of high-precision weapon systems (long-range artillery) and weapons based on new technology (including microwaves, radiation, non-lethal biological weapons).
8. Liquidation of the remaining places of resistance and destruction of the remnants of enemy groups through special operations conducted by reconnaissance units, which search for enemy units and report their coordinates to rocket and artillery units; fire using advanced weapons, focused on destroying opposing units; deploying airborne units to surround the last points of resistance; and terrain clearance operations through ground units.

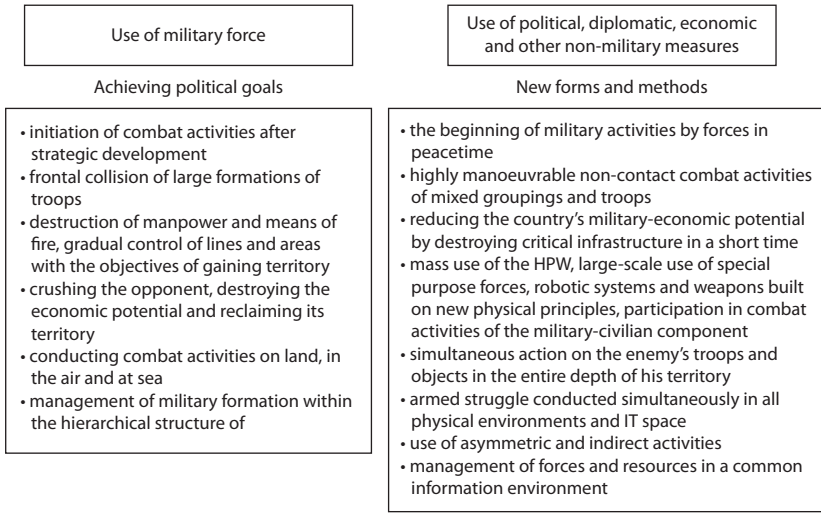

Figure 1: Changes in armed struggle
Source: www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

It follows from the above that the Russian view of conducting modern warfare is based on a theory where the main battlefield is the mind and the main idea of General Gerasimov is the fact that the difference between peace and war is being blurred, and we are now in the stage of permanent war. The public debate is a very good indicator of overall Russian military thinking, including what is hidden from public view. In Russia, the new National Security Strategy (NSS) of the Russian Federation (RUS) was published on 2 July 2021. It is the basic document of Russia's security policy, which defines the national interests and strategic priorities of the RUS, as well as the goals and tasks of the country's security policy. The document states that the strategy is based on inseparable relations and interdependence of the national security of the RUS and the socio-economic development of the country. Among other things, the document talks about the legitimacy of adopting symmetric and asymmetric measures to eliminate hostile actions that would threaten the sovereignty and territorial integrity of Russia. According to the strategy of the U.S. and its allies, they are actively attacking traditional Russian spiritual, moral, cultural and historical values. Foreign non-profit non-governmental, religious, extremist and terrorist organisations are also taking the same steps. The document lists nine strategic national priorities. These are the protection of people, defence, state and public security, information security, economic security, scientific and technological development, environmental security, protection of traditional values, strategic stability. The strategy also sets goals in the country's economic stability, which should eliminate the effects of the adopted sanctions against the Russian Federation. The document replaces the previous security strategy from 2015.[36] It is likely that the Russian Ministry of Defence (MoD) is having both internal and public discussions about hybrid warfare and the future of warfare as such. Much of Russia's discussion of hybrid warfare is conducted in public military journals. The Russian military almost certainly additionally discusses the details of hybrid warfare in secret forums and conducts assessments of the lessons learned about ongoing hybrid wars, such as the Ukraine campaign. However, unclassified publications in Russian reach a larger military audience than classified documents and influence the thinking of more Russian officers. Theories and priorities of the development of the MoD are published in recognised magazines, where senior officers outline the main priority of the Russian Armed Forces, including the

[36] Russian Federation Presidential Decree 2021.

conduct of hybrid warfare.[37] Open discussion of hybrid warfare and the future of warfare benefits the quality of Russia's educational process. Authorship is easier in unclassified publications than in classified ones, which are likely to be limited to select groups of officers and planners. Inputs to the open discussion include contributions from officers with experience in waging war in Syria, which the Kremlin views as a hybrid war. Military academics discuss the future of the conflict in military journals, further discuss how they will synchronise their information campaigns, military veterans and military educators provide historical context for the conduct of the operation, among other things. Public discussion is an iterative process that allows authors to share experiences and learn from each other.[38] Unclassified Russian military discourse occurs in two types of sources such as military doctrine and Kremlin-run intelligence servers. Russia mainly uses military magazines as a forum for discussing past operations and planning future doctrines. Typical Objectives of Russian Hybrid Warfare, as practised today, can have at least three objectives:[39]

1. *Capturing territory without resorting to overt or conventional military force.* This was the objective of Russia's successful annexation of Crimea in 2014, the move that launched the debate over Russian "hybrid strategies". The annexation of Crimea relied heavily on the now infamous "little green men" primarily Russian special forces operating through a newly created Russian special operations command. The use of these elite troops, in conjunction with an information warfare campaign and the deployment of loyal Russian proxies, created circumstances that laid the groundwork for a bloodless conventional takeover of Crimea. Russia used some similar tactics ahead of its 2008 invasion of Georgia. The resulting "frozen conflicts" in Ukraine and Georgia have hampered these countries' efforts towards integration with Western Europe. In a much-referenced 2013 article on modern warfare, Russian Chief of the General Staff General Valery Gerasimov argued that non-military means are used four times more often in modern conflicts than conventional military measures.
2. *Creating a pretext for overt, conventional military action.* Russia's annexation of Crimea generated concerns that the Kremlin might seek to use a hybrid strategy to create a pretext for military action elsewhere, such

[37] Security Council of the Russian Federation 2016.
[38] *Military Thought.* A Russian Journal of Military Theory and Strategy.
[39] Chivvis 2017.

as in the Baltic states. Russia might seek to foment discord between the minority Russian population in a country like Estonia, creating a narrative that portrays the Estonian Government as repressive and then exploiting this narrative to justify a Russian military intervention on behalf of the Russian minority. Such an operation would likely be accompanied by cyber operations aimed at inflaming tensions or complicating national and NATO responses. It would almost certainly be accompanied by efforts to influence broader European and world opinion in ways that favoured Russia's intervention. On the ground, it would involve the use of Russian secret agents and proxies.

3. *Using hybrid measures to influence the politics and policies of countries in the West and elsewhere.* This objective is currently the most pressing challenge for Western governments, including the United States. Here, the Kremlin does not seek to use hybrid strategies as a substitute for military action or as a precursor for war. Instead, it seeks to ensure that political outcomes in targeted countries serve Russia's national interests. Most vulnerable are countries with weak legal and anticorruption measures or where key domestic groups share Russia's interests or worldview. However, even strong countries, such as the United States and Germany, are far from immune.

Moscow has many mechanisms and levers for hybrid war. These are primarily the following:[40]

1. *Information operations.* Russia has become notably more effective in its use of strategic communications to shape political narratives in many countries. Outlets such as *Russia Today* and *Sputnik News* are among the most well-known vectors for this strategy, but Russia also uses targeted television programming; funds European think tanks to promote its views; and employs large numbers of Internet trolls, bots and fake news farms. The objective of these information operations is primarily to muddy the waters and cast doubt upon objective truths and to shape the political discussion in ways that will benefit the Kremlin.
2. *Cyber.* The Kremlin now has access to a growing cadre of cyber warriors that allows it to hack into Western information systems to collect valuable

[40] Chivvis 2017.

information. The information is then used to influence elections and other political outcomes outside Russia's borders.

3. *Proxies.* Russia also uses a range of proxies to further its interests. Proxies are often groups that have broad sympathy with Russia's objectives. One of the Kremlin's typical proxies is the Night Wolves, a biker club and ultranationalist, anti-American gang, whose leader is a friend of President Putin. The exact role of the Night Wolves is uncertain, although it can be used to intimidate populations and may facilitate a range of hybrid activities behind the scenes. Russia also seeks to exploit European protest movements. For example, it backed anti-European Union (EU) groups in a 2016 referendum on trade with Ukraine in the Netherlands. It is also suspected of supporting the anti-shale gas and other protest movements in Bulgaria that have complicated Bulgaria's efforts to reduce its dependence on Russian energy sources.
4. *Economic influence.* Russia uses both direct and indirect economic influence to affect European politics. Moscow used energy as a tool of foreign policy when it shut off the natural gas supplies to Ukraine in the dead of the winter in 2006 and 2009 in an overt effort to coerce Ukraine into agreement on the price of its gas. The indirect influence Moscow has built in Europe, however, may be even more important. Taking advantage of the vast network of natural gas pipelines built in Soviet times, the Russian state-owned gas giant Gazprom and its subsidiaries wield influence over the politics and economics of many European countries. Russia has also offered large-scale investment to build energy pipelines and other infrastructure in countries that are dependent on Russian energy supplies as a means of growing its influence – often through murky backroom deals.
5. *Clandestine measures.* Russia also could use traditional espionage as part of its hybrid methods, bribing, extorting and otherwise attempting to influence vulnerable political figures to further its interests. As part of its broader military modernisation program, Russia has invested in strengthening its special operations forces. These forces have a variety of roles, but one of their most dramatic tasks has been to infiltrate other countries and lead hybrid warfare efforts there. Russian military intelligence, for example, is believed to have instigated a 2016 lot to overthrow the pro-NATO government of Montenegro. Russian Special Forces were crucial in seizing Crimea and supporting separatists in the Donbass, and they are likely operating in several NATO-allied countries.

6. *Political influence.* Of course, Russian leaders also use traditional diplomacy to support their preferred political parties and candidates, offering high-level visits in Moscow and otherwise attempting to champion their claims, while deriding the positions of political leaders more critical of Moscow. Behind these levers lies the implicit threat of Russian conventional and, in the extreme, nuclear force. A discussion of Russia's full military capabilities is unwarranted in this testimony, but it is important to recognise that these higher-end military capabilities are the backdrop against which hybrid warfare is carried out.

Definitions and perceptions

The Russian Army is evaluating war in increasingly unusual, rapid and varied ways in terms of the tools used and the people involved. Russian analysts believe that the West is waging an ongoing hybrid war against Russia. The Kremlin also believes that the likelihood of a conventional war against Russia is declining, and this motivates Russia to engage in other types of conflict, namely hybrid wars, to best prepare for a future war. The Russian Armed Forces define hybrid war as a war in which all efforts, including military operations, are subordinated to an information campaign.[41] The Kremlin does not see hybrid war as a model for all future conflicts. The operational approach within the broader conventional war perceives Russia as a set of means to achieve state policy goals. The Kremlin considers hybrid warfare a state activity, including the use of conventional military force. Russian analysts aim to gain the ability to determine the long-term strategic orientation of the state with the use of hybrid warfare. In Russia's view, victorious states or coalitions in hybrid wars successfully assert their worldview, values, interests, including the allocation of resources to fulfil the state's goal. The winning states or coalitions then gain power and, from the Russian point of view, have the right to determine the future of the country.[42] Researcher of the Academy of Sciences of Russia Kiselev claims that the goal of hybrid art is to divide states and change their governments to achieve their goal (it was the goal of the Arab spring).[43] The Russian army uses a political goal as the primary

[41] Chekinov–Bogdanov 2017.
[42] Bartosh 2018.
[43] Kiselev 2015.

prerequisite for action, while the broader goal is a hybrid war. With its help, they gain control over the worldview and orientation of the state, which is an information goal that requires the use of an information campaign centre.[44] Russian analysts believe that hybrid wars represent protracted conflicts as the aggressor uses a combination of "crush and starve" to undermine the will of the adversary by targeting both its resource and political base.[45] A large set of works by Western authors discusses hybrid means and uses various concepts such as "gray zone conflict", "hybrid warfare", "hostile measures" and more. The Russian military uses several vague terms to describe hybrid assets, loosely defined as any action beyond traditional kinetic operations. Examples include "hybrid conflict", "asymmetric operations", "information warfare", "non-military combat" and "unconventional warfare".[46] The Russian military identifies a broad set of assets that are currently being discussed as the characteristic tools of hybrid warfare. The Russian Armed Forces use the range of conflict objectives to define the boundary between hybrid warfare and international competition. The Kremlin holds the institutional worldview that the West has been waging a hybrid war against Russia since the end of the Cold War. He further claims that his civilised duty is to fight against the West's attempts to dominate the world. The Kremlin also believes it must adapt to the current situation to win this battle. This worldview deeply shapes Russian military development and assessment of future war. The Kremlin notes that many different conflicts are part of this Western hybrid war against Russia. Russian military thinkers argue that the U.S. is trying to maintain its status and is using NATO to consolidate its dominance and limit Russia.[47] Since 1991, Russian analysts have assessed globalisation as a concerted effort by the West to dominate the world.[48] Russian analysts argue that the hybrid war between the U.S. and Russia resembles the Cold War because of its intention to shape the "basic moral core of humanity".[49] This is claimed by the leaders of the Russian armed forces, and this opinion is not marginal. In March 2019, Gerasimov said that the U.S. and its allies are developing offensive capabilities, including a "global strike" in several domains, to remove

[44] Bartosh 2018.
[45] Kiselev 2015.
[46] Gerasimov 2016.
[47] Bartosh 2018.
[48] Chekinov–Bogdanov 2017.
[49] Bartosh 2018.

unwanted governments, undermine the concept of sovereignty, change legally elected governments such as in Belarus, Iraq, Libya, Ukraine and Venezuela.[50] Russian military thinkers assess all these Western actions as an element of a hybrid war against Russia, with Kiselev claiming that "the theory of hybrid war was developed in the bowels of the Pentagon".[51] They also say the U.S. is adapting to the rising costs of conventional operations by developing hybrid warfare. From the Russian perspective, Western hybrid wars are a change from the previous U.S. model of "invasion to restore democracy".[52] Dvornikov, in July 2018 stated that the 1991 Persian Gulf War was the last conventional Western war, and the West now achieves its political goals by forcing the enemy to submit to its will by using other methods. The goal of this Western hybrid war, conducted by using a mix of state forces with international legal coverage and non-governmental organisations, is the creation of an obedient government in the given territory.[53] Russian analysts report that NATO previously "picked a victim" and forced other nations to join a large-scale military operation in Yugoslavia and Iraq in order to eliminate unwanted governments and thus achieve its goals.[54] Gerasimov stated in March 2016 that "the falsification of events and the use of mass media activities can be compared to the results of the large-scale use of troops and forces".[55] Gerasimov cites "Inciting Nationalism in Ukraine" and the results of the Arab Spring as examples of Western hybrid warfare. Western governments can now achieve regime change through hybrid warfare primarily using information warfare rather than conventional force.[56] Prominent hybrid war theorist Bartosh further claims that the West is fine-tuning this model in ongoing operations in Latin America, the Middle East and the Balkans. Other Russian authors specifically cite NATO interventions in Libya, the former Yugoslavia and the Syrian war as key examples of western hybrid warfare.[57] The Kremlin sees the Western hybrid war against Assad in Syria as part of a wider, ongoing Western hybrid war against Russia, with the dual purpose of pressuring Russia and allowing the West to further develop and refine

[50] Gerasimov 2019.
[51] Kiselev 2015.
[52] Kiselev 2015.
[53] Dvornikov 2018.
[54] Kiselev 2017.
[55] Gerasimov 2016.
[56] Gerasimov 2016.
[57] Bartosh 2018.

its approaches to hybrid warfare.[58] This Russian concept, according to which the West is already waging a hybrid war against Russia, forms the basis of the assessment of the future war. The need to reassess the future war is based on "the West's quest for world domination", and it will include activities that would not be considered war according to traditional definitions.[59] If the Russian army does not adapt to the growing importance of hybrid warfare, the Kremlin will lose the civilisation struggle for survival. The Russian narrative about the U.S. and its involvement in global conflicts certainly serves the Kremlin's propaganda interests and often mischaracterises U.S. intent and capabilities. But this story really shapes Russian military thinking and planning. Deeply paranoid and frankly hyperbolic, the worldview ignores superpower conflicts, sidesteps other actors, including China, and presents a truly distorted picture of events in the U.S. Readers may legitimately question whether this worldview is intentional for Russian information operations or propaganda. The Kremlin could intend to use this rhetoric to shape Russian public opinion against the U.S., or to obscure Russian discussions about how to conduct its own hybrid wars while describing any offensive actions by the West.[60] The worldview that the West is applying a hybrid war against Russia permeates official Russian military planning and discussions. The discussion about the Western hybrid war against Russia is not limited to propaganda outlets like *Russia Today* and *Sputnik News.* Arguments and analyses that shape this worldview are published in *Military Thought,* the most respected discussion forum of the Russian Armed Forces. The highest officers of the Russian army argue for this worldview in public speeches in which they clarify the priorities of the armed forces. The researchers mentioned above are recognised military academics and heads of major military research institutions, not fringe analysts or junior officers. In addition, Russian military analysts are openly discussing how to conduct offensive hybrid wars. The Russian Army does not hide its intention to use hybrid means offensively. Russia's conception of continued hybrid warfare against the West shapes strategic priorities and assessments of the future of warfare. Indeed, the Kremlin believes it is on the defensive against a Western hybrid war and is shaping its preparations for a future war based on this assessment.[61] Norwegian scientists

[58] Bartosh 2018.
[59] Chekinov–Bogdanov 2017.
[60] Chekinov–Bogdanov 2017.
[61] Chekinov–Bogdanov 2017.

within the Countering Hybrid Warfare project[62] characterise hybrid warfare as the involvement of state and non-state actors, the use of various means, while the actors' activities may differ. All actors exhibit the capability to synchronise various instruments of power against specific vulnerabilities (weak spots) to create linear and non-linear effects. Hybrid warfare is described as the synchronised use of multiple instruments of power tailored to specific vulnerabilities across a full spectrum of societal functions to achieve synergistic effects. They came to the view that hybrid warfare is asymmetric and uses multiple instruments of power along horizontal and vertical axes. This distinguishes hybrid warfare from an attrition-based approach to warfare, where one force matches the strength of the other, either qualitatively or quantitatively, to degrade the adversary's capabilities. A hybrid warfare actor can synchronise its military, political, economic, civil, information (MPECI) instrument of power to escalate a series of specific effects-producing activities vertically and horizontally. It also shows how a hybrid warfare actor can either vertically escalate by increasing the intensity of one or more instruments of power, and/or horizontally "escalate" through synchronising multiple instruments of power to create effects greater than through vertical escalation alone. The key is to understand that the various instruments of power are used in multiple dimensions and at multiple levels simultaneously and in a synchronised fashion. This type of thinking allows hybrid warfare actors to use the various MPECI means at their disposal to create Synchronized Attack Packages (SAPs) that are specifically tailored to the perceived vulnerabilities of a target system. The instruments of power used will depend on the capabilities of the hybrid warfare actor and the perceived vulnerabilities of its opponent, as well as the political goals of the hybrid warfare actor and its planned ways to achieve those goals. As with all conflicts and wars, the nature of hybrid warfare depends on the context. Ilmari Käihkö[63] in the article *The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession* (2021) emphasises that hybrid warfare and gray zone conflict suggest that success in modern warfare depends on the coordination and combination of military and non-military means. This is not a new argument and has been

[62] Cullen – Reichborn-Kjennerud 2017.

[63] Ilmari Käihkö, PhD is Associate Professor of war studies in the Department of Security, Strategy, and Leadership at the Swedish Defence University.

debated since at least the so-called three block war[64] in the late 1990s. Neglecting to analyse our own experiences in places like Afghanistan and equating Russian action and hybrid war have contributed to a poor understanding of Russia and how we can combine various means and ways to achieve our desired political ends. Associating hybrid war with Russia alone also reflects the absence of a major rethinking of war and warfare in general even though the Afghanistan War alone illustrates how we struggle to wage this kind of war ourselves. It is equally difficult to see any major organisational reforms these new insights have heralded, for instance the need to coordinate and combine military and non-military means. Considering that armed forces do not possess most of the non-military means emphasised by notions of hybrid warfare, it is unsurprising that the use of force and military technology have remained top priorities even in Russia.[65] As its title suggested, even Gerasimov's speech focused on carrying out combat operations and soon turned to high-tech capabilities, including artificial intelligence and robots. Military professionals around the world still assume the centrality of traditional military operations and above all the use of violence in war. This kind of narrow military strategy does not correspond with the emphasis in contemporary conflicts that has shifted from use of force in war to use of nonviolent means below the threshold of war. The evolution of hybrid war indicates that the current emphasis lies in a grand strategy that applies all available means an actor possesses, not in narrow military strategy that focuses on mere violence.

Means used

Wars no longer appear according to typical (classical) templates but change significantly. Russian analysts and senior military officials consider the course of conflicts such as the flower revolutions of the Arab Spring, Ukraine and

[64] The Three Block War is a concept described by U.S. Marine General Charles Krulak in the late 1990s to illustrate the complex spectrum of challenges likely to be faced by Marines on the modern battlefield. In Krulak's example, Marines may be required to conduct full-scale military action, peacekeeping operations and humanitarian aid within the space of three contiguous city blocks. The thrust of the concept is that modern militaries must be trained to operate in all three conditions simultaneously, and that to do so, leadership training at the lowest levels needs to be high.

[65] Renz 2016.

conflicts in the Middle East as examples of hybrid warfare, during which, as experience shows, quite happy countries can turn into an arena of bitter military struggle in a few months or days, or become victims of foreign intervention, plunge into the abyss of chaos, humanitarian disaster and civil war. We already mentioned in the third part of the article that General Gerasimov considers just such wars to be typical wars of the 21st century. According to him, the role of the non-military to achieve political and strategic goals has increased, which in many cases greatly exceed the power of weapons in their effectiveness. On the other hand, Western countries consider it important to investigate the Chechen War (William J. Nemeth), Israel's war against Palestine (Frank Hoffman), the civil war in Syria, the annexation of Crimea, etc. Hybrid War is not a new type of war, but a form of war that has been present since the beginning of written history. The combination of regular and irregular military forces, along with other measures aimed at destabilising the opponent is not new. However, in relation to hybrid struggle in the past, it is a key dimension today to achieve domination in the information field. In the analysed examples of hybrid warfare (Croatia, Ukraine), the importance of achieving information dominance is visible. The use of propaganda psychological struggle in combination with intelligence operations and other types of coercion is aimed at destabilising society and facilitating external intervention aimed at obtaining control of it. A very important means and a characteristic symptom of hybrid warfare is the use of the protest potential of the population (dominant in the conflict of the Arab Spring, Syria, Ukraine). Violence in any form has an important position in the definition of hybrid war. Different means for the guide of hybrid warfare can be considered e.g. classical (symmetrical) and asymmetrical warfare, regular and non-regular armed groups (unmarked, unidentified, insurgents), political, economic and diplomatic missions, propaganda dissemination in various types of media that disrupt the basic principles of democracy, especially through social networks, cyber and activities of organised criminal groups, etc. The important thing is that these activities are carried out synergistically in time and space and with the sole goal: to defeat the opponent, or to impose our will. Schematically, the means of hybrid warfare are shown in Figure 2.

As part of the research at the Armed Forces Academy General Milan Rastislav Štefánik, Slovakia, the team led by Vojtech Jurčák worked on the project "Identifying the Symptoms of Hybrid Warfare". Within research, we analysed the course of hybrid war in Croatia, Ukraine, Georgia, Libya, Israeli–Palestine conflict and Islamic state, and identified the means used to conduct hybrid warfare in

individual conflicts. We analysed the course of the hybrid warfare and concluded that the most common means of guiding a hybrid warfare are:[66]

- political means, focused primarily against the foundation of a democratic state and membership in the Regional or Security Alliance
- information means, represent the spread in the media, social networks, etc.
- cyber means, nowadays an increasingly important area in terms of security and defence policy, as evidenced by the decision of the NATO Summit in Warsaw in 2016, where the Alliance defined cyberspace as the fifth dimension of combat activities
- propagandist means, directed against central state administration bodies, the NATO and the EU membership, constitutional officials and constitutional authorities

In addition to these means, the ways of the protest potential of the population are also used in which the credibility of the constitutional and management bodies of the country is undermined and their decisions are questioned.

Figure 2: Possible means of guiding a hybrid war
Source: Compiled by the authors

[66] Jurčák et al. 2017.

This group also includes asymmetrical means to cause fear in the population by using terrorist attacks, destabilising the security situation, manifestations of extremism, criminal groups, etc.

If we want to operate preventively in relation to hybrid wars, it is necessary to reduce the vulnerability of the areas where these funds are used to wage hybrid wars, which means analysing their weaknesses and then increasing their resilience or restoring the disrupted areas of politically, socially and economically weaker countries. Moscow uses a wide array of subversive tools, many of which are non-military, to support Russian national interests. Moscow is trying to use hybrid warfare to achieve several specific political objectives: to divide and weaken the NATO; subvert pro-Western governments; create excuse for war; attach the area and ensure access to European markets under its own conditions. Experts use the term "hybrid war" in different ways. Currently, several related expressions are used, including "gray zone strategies", "competition without conflict", "active measures" and "new generation war". Despite the subtle differences, all these terms point to one direction: Russia uses several instruments of power with an emphasis on non-military instruments to promote their national interests outside their borders – often to the detriment of the U.S. and the interests of their allies. Russian use of hybrid strategies has increased significantly in recent years. This growth is a key dimension of the overall increase in Russian military capabilities and the antagonistic attitude of the Kremlin towards the West. Of course, Russian sources for hybrid warfare are not infinite, and Russia faces many of the same difficulties as any other country that has to coordinate its multifaceted foreign policy. Its hybrid tactics will also not be effective everywhere. Nevertheless, the U.S. and their allies need a clear understanding of the threat and strategy to effectively face Russian hybrid strategies before the U.S. critical interests are damaged in Europe and elsewhere.

Conclusion

The aim of the article was to analyse the approach of the Russian Federation to hybrid threats, what they consider important, how representatives of the Russian Army perceive this term and its characteristics, what is their goal and how they applied theoretical conclusions and ideas in practice. It is possible to state that General Gerasimov can be considered the creator of the concept of hybrid war, who researched and characterised it based on the conflict of the Arab Spring,

wars in the Middle East, etc., also known as the Gerasimov Doctrine, which is the basis of conventional and unconventional means in hybrid warfare, or also called "new war" or "permanent war". There is also disagreement concerning the notion of gray zone. From the Russian point of view, the entire gray zone is part of a hybrid warfare, which additionally involves the use of military forces above its upper limit. The U.S. debate on hybrid warfare focused heavily on unconventional means of conflict. Russian theorists insist that all conflict is now hybrid in nature. Therefore, the Russian Army is adapting its capabilities to hybrid warfare and does not hide its intention to conduct offensive hybrid warfare, in which political, military, economic, civil and environmental means are used. The challenges posed by Russia's hybrid war and preparations for future wars are not insurmountable. The Western community must fully understand Russian threats and successfully confront the Kremlin. Russia is shaping military and non-military instruments of state power to combat hybrid threats.[67] The Russian military defines hybrid warfare as an effort at the strategic level to shape, direct and geostrategically orient a target state in which all means received, including the use of conventional military forces in regional conflicts, are subject to an information campaign. Russia sees the Venezuelan presidential crisis, the Libyan conflict, the Syrian civil war and the crisis in Belarus and Ukraine as examples of hybrid warfare. The Russian military is actively focusing on preparing for future conflicts and increasing the capabilities it deems necessary to win the hybrid war. In relation to hybrid warfare, there are also critical comments. Hugo Klijn and Engin Yüksel,[68] reflect on the word "hybrid" and consider it a buzzword, which is appropriate because it aims to describe something that is impressive, hardly Russian, and hardly new. After General Gerasimov's article was published, the Russian way of waging hybrid warfare emerged, which was a combination of traditional tools and tactics and preparing for unconventional warfare. The annexation of Crimea was the result of social and political changes in Ukraine and within it a favourable situation for Russia to acquire (legal presence of Russian forces in Sevastopol, majority population, dismal quality of the Ukrainian armed forces) and maintain the availability of the Russian naval forces to warm seas, that was a unique circumstance not "easily reproducible" in another country. Nevertheless, whatever Russia has undertaken since this episode, which otherwise might have been labelled as 'integrated', 'non-linear',

[67] Jurčák et al. 2017.

[68] Klijn–Yüksel 2019.

'cross-domain', 'informational' or even 'public diplomacy' activities, has been grouped under 'hybrid' methods of conflict or, indeed, warfare. Meanwhile, strong evidence that Russian outlets have been actively engaged in influencing, not deciding, election or referenda outcomes in a number of Western countries has boosted the prominence of the 'hybrid' category headings, and tilted interpretation towards disinformation efforts – purportedly serving as precursors to other forms of conflict that are "conveniently categorized as being under the threshold of war". Various authors have, patiently but fruitlessly, debunked the notion of a Russian hybrid warfare doctrine or the newness of some of its apparent components. Rather, it appears the West has attempted to cast a mirror image of its own concepts onto Russian military thinking. By doing so, the West has framed a distracting threat perception that may keep it from addressing the right issues.[69] Both in his now famous 2013 article and in a more recent, March 2019 strategy speech at the Academy of Military Sciences, Gerasimov pointed to the increased role of non-military methods by Western states to achieve strategic objectives. Indeed, according to Russian military thinkers "gibridnaya voyna" is about (Western) attempts to erode the socio-cultural cohesion of the adversary's population, ultimately leading to the replacement of an unfriendly regime by a colour revolution, with minimum (if any) military intervention. It is important to note that in his 2019 speech Gerasimov concluded that the decisive role in conflict is still played by military force.[70]

Questions

1. What is the view of the Western community on hybrid war in relation to Russia?
2. How Russian theorists define the theory of hybrid warfare?
3. What is Russia's view of future conflicts in the world?
4. What measures should the international community take to effectively eliminate hybrid threats?

[69] Klijn–Yüksel 2019.
[70] Klijn–Yüksel 2019.

References

Asymmetric Warfare Group (2016): *Russian New Generation Warfare Handbook.* Online: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

Bartosh, Aleksandr A. (2018): *Strategy and Counter Strategy in Hybrid Warfare.* Online: https://dlib.eastview.com/browse/

Bartosh, Aleksandr A. (2021): Gray Zones as Key Elements of the Current Operational Space in Hybrid Warfare (Part II). *Military Thought,* 30(2), 17–32. Online: https://dx.doi.org/10.21557/MTH.69110446

Blank, Stephen J. ed. (2019): *The Russian Military in Contemporary Perspective.* Carlisle, PA: U.S. Army War College Press. Online: https://publications.armywarcollege.edu/ pubs/3705.pdf

Brühl, Marie von (2016): *Dielo „O vojne" vydala Clausewitzova manželka 1834 po jeho smrti.* Banská Bystrica: Belianum.

Chambers, John (2016): *Countering Gray-Zone Hybrid Threats: An MWI Report.* Modern War Institute at West Point. Online: https://mwi.westpoint.edu/countering-gray-zone-hybrid-threats-mwi-report/

Chekinov, Sergey G. – Bogdanov, Sergey A. (2017): *Evolution of the Essence and Content of the Concept of "War" in the 21st Century.* Online: https://dlib.eastview.com/browse/doc/50724910

Chivvis, Christopher S. (2017): *Understanding Russian "Hybrid Warfare" and What Can Be Done about It.* Santa Monica: RAND. Online: www.rand.org/pubs/testimories/CT468.html

Clark, Mason (2020): *Russian Hybrid Warfare.* Institute for the Study of War. Online: www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

Clausewitz, Carl von (1832): *Vom Kriege.* Berlin: Ferdinand Dümmler. Online: www.clausewitzstudies.org/readings/VomKriege1832/_VKwholetext.htm

Connable, Ben – Young, Stephanie – Pezard, Stephanie – Radin, Andrew – Cohen, Raphael S. – Migacheva, Katya – Sladden, James (2020): *Russia's Hostile Measures. Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition.* Santa Monica: RAND. Online: www.rand.org/pubs/research_reports/RR2539

Cullen, Patrick J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* A Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Dalton, Melissa – Sheppard, Lindsey R. – Donahoe, Megan – Conklin, Matthew – Kiernan, Joseph – Hicks, Kathleen H. – Federici, Joseph – Matlaga, Michael eds. (2019): *Gray Zone Project.* Center for Strategic and International Studies. Online: www.csis.org/grayzone

Defense Intelligence Agency (2017): *Russia's Military Power. Building a Military to Support Great Power Aspirations.* Online: www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf

Dvornikov, Alexander (2018): *Staffs for New Wars.* Online: https://vpk-news((.))ru/articles/43971

Encyclopedia Britannica (s. a.): *Wars, Battles & Armed Conflicts.* Online: www.britannica.com/browse/Wars-Battles-Conflicts

Gerasimov, Valery (2016): *On the Experience of Syria.* Online: https://vpk-news((.))ru/articles/29579

Gerasimov, Valery (2019): *Vectors of Military Strategy Development.* Online: http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1

Ivančík, Radoslav (2016): Hybridná vojna – vojna 21. storočia. *Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje,* 22(22), 205–239.

Joint Chiefs of Staff (2019): *Joint Doctrine Note 1-19. Competition Continuum, 03 June 2019.* Online: www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/ jdn1_19.pdf

Jurčák, Vojtech – Bučka, Pavel – Kredatus, Ondrej – Labuzík, Milan – Ganoczy, Štefan – Sipko, Adrián eds. (2017): *Identifikácia príznakov vedenia hybridnej vojny.* Výskumný projekt. Liptovský Mikuláš: AOS GMRŠ.

Kiselev, Viktor (2015): *Hybrid War as a New Type of War of the Future.* Online: https://dlib.eastview.com/browse/doc/45952340

Kiselev, Viktor (2017): *What Wars the Russian Armed Forces Will Be In.* Online: https://dlib.eastview.com/browse/doc/50729309

Klijn, Hugo – Yüksel, Engin (2019): Russia's Hybrid Doctrine: Is the West Barking Up the Wrong Tree? *Clingendael Magazine,* 28 November 2019. Online: www.clingendael.org/publication/russias-hybrid-doctrine-westbarking-wrong-tree

Kompan, Jaroslav – Hrnčiar, Michal (2021): The Security Sector Reform of the Fragile State as a Tool for Conflict Prevention. *Politické Vedy,* 24(2), 87–107.

Majumdar, Dave (2018): How The Russian Military Turned War-Torn Syria into a Testing Playground. *Task and Purpose,* 31 July 2018. Online: https://taskandpurpose.com/russian-military-syria-weapons-testing

Military Thought. A Russian Journal of Military Theory and Strategy. *East View Information Services.* Online: www.eastview.com/resources/journals/military-thought/

Mueller III, Robert S. (2019): *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* U.S. Department of Justice. Online: www.justice.gov/storage/report.pdf

NATO (2023): *NATO's Approach to Countering Disinformation.* Online: www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

Renz, Bettina (2016): Russia and 'Hybrid Warfare'. *Contemporary Politics,* 22(3), 283–300.

Rose, Frank A. (2018): *As Russia and China Improve their Conventional Military Capabilities, Should the US Rethink its Assumptions on Extended Nuclear Deterrence?* Brookings Institute. Online: www.brookings.edu/blog/order-from-chaos/2018/10/23/as-russia-and-china -improve-their-conventional-military-capabilities-should-the-us-rethink-its-assumptions-on-extended-nuclear-deterrence/

Rossiyskaya Gazeta. Eurotopics. Online: www.eurotopics.net/en/192468/rossiyskaya-gazeta

Russian Federation Presidential Decree (2021): Указ Президента Российской Федерации О Стратегии национальной безопасности Российской Федерации [Decree of the President of the Russian Federation on the National Security Strategy of the Russian Federation]. Online: http://publication.pravo.gov.ru

Security Council of the Russian Federation (2016): *Doctrine of Information Security of the Russian Federation.* Online: www.scrf.gov.ru/security/information/DIB_engl/

Sokolsky, Richard (2017): *The New NATO–Russia Military Balance: Implications for European Security.* Carnegie Endowment for International Peace. Online: https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222

Stratégia národnej bezpečnosti RF 2021. Online: http://mepoforum.sk/staty-regiony/europa/vychodna-europa/rusko/strategia-narodnej-bezpecnosti-ruskej-federacie-2021/

The Government of Hungary (2020): *Hungary's National Security Strategy.* Online: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html

U.S. Congress, House, Armed Services, The Evolution of Hybrid Warfare and Key Challenges 115 Cong., 1st sess., 2017. Online: www.govinfo.gov/content/pkg/CHRG-115hhrg25088/html/CHRG-115hhrg25088.htm

U.S. Department of Defense (2010): *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms.* Online: https://irp.fas.org/doddir/dod/jp1_02.pdf

U.S. Department of Defense (2018): *Summary of the National Defense Strategy of the United States of America*. Online: https://dod.defense.gov/ Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Department of Defense (2022): *National Defense Strategy*. Online: https://apps.dtic.mil/sti/trecms/pdf/AD1183539.pdf

Vladykin, Oleg (2018): *Military Science Looks to the Future*. Online: http://redstar.ru/voennaya-nauka-smotrit-v-budushhee/?attempt=2

Ionuț Alin Cîrdei – Lucian Ispas[1]

The Role of Proxies

The international security environment is a complex reality, a place where divergent interests collide, spheres of influence are drawn, and political, economic or military objectives are sought to be achieved by any means. However, these actions may lead to conflict with other powers that are interested in expanding influence in the same area or want to limit the influence of potential adversaries. Conflicts that arise in different areas of the world can be used by regional or global powers as a tool to promote their own interests, without fuelling tensions that can give rise to a large-scale confrontation with other powers. Regional or global powers may choose to support conflicting parties overtly or covertly during a conflict by providing material support, in the form of weapons, ammunition or military technologies, or in the form of intelligence, avoiding direct involvement in military action. Thus we are witnessing the birth of conflicts that go through intermediaries or proxy conflicts, which are a form of manifestation of the hybrid conflict. In this hybrid conflict, the great powers are involved, which play the role of sponsor, shadow protector and small states or even political, ethnic groups or organisations which play the role of intermediary, instrument of struggle, which actively participate in military actions and which have own objectives, but they also have in mind the promotion of the objectives of the protectors.

Considerations on proxy warfare

Hybrid confrontations are not specific to the modern era, they can be encountered throughout history, but in the modern era proxy wars have acquired a new dimension, becoming the main tool of the great powers.[2] Throughout history, states or even empires have used intermediaries to conduct military campaigns on their behalf, even encouraging them to attack more powerful but inconvenient opponents than the intermediary, in order to advance the sponsor's political and

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] Watts et al. 2023.

DOI: https://doi.org/10.36250/01236_03

military interests. Thus, even the title of client state or client of the Roman Empire or later of the Ottoman Empire appears. The client states enjoyed the protection of the stronger state, its support, but in exchange for the protection, they obliged themselves to carry out military actions in support or even on its behalf, being ex officio allies of the protector in the event of a conflict. Limiting or prohibiting the right to have its own foreign policy actually meant turning the client state into an instrument of the powerful one, which could use it including as an intermediary in smaller or larger confrontations.[3] Proxy wars became more popular when classical warfare became much more complex, when it turned into total war. Thus, with the development of destructive technologies, with the proliferation of weapons with great destructive power and with the extension of their range, war became a confrontation of the entire country, which applied its full power in a military conflict, the battle strategy becoming the art of using all resources and all means to achieve victory. World War I and II are examples of total wars, in which the achievement of objectives was done at an enormous cost to all parties to the conflict, and the military instrument of power was used, along with other instruments, to achieve political objectives. Based on the lessons learned from these two major conflicts, the conclusion was reached that political objectives must be met with as little loss as possible on both sides,[4] because society became increasingly interconnected, and the costs of reconstruction had to be borne by everyone, victors and vanquished alike. When the spectre of the destruction of the planet and the extinction of life on earth became a reality, as a result of the emergence of the nuclear threat, the great powers became much more attentive to the confrontational relationship between them to prevent the outbreak of a new total conflict. The conflict through intermediaries starts from the idea that the enemy of my enemy becomes my ally, and as long as the parties have something to gain, they can develop collaborative relationships, being able to state, based on the analysis of recent conflicts, that "in the 21st century, the most success is to stand aside and let others fight for you".[5] The justification for the widespread use of proxy warfare is that the great powers USA and USSR avoided direct confrontation during the Cold War and thus reduced the chances of a nuclear war to zero. Later, after the end of the Cold War, proxy conflicts continued to exist as they represented a safe and cheap way to obtain strategic

[3] Dzwonczyk 2020.
[4] Lider 1981.
[5] Harari 2018: 176.

advantages with minimal risks, using not only third world states, but also non-state actors and even terrorist organisations, the final state after these conflicts being influenced by the powers that played the role of sponsor and not by the intermediary,[6] thus reinforcing the idea that this kind of confrontation is a form of hybrid warfare that is going on all around us, in all domains and dimensions and by using all means at our disposal. The global competition between the U.S. and the USSR fuelled local conflicts in different areas of the world, especially Africa, the Middle East and Southeast Asia, high-tension areas artificially maintained by regional or global powers. Researchers analysing the Cold War period have concluded that the U.S. and the USSR participated in various forms in about 120 proxy wars that took place in developing states.[7] Even before the Cold War and before the USA asserted itself as a world power after World War I, a position cemented during World War II, some scholars identified Russia as one of the states that used proxy warfare. The Romanov dynasty used the Cossacks as a proxy and as an amplifier of their own fighting power.[8] In the 20th century, the most famous proxy wars are considered to be the Korean War (1950–1953), the Vietnam War (1953–1975), the Suez Crisis (1956–1957), the Angolan Civil War (1975–2002), the war in Afghanistan (1979–1989) and the war in Transnistria (1990–1992). In most of these conflicts, the role of sponsor was played either by the USA in the case of Afghanistan, or by the USSR (later Russia) or China in the case of the wars in Korea, Vietnam, Angola, but there were other regional powers that tried to defend their interests through intermediaries, such as would be France and Great Britain in the case of the Suez crisis. After the collapse of the USSR, proxy wars continued to take place, with other states being involved in the role of sponsor, states that identified regional opportunities. In this sense, we can mention the support given by Pakistan to the Taliban who were fighting in Afghanistan, the support given by Iran to the terrorist organisations Hezbollah and Hamas, the support given by Saudi Arabia, on the one hand and Iran on the other hand, to the fighters in the civil war in Yemen, the support given by the U.S. for Syrian rebels, support for liberation movements known as the Arab Spring or Colour Revolutions, or Russia's support for separatists in Ukraine's Donbas region. These conflicts through intermediaries had a different evolution and led in some cases to the sponsor coming out of the shadow and directly

6 Karabulut–Oğuz 2018.
7 Karabulut–Oğuz 2018.
8 Fox 2019b: 31.

supporting the protected party as its interests were threatened. In the post-Cold War era, the Western states and Russia remained faithful to the idea of avoiding direct confrontation, but tensions did not disappear, mainly due to the fact that Russia, after recovering from the shock caused by the collapse of the USSR, wanted to regain its influence and the international position in Central Asia, the Middle East or the Caucasus.[9] Unlike during the Cold War, when confrontations through intermediaries took place at the state level, in the current period the role of states can be taken by non-state actors, terrorist organisations, private security and military companies, which can be either sponsors or proxies. The basic idea remains the same as the sponsor seeks to achieve its strategic objectives as efficiently as possible, at the lowest possible cost, with the lowest possible exposure both at home and abroad and minimising the risk of being involved in a direct conflict and ensuring that he always can deny any involvement. Most often sponsor states use intermediaries to advance military objectives and fight on their behalf, while non-state organisations and actors may use intermediaries to advance their political objectives and interests, while using the military capabilities of intermediaries to secondary security or logistics tasks and less for offensive actions.[10] The only notable difference between the state-level sponsor–intermediary relationship and that involving non-state actors lies in their potential to support certain actions and perform certain tasks. A variant of conflict by proxy that has been used by both the U.S. and Russia has been the use of private security and military companies to carry out certain military actions. These companies, such as Blackwater (currently Academi), DynCorp or the Wagner Group take security contracts from different states and ensure the protection of important objectives, provide logistical support or even carry out combat actions in different areas of the globe.[11] The most recent proxy conflicts are considered by some researchers to be Operation Inherent Resolve, in which the U.S. and other coalition states fought Islamic State forces in Iraq and Syria through proxy Iraqi and Kurdish groups, defeating them militarily.[12] On the other hand, the war in Ukraine that started in 2014 can be considered a proxy war waged by Russia against Ukraine, through the consistent support provided by Russia to the separatist rebels in eastern Ukraine, in the Donbas

[9] Karabulut–Oğuz 2018.
[10] Moghadam–Wyss 2020.
[11] See Security Degree Hub s. a.
[12] Fox 2022.

region. Russian support consisted of military materials and equipment, intelligence, military trainers and even forces that actively participated in the confrontations, but without the Russian military presence being directly recognised, which amplifies the hybrid nature of the confrontation.[13] Also, even the conflict that broke out in Ukraine in February 2022 can be considered a proxy war waged by the U.S., NATO and other partner states against Russia, using Ukraine as a proxy. This positioning is debatable, but Russian partisans may see the support of money, military equipment, weapons and ammunition, information provided by Western states to Ukraine as an indirect war, as it aims to weaken Russia and achieve certain objectives by Western states. The answer to this question is not very simple, it cannot be seen in shades of black and white, but we believe that this is not a conflict through proxies, because the USA and NATO did not encourage this invasion, they do not have direct and immediate goals to fulfil them, and the support provided is intended to strengthen the defensive capacity of Ukraine, to defend this country against an external and extremely violent military aggression. The support can be seen as a normal reaction of the international community that has no other means to condemn the aggression of a regional power, a permanent member of the UN Security Council, support that consists of a wide range of coordinated measures, taken both economically, politically, diplomatically, as well as militarily. Moreover, Ukraine has its own objectives in this conflict – the defence of sovereignty and territorial integrity, its actions being defensive, which does not fit into the general framework of conducting a conflict through intermediaries, and the thesis of using Ukraine as a means of exhausting Russia and leading a war of attrition does not stand up to logical arguments.

Characteristics of proxy wars

Although proxy warfare was used long before the 20th century, it reached its peak during the Cold War,[14] when the major nuclear powers used this type of warfare as a relief valve for international tensions, to promote interests, to limit the adversary's influence in certain areas, but also as a means of testing some concepts and technologies, without the risk of a direct confrontation, which could

[13] Marples 2022.
[14] Watts et al. 2023: 7.

have degenerated into a nuclear conflict.[15] We can mention here the most representative conflicts through intermediaries from the Cold War period, such as: the war in Vietnam, the war in Korea, the civil war in Angola, the war in Afghanistan (between the USSR and Afghanistan), etc. War through intermediaries differs from other forms of international intervention, in that it takes place on several levels, in several realities, as we have in the foreground the confrontation of the intermediary or intermediaries, and in the second plan we have the confrontation of the sponsors or the sponsor to achieve their own interests and accomplishing one's goals. Proxy wars have occurred and will continue to occur because there will always be sponsors willing to finance the efforts of other states, just as there will always be states or non-state entities willing to act as intermediaries in exchange for military advantages, in exchange for support that can influence the outcome of a confrontation with neighbours or internal or external adversaries. Conflicts through proxies are local or regional military actions, of high complexity and can be defined as "an international conflict between two foreign powers, fought out on the soil of a third country; disguised as a conflict over an internal issue of that country; and using some of that country's manpower, resources and territory as a means for achieving predominantly foreign goals and foreign strategies".[16] From this perspective, proxy warfare can be seen as a low-cost, low-risk way for great powers to achieve their strategic goals while avoiding direct losses and avoiding international exposure, both at political and public opinion level. The better the support is hidden and the degree of direct involvement is reduced, the easier it is for the main power to avoid material and moral responsibility for the results of the conflict and for the consequences of the actions of the smaller state that plays the role of the fighting instrument, of the intermediary.[17] Most of the time, a symbiotic relationship is built between the strong state and the proxy, as both sides have something to gain, at least theoretically, from this relationship. In the specialised literature, the two parts of the symbiotic relationship are called either sponsor and intermediary, or principal and agent. Regardless of the name given to the two entities involved in this collaborative relationship, their role and the characteristics of their actions are the same. On the one hand, the sponsor or principal has the role of protector, supplier of weapons, military equipment,

[15] Mumford 2013.
[16] Karabulut–Oğuz 2018: 78.
[17] Pfaff 2017.

economic and financial assistance, training and advice, information, direct and indirect protection; moreover, it may also provide the element of deterrence against the intervention of other parties in the ongoing conflict. On the other hand, the intermediary or agent plays the role of the working tool, the means by which the sponsor or principal achieves its objectives, even if part of the resources and support provided are used, as is normal, also to fulfil the objectives of the proxy and to strengthening its local or regional position. The intermediary can provide the military means by which the fight against a common adversary is carried out, the collection of information, the securing of areas or the exercise of control over areas in its own name or on behalf of the sponsor.[18] In order for the sponsor–proxy relationship to work, it is necessary that both have consistent advantages from the development of this relationship, and in order for the sponsor to benefit from the maximum freedom of movement, it is necessary that the support it gives is as well disguised as possible, not be obvious because by openly assuming this support the sponsor assumes from the start also the consequences of the conflict it fuels and supports. If the support is provided covertly and the influence exerted on the intermediary is not obvious, the sponsoring state can always deny involvement, shield itself from the direct and indirect effects of the support, manoeuvre if military operations do not go according to plan, and can protect its international reputation and internal and external credibility. In the case of conflict through intermediaries, most of the time the sponsor has more freedom of action, he can choose whether and how to support the proxy, while the proxy of course has the possibility to refuse support or to impose certain conditions, but his freedom to choose is less because the existence of this external support may depend on the fulfilment of its own objectives or even the survival of the state or entity that plays the role of intermediary. A powerful state may choose to use an intermediary because of the advantages that the latter can offer. A powerful state may choose to support a third party because of its potential, for it has certain knowledge or skills, knows the terrain, the population very well, or has certain operational capabilities that make it attractive. One can use as an example the support given by the U.S. to the Kurdish groups that fought the Islamic State in Iraq and Syria.[19] The U.S. has provided air support to Kurdish forces during ground operations, provided intelligence and even deployed special forces elements for a limited period to

[18] Moghadam–Wyss 2020.
[19] Maguire 2020: 5–8.

support Kurdish forces in the fight against ISIS, and the support granted to Kurdish groups led to tensions with other states, such as Turkey. Another argument for the use of intermediaries is related to the costs of a conflict, as it is often more convenient to support certain forces, which assume the main effort and which will settle the human and material losses, as well as the image deficit, than to justify in front of political decision-makers, domestic and international public opinion, human losses, damage caused to the civilian population in the area of operations, etc. We can exemplify the use of private security companies to carry out certain tasks, both by the U.S. in Afghanistan or Iraq, and by Russia in Syria, but also the support of various groups fighting against terrorist organisations in certain areas of Africa or the Middle East. Another advantage of using proxies to achieve political or military objectives is that the sponsoring state can always deny any involvement and distance itself from the negative consequences of the intermediary's actions.[20] Another side of proxy warfare can emerge nowadays, when on the international stage there are not only states as relevant actors, but also non-state actors, terrorist organisations, etc. are beginning to appear, which can become fearsome tools for attacking and harming an adversary or potential adversary. By using non-state organisations as intermediaries, the conflict can be directed to any region, because these organisations, especially terrorist ones, are not tied to a territory to defend and to be the base of operations. They can act in small cells, in any area of the globe and take the conflict right into the territory of the sponsor state's adversary, where they can unleash terror and attack diverse targets with a high degree of vulnerability and exposure and with a high material and moral impact. Also, the internationalisation of crime and the criminalisation of war have become strategic issues, highlighting the complexity of transnational challenges to security, where conflicts between states can be replaced by hybrid wars and other asymmetric conflicts, where there is no clear distinction between crime, terror and war.[21] Therefore, proxy wars where the intermediaries are terrorist or criminal organisations, non-state entities can be much more unpredictable, more difficult to control, their evolution can be more difficult to anticipate, and the consequences can be much more serious, there can be many and more serious violations of the norms of international humanitarian law, etc. because there is no central entity that can be held accountable, accountability being diluted behind an actor with

[20] Ivanov 2020.
[21] Dupont 2003.

no personality, no leadership structures, no legal and moral constraints. Analysing the relations between the sponsor and the intermediary that materialised in the conflicts carried out both in the Middle East and in other areas, it can be observed that there are two types of intermediaries. Those who are forced to act within the conflict, as was the case with the separatist republics of Luhansk and Donetsk that fought to fulfil Russia's goals in the war in Ukraine between 2014 and 2022, and those who act with their own motivation, such as the fact that there is an older conflict with the adversary, that they want to obtain a reward from the sponsor whose interests they promote and defend or improve its position in relation to the sponsor[22] and we can take as an example the intermediaries in Yemen who sought the support of Iran and Saudi Arabia to fulfil their own objectives, and later became tools of the protectors. This situation occurs especially in case of civil wars when, during the conflict, when one or both parties, after the start of the conflict, seek support from outside. While proxy wars can help sponsors achieve their political and military goals, increase their influence in a region, or weaken their adversary, cause damage to their image, etc. They contribute decisively to increasing and perpetuating instability in certain areas as the conflicting parties will be encouraged by external support to seek confrontation rather than peaceful resolution of differences. They will also try to maximise their gains by relying on current and especially future support from the sponsor, who will be forced to support the intermediary in future conflicts. However, proxy wars will not disappear as long as the calculations of the great powers reveal that it is more convenient economically, financially, politically, militarily to support indirect confrontation, which also absolves them of physical and moral responsibility and to avoid a direct, violent, devastating confrontation with effects and consequences that are difficult to anticipate under conditions where weapons of mass destruction have the potential to guarantee mutual destruction.[23] On the international level, a paradigm shift can be observed with regard to proxy wars, in the sense that the place of intermediary states is often taken by local groups, terrorists, insurgents, etc. the relationship between them and the sponsoring state. This can be complicated by the fact that the intermediaries do not always have the same objectives as the sponsors, and the eventual collaboration can be based on momentary interests. Moreover, irregular groups can be difficult to control and rely on because of the way they

[22] Bar-Siman-Tov 1984.
[23] Fox 2019a.

exist, operate, etc. An example in this case could be the Wagner Group which fought for Russia in Ukraine and which at a certain point even organised a revolt against Russia in 2023 or the terrorist group Hamas which, at least declaratively, attacked Israel in October 2023 without the approval or the prior notice of his sponsor, which is Iran. However, proxy wars will continue to exist on the agenda of the great powers, who will find reasons and arguments to settle their accounts, to maintain or expand their influence in certain areas, or to deny this to their adversary. Nowadays, we are witnessing atypical developments on the international scene, where major regional powers want to assert themselves and impose their own agenda, denying the supremacy of the U.S. and NATO, which can create the conditions for a direct, high-intensity conflict between the various blocs. In the current international context it is obvious that proxy war will continue to represent an attractive option for powerful states because it is more convenient for them to fight from a distance without getting directly involved. Even with the use of intermediaries, there will always be the risk of a direct confrontation between rival great powers, with catastrophic consequences regionally or even globally, but the advantages of using intermediaries outweigh the direct and indirect risks and costs. Using intermediaries can create problems in terms of command and control of forces and can increase the risk of conflict escalation, because in the contemporary era we are no longer talking about the existence of a state-level sponsor and intermediary but coalitions of sponsors and intermediaries, some of them being non-state level as well.[24]

The role of proxy

The relationship between the sponsor and the proxy is extremely complex and to understand it one must consider the problems between the sponsor and the intermediary, the role of power in the symbiotic relationship, but also the role of the time factor in this relationship. Following the analysis of these three elements, two models of actions through proxies can be identified: the transactional model and the exploitative model.[25] Regardless of the type of relationship established between the sponsor and the proxy, we must not lose sight of the fact that in all situations it is about the existence of political interests that dictates

[24] Wither 2020.
[25] Fox 2019b.

the need to establish relations between the two parties and that represent the engine of establishing military relations in order to achieve the primary military objectives and through them, the political objectives. Also, cooperation and support relationships involving a proxy have a limited duration, usually set by the sponsor, who will provide support as long as it has the necessary means and as long as its interests require it. The cooperation relationship can also reach an end when the proxy has accumulated enough strength to be able to continue on its own, as was the case with U.S. support for the Syrian opposition fighting ISIS, and as the power of ISIS declined, so did the level of U.S. support as the proxy was deemed strong enough to fend for itself, when the situation that led to the start of the cooperation has changed, when it has fulfilled its objectives or when the sponsor's requests exceed certain limits, beyond which the intermediary is not willing to pass for various reasons. The proxy being the instrument and interface of a sponsor, aiming to achieve his own objectives, but also those of the benefactor. The proxy has greater freedom in choosing the means of war used, and compliance with the rules of the conflict is easier to ignore, just as, in in many cases, when the intermediary is a non-state entity, it is not limited by state-specific international agreements or treaties. For these reasons, the intermediary can wage a total war against the adversary using both conventional and hybrid means.[26] Powerful states may resort to proxy wars not because of the lack of ability to achieve victory in a conflict, but because of objective reasons such as: no vital interests are affected that justify direct military intervention; even if there are vital interests at stake, the risks of direct military intervention are too high; by using an intermediary the crisis can be managed more effectively to avoid direct intervention; there is no internal or external legitimacy to justify military intervention; there are no viable military options for the particular situation at hand, and a proxy offers the possibility of achieving objectives efficiently, with reduced cost and risk.[27] Returning to the two basic models of the proxy–sponsor relationship, the transactional and the exploitative model, we can identify some of their characteristic aspects, as well as the direct and indirect role played by each part of the partnership.[28] The transactional model is based on an exchange between the two parties. The sponsor provides support, protection, information, advice to the proxy in exchange for the promise that it will

[26] Deep–Biberman 2021.
[27] Bar-Siman-Tov 1984.
[28] Fox 2019b.

carry out activities that lead to the fulfilment of the sponsor's objectives, and the intermediary provides the armed hand, which fights against the common adversary, who assumes human, material and image losses in exchange for support from the sponsor. The common point is the desire to defeat a common opponent. In this type of relationship, the proxy has greater negotiating power and it is he who requests the support and can determine how much support and in what form it is provided. In the transactional model, the relationship between the two parties has a limited duration and ends when the objectives are met and when the proxy wants to return to the previous situation, without obligations. Within the transactional relationship, the proxy is not without power, but believes that the involvement of a sponsor increases its chances of success and will therefore try to maximise the benefits they extract from this relationship, with a little surrender of authority, freedom of decision and action in favour of the sponsor. An example of this type of model can be Iraq, which requested the support of the international community, and especially the U.S., to defeat the Islamic State.[29] In case of the exploitative model, most of the time one is dealing with an intermediary with little power and influence, with a limited ability to defend himself or to achieve his goals, and then he accepts the influence of the sponsor, who provides support in exchange for some submission. The sponsor being in a position of power from which he dictates how the relationship evolves, as well as the mode of action of the proxy, who is more of a tool in the hands of a higher power. The exploitative relationship is most often sought by the sponsor, who turns to a state or non-state entity in need of support and who is willing to accept submission in exchange for survival and benefits. The relationship between the two parties works as long as the sponsor has an interest in it. When he sees his goals fulfilled or when he is not satisfied with the actions of the proxy, his agent, he can decide to stop the support and end the relationship.[30] A good example of this exploitative relationship is the case of the support that Russia has given to the separatists in Eastern Ukraine who have formed the two breakaway republics and who wanted independence from Ukraine and even annexation to Russia, but who did not have neither their own economic, financial or other means for own survival, nor the ability to carry out military actions against Ukraine. In this case, Russia is the party that dictated, that established the terms of the relationship, and that will decide how it will evolve, what are the actions carried out by

[29] Fox 2019b.
[30] Fox 2019b.

the separatist forces and, most importantly, will decide what will be the final state and when this partnership will end. Another example of an exploitative relationship can be that between Iran and the terrorist organisations in Palestine, such as Hezbollah or Hamas, which are sponsored to fight against Israel. These groups are supported with weaponry and expertise, intelligence, etc. to oppose Israel, inflict damage on the Israeli military and reduce the influence of the Jewish state in the region in exchange for Iran providing the necessary support, providing some protection and training of the fighters.[31] For proxy warfare to be viable, the proxy needs to be of approximately equal value to its adversary. When the difference in potential is very large, we can hardly speak of a proxy war, which can at best only be used as a *casus belli,* a reason for the sponsoring state to enter into conflict with a regional or global power. This argument can strengthen the idea that the war in Ukraine, the so-called "special military operation" of Russia, is not a war waged by NATO, respectively the U.S. against Russia through Ukraine. For the same reasons, one cannot consider a conflict to be of the proxy type if between the strong state and the supported state there was a prior military agreement of assistance, mutual support or defence in the event of aggression. The relations between the sponsor and the intermediary can be of the most diverse, depending on the characteristics and interests of the two, but in many cases, ideological approaches are what create the conditions for them to consolidate and amplify. Studying the proxy wars of the 20th century in particular, we can see that in many cases the relations between the two were closer when both were animated by the same ideology. When a potential common enemy appeared, it was much easier for them to materialise and to amplify the symbiotic relationship, sometimes without taking into account the risks to which they are exposed or the price paid by the proxy to fulfil the sponsor's objectives. Regardless of the type of relationship established between the sponsor and the proxy, the essence of the partnership remains the same. The sponsor provides various forms of support and protection directly or indirectly, and the proxy acts to fulfil the sponsor's objectives. Within the relationship, depending on the proxy's potential, the sponsor's interests and level of involvement, the intermediary's negotiating ability, etc., each party will have more or less decision-making power, and the proxy may or may not decide what it does, when it does it and how it does it. Its freedom of action is determined by the desire of the sponsor, the degree of exposure of the proxy and its vulnerabilities. The more

[31] Wither 2020.

desperately the intermediary seeks the support of the sponsor, the less freedom of action and decision-making power it will have.[32] The relationship between the sponsor and the proxy can also be favoured by the existence of cultural, economic, ethnic, historical affinities or the appearance of concerns related to the safety of the sponsor due to the proximity of the conflict zone. Other reasons that could encourage the development of the protector–protected relationship can be:

- the sensitivity of public opinion towards the suffering of the victims and the population
- the attempt to discourage a high-intensity conflict
- the creation, maintenance or expansion of spheres of influence
- the desire of obtaining economic advantages in the medium and long term

The sponsor–proxy relationship can be complicated and the importance and appreciation enjoyed by the latter depends on the character, goodwill and interests of the powerful one. There will never be equality in this equation and the sponsor will always want to have the last word, as legitimate reward for the support given. Once a state or group agrees to play the proxy role for an external power, it is virtually bound to act as long as the sponsor requests it and to pursue its own and the sponsor's goals in addition. Any refusal may mean the withdrawal of support and implicitly the possibility of defeat or, worse, the redirection of support to the opponent, who will perhaps be willing to do more. This does not mean that the proxy automatically becomes only an executor, cannon fodder, the party that assumes all the risks. The proxy–sponsor relationship must be mutually beneficial, win–win type, and involve guarantees and advantages for the intermediary.[33] In order for the sponsor–proxy relationship to be effective, it is necessary to have cooperative relations between them prior to the conflict, and the sponsor must be sure that he can control the intermediary, so that there are no serious slippages on his part, which could affect the general interests and the sponsor's reputation, the sponsor must reward the proxy's efforts both during and after the conflict, the sponsor must be ready to bear the consequences of any failure, etc. The relationship between the sponsor and the proxies is extremely complex and differs from one situation to another as the degree of dependence of the intermediary on the sponsor is variable and can change over time. The

[32] Temple 2021.
[33] Fox 2021.

more dependent the proxy is on the sponsor, the more he will be careful to follow the limits set by the sponsor and mainly follow the objectives set by him. When the degree of dependence decreases, then one can witness a desire of the proxy to emancipate, to establish one's own agenda and to prioritise objectives according to one's own interests, as it was the case of the Krajina and Bosnian Serbs who refused to accept peace proposals although their sponsor, Yugoslavia, openly embraced this option or the case of Tamil Tigers in Sri Lanka who refused the accord intermediated by India and preferred secession. Also, regardless of the type of relationship that exists between the proxy and the sponsor, the limits set and the degree of compliance of the intermediary, there is a risk that at some point the sponsor will be tempted or even forced to intervene directly in the conflict, when the proxy is in major danger or when its own interests and objectives may be irreparably harmed.[34]

Objectives in proxy warfare

Conflicts carried out through proxies involve a series of risks for the sponsoring state, such as associating its image with atrocities committed by proxies, violations of international law, supporting increased and unjustified expenses, supporting ideological movements that may have their own agenda in parallel, even the desire for emancipation, the increasing instability and unpredictability of the area, the need to directly support the proxy forces by providing instructors, advisers, specialists, etc.[35] A big problem with proxy conflicts is that the sponsoring state has no clear end state to achieve and no well-defined goals, everything depends on the actions of intermediaries. In a classic conflict, the desired end state is the defeat of the opponent and the creation of favourable conditions for the winning side, while the consequences of a conflict through proxies are limited to weakening it and possibly drawing some limits, some red lines beyond which one must not to pass, to avoid future confrontations.[36] One must bear in mind that the goals of war are not achieved only by military means, military means being complemented by economic, political, diplomatic means, etc.,[37]

[34] Gray 2011.
[35] Moghadam–Wyss 2020.
[36] Bryjka 2020.
[37] Franke 2015.

all these means being employed both directly and through the use of proxies. Conflicts through proxies, whether the role of proxies is played by states or non-state entities, will continue to exist in different areas of the globe and will materialise especially when the objectives of global or regional powers cannot be achieved by using economic or political means. Direct conflict will be avoided as much as possible because its costs are high and war produces dysfunction in all areas, especially in the economic one. Western societies are less and less willing to support a conflict whose justification or necessity they do not understand and agree with. They are even less willing to accept the high casualty and indirect costs, and voluntary participation in the war effort as a member of the armed forces is increasingly less likely due to the transition to professional armies and the removal of the spectre of war from the ordinary population, which is in the second generation without any knowledge of the traumas of a conflict. Nowadays the threat of a classic conflict between great regional or global powers is increasing. At any moment the conflict in Ukraine can degenerate or China can provoke a conflict in East Asia, which can have unforeseen consequences, but the possibility of developing hybrid, asymmetric conflicts, which will lead to the creation of favourable conditions on a regional level for some states is in growth. With this in mind, it can be said that as long as the great powers do not have a direct interest, "developing states seldom have the means to fund expensive wars with neighbours",[38] and proxy wars will exist, as a form of manifestation of the new hybrid conflict as long as there is a sponsor willing to finance the military operations of another state or non-state actor that does not have the capacity or resources to resolve its conflicts locally,[39] in exchange for obtaining favourable circumstances regionally or even globally. The essence of proxy wars lies in the fact that powerful states used smaller states eager to assert themselves as a tool to promote their own objectives, but also to reduce the influence of their opponents in certain areas. This was evident during the Cold War, when the two superpowers chose a hybrid form of confrontation, a proxy war to avoid a direct confrontation, with the risk of using nuclear weapons. The U.S. supported anti-communist or anti-revolutionary movements in various states, in Asia, Africa or Central and South America, while the USSR supported anti-colonial movements and revolutionary movements opposing

[38] Dupont 2003: 10.
[39] Votel–Keravuori 2018.

Western states.[40] Proxy warfare will continue to exist as long as small states and non-state actors are willing to accept the patronage of other states, who play the role of protectors, who provide direct and indirect support in local conflicts, and as long as the great powers are able to settle their differences without a direct involvement in a potentially devastating conventional conflict. We are also witnessing a tendency to replace proxies, which are not only small, developing states, but may be non-state entities or private security companies. Ultimately, proxy warfare is a type of complex hybrid confrontation, which takes place on two parallel planes. On the one hand we observe the confrontation of the proxy or proxies, as the main instrument of struggle and as the main force involved in the conflict, which pays the greater price in terms of human and material losses caused directly and indirectly by military confrontations. On the other hand we are witnessing a confrontation of sponsors, of powerful states that are in the background and feed the war machines. They try to achieve political and military objectives without human costs and with some economic costs arising from support to the intermediary, but which are incomparably lower than the costs of direct involvement in the conflict.[41] The sponsor's intervention in various conflicts to support one of the combatants may have cost-related reasons (an indirect war will always have lower costs than a direct war, both direct, visible and indirect costs related to image, perception, acceptance etc.), related to legitimacy (local fighters are easier to accept and can even gain the support and sympathy of the local population, while foreign forces could be seen as aggressors, invaders, oppressors).[42] Supporting a proxy or accepting support from a regional power is based on the calculations that the parties make regarding the gains and losses that may result from this relationship. The intermediary will most often accept support to reduce a handicap or create an advantage over local opponents to increase their chances of victory in an ongoing conflict or conflict emerging, or even to deter the escalation of tensions and violence. On the other hand, for the sponsor, proxy warfare is a cheap and convenient way to achieve their foreign or domestic policy goals, to increase their influence, to strengthen their presence in certain areas, or to weaken opponents or potential opponents. The sponsor can provide support in organising, training, equipping forces, advising security forces from the lowest level up to the level of political-military decision-makers.

40 Wither 2020.
41 Wither 2020.
42 Moghadam–Wyss 2020.

The U.S. has developed an operational approach that includes this sponsor–intermediary relationship, which is known as the approach[43] to conduct military action with less direct combat involvement of U.S. forces based on three options in terms of engaging in a conflict. Fighting by other, with others and through others, U.S. forces and decision-makers can choose the level of national and international exposure and determine the level of engagement. This approach can mean smaller and more covert support in the early stages of a crisis, which can consist of advice and force training, support that can diversify, amplify and even become overt if the situation goes in the wrong direction for the proxy and thereby endangering American interests and forces. The sponsor's involvement depends on the sponsor's desire to stand out or remain in the shadow. If the sponsor wants to maintain as little visibility as possible on its actions, it will choose that the support is as hidden as possible, so as not to be visible from the outside, and will ask the proxy to maintain the confidentiality of all support actions. If, on the other hand, the sponsor wants its actions to be more open or if the intensity of the conflict increases, then its support will be more open, it will no longer try to hide behind the proxy and induce the impression that it does not have direct interests and goals related to the ongoing conflict.[44] The proxy war strategy represents the art of influencing the course and finality of a conflict, in accordance with the interests of a third party, by supporting an intermediary party, without the need for direct military intervention and without the risks arising from it for the sponsoring state and even for the region or planet,[45] knowing that a direct war between the great powers can degenerate into a total conflict involving the use of nuclear weapons, as is happening today, when various representatives of Russia directly or indirectly threaten with the use of nuclear weapons in Ukraine, if Russia's interests as well as its security would be affected.[46] Making such a decision will trigger chain reactions, and the consequences would be difficult to anticipate, and de-escalation rather difficult to achieve. Launching such an attack would most likely mean entering a path of no return and total annihilation. For these motives, as long as reason still exists and the instinct of self-preservation prevails, any great power will favour the use of hybrid tactics to engage adversaries, and proxy warfare will not be missing from

[43] Votel–Keravuori 2018.
[44] Moghadam–Wyss 2020.
[45] Bryjka 2020.
[46] Schlosser 2022.

the list of options considered. The fluidity and volatility of the international environment, the changes taking place on a regional and global level encourage the use of proxies to achieve the goals of the great powers. Through this way of fighting without getting their hands dirty, the great powers streamline activities aimed at increasing or maintaining influence, with direct and indirect costs as low as possible. However, we must not lose sight of the fact that the relationship between the intermediary and the sponsor does not always go according to plan, that the proxy may have its own agenda and objectives, which are not identical to those of the sponsor, that some actions may have consequences that could not have been anticipated, that the cascading effects cannot be controlled, etc., and the 2nd or 3rd order effects can affect the relations and the image of the sponsoring state.[47] Encouraged by the fact that strategic political, military, or economic objectives can be achieved without directly engaging in costly and bloody wars, some powerful states will support or seek intermediaries, tools to covertly use in a proxy conflict, fought between two powers, but fought on the territory of another country, using the resources, territory and population of another country[48] and avoiding as much as possible direct and violent confrontation with another power, a confrontation that could have devastating economic, political and military consequences. Achieving objectives through the use of proxies will continue to be a hybrid tool of the great powers, who will use pawns on the global chessboard, pawns they can use and even sacrifice at will, without major consequences in many situations.

Conclusion

Proxy warfare is not something new, but it gained notoriety during the Cold War, when the USA and the USSR, representatives of the two great political-military blocs, began to support certain military actions of third countries, through which they pursued their goals and they were trying to prevent their opponents from accomplishing their goals, all while avoiding creating the conditions for a direct confrontation that amounted to the potential destruction of humanity through nuclear war.[49] Proxy warfare during the Cold War period referred to conflicts

[47] Ivanov 2020.
[48] Mumford 2013.
[49] Fox 2021.

between two smaller states, each or at least one of which was supported by a superpower. Support provided by the superpower was limited to the provision of information, expertise, advice, funding, logistical support, armaments or munitions, without its forces being directly involved in military action. Thus, the superpower had the possibility to defend or promote its local or regional interests without exposing itself too much internally or internationally and without this involving major human, material or image risks. Also, there may even be situations where the stronger state is forced to intervene directly in the conflict, when the supported state is defeated or in danger of being defeated. To be able to speak of a conflict through proxies, one must bear in mind that at least one of the parties involved, either states if we are talking about an interstate conflict, or groups or organisations if we are talking about an intrastate conflict, needs to be directly supported by a third state whose interests it promotes directly or indirectly through the conflict. However, we consider that mere economic or humanitarian interests resulting from the sale of arms or military equipment, or the provision of strictly necessary goods, medical equipment, etc., are not sufficient to consider the conflict to be of the proxy type. For these reasons, we can state that it is sometimes difficult to say whether a conflict is of a proxy type or not. If we take the current war in Ukraine as an example, we will be able to consider it a proxy war from the perspective of Russia who accuses NATO and other states of waging a war with Russia by imposing sanctions and providing information and military equipment for the purpose of obviously to weaken Russia. On the other hand, NATO and other states do not consider that by helping Ukraine they are in conflict with Russia, they consider the support a moral, normal act of supporting a country that is the victim of an illegal and unprovoked aggression. We tend to say that this conflict is not a proxy conflict because NATO did not encourage the conflict, did not ask Ukraine to fight Russia and does not want a conflict with Russia, although Ukraine does not refrain from asking for support and even direct intervention of NATO forces to repel Russian aggression.

Questions

1. Is proxy warfare something specific to the post-Cold War period?
2. What are the sponsor's objectives in proxy warfare?
3. What is the role of proxies in this type of conflict?

4. What are the objectives of the sponsor and the proxy in proxy warfare?
5. What characterises the relationship between sponsor and proxy in modern conflicts?

References

Bar-Siman-Tov, Yaacov (1984): The Strategy of War by Proxy. *Cooperation and Conflict,* 19(4), 263–273. Online: https://doi.org/10.1177/001083678401900405

Bryjka, Filip (2020): Operational Control over Non-State Proxies. *Security and Defence Quarterly,* 31(4), 191–210. Online: https://doi.org/10.35467/sdq/131044

Deep, Alex – Biberman, Yelena (2021): *The Proxy Gambit.* Modern War Institute at West Point. Online: https://mwi.usma.edu/the-proxy-gambit/

Dupont, Alan (2003): *Transformation or Stagnation? Rethinking Australia's Defence.* Canberra: Australian National University, Strategic and Defence Studies Centre. Online: https://sdsc.bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/WP-SDSC-374_0.pdf

Dzwonczyk, John (2020): Modern Problems Require Ancient Solutions: Lessons from Roman Competitive Posture. *Landpower Essays,* 15 December 2020. Online: www.ausa.org/publications/modern-problems-require-ancient-solutions-lessons-roman-competitive-posture

Fox, Amos C. (2019a): Conflict and the Need for a Theory of Proxy Warfare. *Journal of Strategic Security,* 12(1), 44–71. Online: https://doi.org/10.5038/1944-0472.12.1.1701

Fox, Amos C. (2019b): Time, Power, and Principal-Agent Problems: Why the U.S. Army Is Ill-Suited for Proxy Warfare Hotspots. *Military Review,* March–April, 30–42. Online: www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/

Fox, Amos C. (2021): Strategic Relationships, Risk, and Proxy War. *Journal of Strategic Security,* 14(2), 1–24. Online: www.jstor.org/stable/27026631

Fox, Amos C. (2022): Ukraine and Proxy War: Improving Ontological Shortcomings in Military Thinking. *Association of the United States Army, Land Warfare Paper,* 148. Online: www.ausa.org/publications/ukraine-and-proxy-war-improving-ontological -shortcomings-military-thinking

Franke, Ulrik (2015): *War by Non-Military Means. Understanding Russian Information Warfare.* Stockholm: Totalförsvarets Forskningsinstitut. Online: https://dataspace.princeton.edu/handle/88435/dsp019c67wq22q

Gray, Colin S. (2011): *Hard Power and Soft Power. The Utility of Military Force as an Instrument of Policy in the 21st Century.* Strategic Studies Institute, U.S. Army War College. Online: www.jstor.com/stable/resrep11431

Harari, Yuval N. (2018): *21 Lessons for the 21st Century.* New York: Spiegel & Grau.

Ivanov, Zoran (2020): Changing the Character of Proxy Warfare and Its Consequences for Geopolitical Relationships. *Security and Defence Quarterly,* 31(4), 37–51. Online: https://doi.org/10.35467/sdq/130902

Karabulut, Bilal – Oğuz, Şafak (2018): Proxy Warfare in Ukraine. *The Journal of Defense Sciences,* 17(1), 75–100. Online: https://doi.org/10.17134/khosbd.427044

Lider, Julian (1981): Towards a Modern Concept of Strategy. *Cooperation and Conflict,* 16(4), 217–235. Online: www.jstor.org/stable/45083525

Maguire, Dylan (2020): *A Perfect Proxy? The United States – Syrian Democratic Forces Partnership.* Blacksburg: Virginia Tech Publishing. Online: https://doi.org/10.21061/proxy-wars-maguire

Marples, David R. ed. (2022): *The War in Ukraine's Donbas. Origins, Contexts, and the Future.* Budapest: Central European University Press.

Moghadam, Assaf – Wyss, Michel (2020): The Political Power of Proxies. Why Nonstate Actors Use Local Surrogates. *International Security,* 44(4), 119–157.

Mumford, Andrew (2013): Proxy Warfare and the Future of Conflict. *The RUSI Journal,* 158(2), 40–46. Online: https://doi.org/10.1080/03071847.2013.787733

Pfaff, Anthony C. (2017): Proxy War Ethics. *Journal of National Security Law and Policy,* 9(2), 305–353. Online: https://jnslp.com/wp-content/uploads/2018/01/Proxy_War_Ethics_2.pdf

Schlosser, Eric (2022): What if Russia Uses Nuclear Weapons in Ukraine? *The Atlantic,* 20 June 2022. Online: www.theatlantic.com/ideas/archive/2022/06/russia-ukraine-nuclear-weapon-us-response/661315/

Security Degree Hub (s. a.): *30 Most Powerful Private Security Companies.* Online: www.securitydegreehub.com/most-powerful-private-security-companies-in-the-world/

Temple, Brandon (2021): *The Formation of Proxy Force and External State Relationships: Prospect Theory and Proxy Force Decision Making.* Dissertation. The University of Southern Mississippi. Online: https://aquila.usm.edu/dissertations/1969

Votel, Joseph L. – Keravuori, Eero R. (2018): The By-With-Through Operational Approach. *Joint Force Quarterly,* 89, 40–47. Online: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89_40-47_Votel-Keravuori.pdf?ver=2018-04-11-125441-307

Watts, Stephen – Frederick, Bryan – Chandler, Nathan – Toukan, Mark – Curriden, Christian – Mueller, Erik E. – Geist, Edward – Tabatabai, Ariane M. – Plana, Sara – Corbin, Brandon – Martini, Jeffrey (2023): *Proxy Warfare in Strategic Competition. State Motivations and Future Trends.* Santa Monica: RAND. Online: www.rand.org/pubs/research_reports/RRA307-2.html

Wither, James K. (2020): Outsourcing Warfare: Proxy Forces in Contemporary Armed Conflicts. *Security and Defence Quarterly,* 31(4), 17–34. Online: https://doi.org/10.35467/sdq/127928

Anna Molnár[1]

The Role of the European Centre of Excellence for Countering Hybrid Threats

The aim of this descriptive chapter is to summarise the tasks and roles of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). In order to understand the reasons behind the creation of this new tool it is important to describe the process leading to that and the cooperation between the European Union (EU) and the North Atlantic Treaty Organisation (NATO). At the beginning of the 2000s 'hybrid warfare' was defined by U.S. Marine Corps Lieutenant Colonel Frank G. Hoffman as a "combination of new technologies and fanatical fighting styles without state structures, uniforms or obedience to the laws of armed conflict".[2] Although the definition of this term has been changed since then, the concept of hybrid warfare is closely connected to the concept of hybrid threats.[3] The deteriorating security environment in the Southern neighbourhood following the Arab Spring in 2011 and the aggression of the Russian Federation against Ukraine in 2014 became decisive factors for policy makers of the EU and NATO regarding hybrid threats to foster stronger cooperation between the two organisations. The member states and EU institutions started to put greater emphasis on the capacity building, identification of hybrid threats, raising awareness and joint responses. The annexation of Crimea was described as one of the first examples of hybrid warfare.[4] According to the definition of Simon Sweeney and Neil Winn (2022) hybrid threats include manipulation of the information environment, cyberattacks on critical infrastructure, interference in elections, direct and indirect financial support and economic coercion of political actors, and subversion of the civil society.[5] Robert Johnson uses the term as "protracted forms of warfare, use of proxy forces for coercion and intimidation, terrorism and criminality to manipulate the information environment,

[1] Ludovika University of Public Service.
[2] Johnson 2018: 141; Hoffman 2006.
[3] Johnson 2018; Balcaen et al. 2022.
[4] Renz 2016.
[5] Sweeney–Winn 2022.

DOI: https://doi.org/10.36250/01236_04

target energy resources, attack economic vulnerabilities and exploit diplomatic leverage".[6] It is not a coincidence that all these factors have created breeding ground for the creation of a new European Centre of Excellence for Countering Hybrid Threats in Helsinki, in 2017.

Cooperation between the EU and NATO

Security threats to and within the EU have intensified and acted as an incentive to strengthen the role of the NATO and that of the Common Security and Defence Policy (CSDP) of the EU. The worsening relationship between the West and Russia since 2014, the migration–refugee crisis in 2015 and the 2016 U.S. presidential election have all acted as a spurs to an improved relationship between the NATO and the EU. During the last decade these two organisations were forced by the weakening of multilateralism and the return to great power politics to bolster their positions as international security actors. After the adoption of the EU Global Strategy (GS) in 2016, this process has been accelerated.[7] The EU GS emphasises the need to deepen Transatlantic relationships and links with NATO in order to strengthen collective security.[8] One of the most important and tangible results of the improved cooperation between the EU and NATO was the establishment of the European Centre of Excellence for Countering Hybrid Threats in 2017.[9] The year 2016 can be considered an important turning point in the relations between the EU and NATO. From that year, an intensified relationship between the two international security organisations has been established in the implementation process following the adoption of the EU Global Strategy (GS). The document stressed that Europeans should take greater responsibility for their own security, ready to deter, respond to and protect themselves against external threats.[10] The text emphasises that while NATO provides the primary framework for collective defence of most Member States, Europeans must be able to protect Europe, addressing internal and external challenges "such as terrorism, hybrid threats, cyber and energy security, and organized crime and external

6 Johnson 2018: 145.
7 Molnár 2019.
8 European External Action Service 2016; Molnár 2019.
9 Hybrid CoE 2017a.
10 European External Action Service 2016.

border management. […] A more credible European defence is essential also for the sake of a healthy transatlantic partnership with the United States."[11] The strategy, taking into consideration also the non-NATO member states, intends to strengthen the relationship between the EU and NATO, primarily based on synergies and complementarity.[12] Immediately after the adoption of the EU GS, the relationship between the two organisations improved. At the NATO Summit in Warsaw on 8 July 2016, the President of the European Council, the President of the European Commission and the NATO Secretary General signed a joint declaration on EU–NATO cooperation. This included seven areas of information sharing and concrete cooperation:[13]

- countering hybrid threats
- operational cooperation, including on maritime and migration issues
- cybersecurity and defence capabilities
- defence industry and research
- exercises
- support for the capacity-building efforts
- resilience of the Western Balkan and Eastern and Southern European partners

To enhance staff-to-staff cooperation, points of contact were established in both organisations, and reports monitoring the implementation were published annually, and countering hybrid threats became one of the most significant fields of strengthened cooperation.[14] Although a NATO Permanent Liaison Team was created within the EU Military Staff in 2005 and an EU Cell at SHAPE (NATO's strategic command for operations in Mons, Belgium) was established in 2006, therefore further improvement of close cooperation was urgently needed. NATO and the EU meet on a regular basis to discuss issues of common interest. Since 2016 the NATO Secretary General meets regularly his EU counterparts and has delivered addresses at the European Parliament's Foreign Affairs Committee and the sub-committee on Security and Defence. Meetings have been intensified "at the level of foreign ministers, ambassadors, military representatives and defence advisors". The staff-to-staff meetings have been organised between

[11] European External Action Service 2016: 20.
[12] European External Action Service 2016.
[13] NATO 2016a.
[14] NATO Watch 2017.

NATO's International Staff and International Military Staff, and the European External Action Service, the European Defence Agency, the EU Commission and the European Parliament. Permanent military liaison positions have been created to exchange ideas and information and to strengthen cooperation.[15] It is worth mentioning that informal meetings of EU and NATO heads of state and government have been organised by "transatlantic dinners" to avoid the conflict between Turkey, Cyprus and Greece.[16]

EU strategies and actions

In 2016, the European Commission and the High Representative of the EU prepared the first relevant document regarding hybrid threats of the EU, entitled *Joint Framework on Countering Hybrid Threats.* The policy paper included the definition and several responses to the threats.[17] The document mentioned the need for establishing a Hybrid CoE addressing hybrid threats in order to focus on researching how hybrid strategies have been applied, and to encourage the development of new concepts and technologies within the private sector and industry to help Member States build resilience. It aims to align EU and national policies, doctrines and concepts, and to ensure that decision-making can take into consideration the complexities and ambiguities associated with hybrid threats. According to the proposition of this policy document one of the tasks of the Hybrid CoE will be designing programmes to advance research and exercises to find practical solutions to existing challenges posed by hybrid threats. The activities of the Hybrid CoE will be based on expertise developed by its multinational and cross-sector participants from the civilian and military, private and academic sectors working together with EU and NATO centres of excellence.[18] The document defined hybrid threats as: "The concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is

[15] NATO 2016b: 1.
[16] Droin 2023.
[17] European Commission 2016.
[18] European Commission 2016.

usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats."[19] In 2016, the Hybrid Fusion Cell was created within the EU Intelligence and Situation Centre of the European External Action Service in order to improve situational awareness and support decision-making of EU institutions and Member States. The Fusion Cell prepares assessments and briefings based on open source information from different stakeholders concerning hybrid threats. The Hybrid Fusion Cell works in close cooperation with the Hybrid CoE in Helsinki.[20] In 2018, the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats was presented by the European Commission and the High Representative. The document stated: "Hybrid activities by State and non-state actors continue to pose a serious and acute threat to the EU and its Member States. Efforts to destabilise countries by undermining public trust in government institutions and by challenging the core values of societies have become more common. Our societies face a serious challenge from those who seek to damage the EU and its Member States, from cyber-attacks disrupting the economy and public services, through targeted disinformation campaigns to hostile military actions."[21] According to the document "hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors. The nerve agent attack in Salisbury on 4 March 2018 further underlined the versatility of hybrid threats and the multitude of tactics now available. In response, the European Council highlighted the need to step up the capacity of the EU and its Member States to detect, prevent and respond to hybrid threats in areas such as cyber, strategic communication and counterintelligence. It also drew particular attention to the need for resilience in the face of Chemical, Biological, Radiological and Nuclear-related threats."[22] The European Commission published the document *The EU Security Union Strategy 2020–2025* in 2020. The strategy presented

[19] European Commission 2016: 2.
[20] European Commission 2018.
[21] European Commission 2018: 1.
[22] European Commission 2018: 4.

a new comprehensive approach to hybrid threats. This new approach proposing the use of the various tools at the disposal of the EU and integrating external and internal dimension aimed to establish stronger intelligence cooperation with Member States' competent services through the EU Intelligence Analysis Centre (INTCEN), in order to better counter hybrid attacks by state and non-state actors, covering the full spectrum of action – from early detection, analysis, awareness, building resilience and prevention through to crisis response and consequence management.[23] Another very important achievement was the fact that the European Parliament established a Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE committee) in 2020. The INGE organises hearings with experts in order to discuss relevant topics. The task of the INGE committee is to assess the level of hybrid threats in different spheres such as:[24]

- major national and European elections across the EU
- disinformation campaigns on traditional and social media to shape public opinion
- cyberattacks targeting critical infrastructure
- direct and indirect financial support and economic coercion of political actors and civil society subversion

In February 2022 (just a few weeks before the unprovoked aggression of Russia in Ukraine), the Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE), together with the Subcommittee on Security and Defence (SEDE) and the Delegation for relations with the NATO Parliamentary Assembly (DNAT), with the NATO StratCom Centre of Excellence exchanged ideas about topics related to "Russia's Strategy in cyberspace, China as a narrative challenge for NATO Member States and the emerging issues in the digital domain".[25] After a two-year process, the Council of the EU adopted the Strategic Compass in 2022, which is an ambitious plan for a stronger EU security and defence policy by 2030. The Strategic Compass aims to create a new Hybrid Toolbox in order to bring together different instruments to detect and respond to a broad range of hybrid threats and to address foreign information manipulation and interference. The document highlights that hybrid

[23] European Commission 2020.
[24] Welcome to INGE by Chair Raphaël Glucksmann.
[25] European Parliament 2022: 5.

threats are growing in frequency and impact by mentioning China and Russia. The Strategic Compass emphasises that state and non-state actors are using hybrid tactics, cyberattacks, disinformation campaigns, direct interference in elections and political processes, economic coercion and the instrumentalisation of irregular migration flows. Within the European External Action Service the Single Intelligence Analysis Capacity (SIAC), in particular the Hybrid Fusion Cell, provides foresight and situational awareness. The staff of the Hybrid Fusion Cell which is part of the Intelligence and Situation Center (INTCEN) prepares documents, reports and analysis in the framework of the SIAC. This later combines civilian and military intelligence capacities of the EEAS in order to strengthen societal and economic resilience, protect critical infrastructure, democracies and the EU, and national electoral processes. The Strategic Compass plans to create EU Hybrid Rapid Response Teams to support Member States, CSDP missions and operations and partner countries in countering hybrid threats. There is need to further develop counter-hybrid cooperation with NATO.[26]

Establishing the Hybrid CoE

In 2016, NATO and the EU recognised countering hybrid threats as a priority for cooperation and released the Joint Communication by the European Commission and the High Representative to the European Parliament and the Council entitled *Joint Framework on Countering Hybrid Threats. A European Union Response* which mentioned first the need for establishing the new Hybrid CoE.[27] The joint communication stated that "building on the experience of some Member States and partner organisations, one or a network of multinational institutes could act as a Centre of Excellence addressing hybrid threats. Such a Centre could focus on researching how hybrid strategies have been applied, and could encourage the development of new concepts and technologies within the private sector and industry to help Member States build resilience. The research could contribute to aligning EU and national policies, doctrines and concepts, and to ensuring that decision-making can take account of the complexities and ambiguities associated with hybrid threats. Such a Centre should design programmes to advance research and exercises to find practical solutions to existing challenges posed by hybrid

[26] Council of the European Union 2022.
[27] European Commission 2016.

threats. The strength of such a Centre would rely on the expertise developed by its multinational and cross-sector participants from the civilian and military, private and academic sectors. Such a Centre could work closely with existing EU and NATO centres of excellence in order to benefit from insights into hybrid threats that have been gained from cyber defence, strategic communication, civilian military cooperation, energy and crisis response."[28] EU Member States were invited to create a Centre of Excellence for 'countering hybrid threats'. The proposal was mentioned in the document on the implementation of the joint EU–NATO Declaration approved by the Council of the EU and the NAC on 6 December 2016.[29] The Hybrid CoE was established on 11 April 2017 as one of the key factors of the improved cooperation between NATO and the EU. The new network-based international organisation has domestic legal personality in Finland.[30] The Centre was created by the Memorandum of Understanding (MoU) signed by the first nine participating states.[31] During the first meeting of the Steering Board, the first Chairman was elected and the Hybrid CoE's role and structure were also discussed.[32] According to the MoU, the Hybrid CoE aims to follow a comprehensive, multinational, multidisciplinary and academic-based approach.[33] Although NATO and the EU are not signatories themselves, they play an important part in the activities of the Hybrid CoE. The unique character of it is given by the fact that "it is the only actor having both the EU and NATO work and conduct exercises together, with activities covering a wide range of domains from civil to military, and from hostile influencing to hybrid warfare".[34]

Participating states

The Centre was created to operate as a "hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special

[28] European Commission 2016: 5.
[29] Hybrid CoE 2017a.
[30] Hybrid CoE s. a.
[31] The first participating states are Finland, Sweden, the United Kingdom, Latvia, Lithuania, Poland, France, Germany and the United States.
[32] Hybrid CoE 2017c.
[33] Hybrid CoE 2017b.
[34] Hybrid CoE 2017b: 3.

focus on European security".[35] The Hybrid CoE is an independent international organisation. EU and NATO countries are encouraged to take part in the network-based operation of the organisation in order to promote "whole-of-government and whole-of-society approach to countering hybrid threats".[36] Nine countries signed the MOU and nowadays there are 35 Participating States, see table below.[37] The cross-governmental, cross-sectoral network-based organisation helps the efficient cooperation between the different independent actors in order to create state-of-art products and services for the whole network to prevent and counter hybrid threats effectively.

Table 2: Participating States of the Hybrid CoE

Year	Participating States
2017 April	Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, the United Kingdom, the United States
2017 July	Estonia, Norway, Spain
2018	The Netherlands, Italy, Denmark, the Czech Republic, Austria, Canada, Romania, Cyprus
2019	Greece, Hungary, Luxembourg, Montenegro, Portugal, Slovenia, Turkey
2020	Slovakia
2021	Croatia, Belgium, Iceland
2022	Malta
2023	Ireland, Bulgaria, North Macedonia

Source: Hybrid CoE 2017c

The Secretariat is located in Helsinki, Finland. It plans and coordinates the activities and general functions of the Hybrid CoE and manages the work of the networks. The first Director of the Secretariat is Teija Tiilikainen, a renowned scholar and former director of the Finnish Institute of International Affairs. The Secretariat is also in charge of preparing and organising the meetings of the Steering Board, as well as the cooperation with the Participating States, the EU and NATO, and building and maintaining networks. Participating States can provide employees on secondment to the Secretariat. The annual core budget amounts to 3.6 million euros. Half of this is provided by the host nation Finland,

[35] NATO Watch 2017: 4.
[36] NATO Watch 2017: 2.
[37] Hybrid CoE 2017b.

and the other half is covered by participation fees paid by the 35 Participating States.[38] The Steering Board of the Hybrid CoE is the main decision-making body. It consists of representatives from the Participating States. The Staff representatives from the EU and NATO are invited to be present at the meetings of the Steering Board. "The Steering Board establishes policies, adopts internal regulations, and approves the work programme, the budget and the accounts, the annual participation fees, and the admission of new Participating States. It also approves such guidance that may be necessary for the functioning of Hybrid CoE and its organs. The Steering Board is led by the Chair, who is currently Mr Jori Arvonen."[39]

Table 3: Hybrid CoE organisation

Mission		
is to strengthen its Participating States' and organisations' security by providing expertise and training for countering hybrid threats		
Vision		
is a world in which our open, democratic societies operate free of hostile outside interference		
Key tasks		
It is a centre of excellence which promotes the countering of hybrid threats at strategic level through research and training.	It creates multinational networks of experts in comprehensive security.	It serves as a platform for cooperation between the EU and NATO in evaluating societies' vulnerabilities and enhancing resilience.
Steering Board (Chair)		
Secretariat (Director)		
Three Community of Interest (COI) networks		
Hybrid Influence	Vulnerabilities and Resilience	and Strategy and Defence
Teams		
The Research and Analysis Team	The Training and Exercises team	

Source: Compiled by the author based on Hybrid CoE 2017c; NATO Watch 2017

The Hybrid CoE's key task is to build its Participating States' capabilities to prevent and counter hybrid threats. This goal is accomplished by multinational and multidisciplinary "sharing best practices, providing recommendations, as well as testing new ideas and approaches. The Centre also builds the operational

[38] Hybrid CoE 2017c.
[39] Hybrid CoE 2017c.

capacities of the Participating States by training practitioners and organizing hands-on exercises."[40] Hybrid CoE has three Community of Interest (COI) networks:[41]

- Hybrid Influence
- Vulnerabilities and Resilience
- Strategy and Defence

The networks are managed by the Secretariat. The cross-governmental, cross-sectoral networks of the Hybrid CoE involve more than 1,500 practitioners and experts from the Participating States, the EU and NATO, the private sector and academia. The main task of the Hybrid CoE is to facilitate the conversation on hybrid threats by publishing publications and organising events in order to better understand and counter hybrid threats. The Secretariat provides space to coordinate actions.[42] "The Research and Analysis team supports the Centre's work by advancing academic research and debate on relevant topics. It hosts a comprehensive network of academic experts. The COIs participate in the research function's work by providing input from their activities. The Training and Exercises team plans and facilitates table-top and experimental exercises with different hybrid threat scenarios, acting as an enabler and implementer."[43]

Progress reports

All of the seven progress reports on implementing the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 emphasised the key importance of countering hybrid threats in EU–NATO cooperation as 20 out of the 74 proposals concentrated on this field. The first progress report, issued in June 2017, highlighted joint actions against hybrid threats.[44] One of the most important results of this cooperation was the 2017 establishment of the Hybrid CoE in Helsinki. This stemmed from a Finnish initiative, but was carried out with the support of the EU and NATO. Thus the main task of the new centre

40 Hybrid CoE s. a.
41 Hybrid CoE s. a.
42 Hybrid CoE s. a.
43 Hybrid CoE s. a.
44 NATO 2017a.

is to "assist member states and institutions in understanding and defending against hybrid threats" by analysing the cybersecurity challenges, disinformation operations and strategic communication.[45] The Hybrid CoE additionally provides an opportunity to organise informal meetings between the NAC and the EU Political and Security Committee, and thus develop coordinated action against the hybrid threats.[46] According to the second progress report, 12 EU Member States and NATO Allies, staffs joined the Hybrid CoE's Steering Board in 2017. The fact that the High Representative – Vice President of the EU and the Secretary General of NATO took part in the official inauguration ceremony of the Hybrid CoE significantly increased the prestige of the event. During the first year, the first classified document of the Parallel and Coordinated Analysis was prepared. The EU Hybrid Fusion Cell and the NATO Hybrid Analytical Branch started discussions about how to best use the capability of the newly created Hybrid CoE. They also maintained consultations on strategic communication support for Ukraine, Bosnia and Herzegovina, the Republic of Moldova and Georgia. Staff-to-staff contacts and information exchange went on between NATO and EU resilience experts in critical strategic sectors for further work in the area of critical infrastructure protection. They also continued to exchange information on NATO's baseline requirements for national resilience and their integration in the NATO Defence Planning Process. In the framework of NATO's Resilience Advisory Support teams, the EU participated with observer status in NATO's advisory mission to Romania. Staff-to-staff contacts aimed to ensure that the implications of hybrid threats are addressed in a coherent way in the EU Capability Development Plan (CDP) and the NATO Defence Planning Process (NDPP).[47] According to the third progress report on implementing the common set of proposals, published in May 2018, the EU Hybrid Fusion Cell, the NATO Hybrid Analysis Branch and the Hybrid CoE continued to work in close cooperation. They also proposed to establish trilateral cooperation using open source material. Two other Parallel and Coordinated Analyses were finalised regarding the Eastern and Southern Neighbourhood. The EU and NATO staffs took part in the Hybrid CoE's activities, participating in workshops, seminars and exercises. In March, EU and NATO staffs meeting focused on improving 1. early warning and situational awareness; 2. strategic communication and

[45] Hybrid CoE s. a.
[46] Hybrid CoE 2018; Molnár 2019.
[47] NATO 2017b.

messaging; 3. crisis response; 4. resilience; and 5. cyber defence and energy security. In May 2018, the Centre of Excellence facilitated a scenario-based workshop *Harbour Protection Under Hybrid Threat Conditions* organised by the EU and attended by staffs of both organisations.[48] The fourth progress report on implementing the common set of proposals emphasised that "the European Centre of Excellence for Countering Hybrid Threats in Helsinki has made impressive progress with a growing membership, consensus approved work programme and a fully functioning budget".[49] Several events, including seminars, workshops and conferences were organised. Experts from the Hybrid CoE's have briefed EU and NATO committees on several occasions.[50] The fifth progress report in 2020 highlighted that the Hybrid CoE in Helsinki has a crucial role in supporting the NATO and the EU with a growing membership (27 participating states). The Hybrid CoE organised workshops, including one on harbour protection against hybrid threats in October 2019, which included a Table Top exercise, and another on the impact of disruptive technologies in hybrid threats in February 2020, as part of the project called *Hybrid Warfare and Future Technologies.* The effective cooperation between the staffs of the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch and the Hybrid CoE continued "to develop through monthly staff-to-staff exchanges with the aim of strengthening situational awareness, mutual understanding of respective activities, as well as to explore further potential cooperation avenues".[51] According to the sixth progress report of 2021, 30 members participated in the work of the Hybrid CoE, which supported various scenario-based discussions, workshops and exercises, with active participation of the staffs of the EU and NATO. The Director of the Hybrid CoE briefed NATO Member States and selected partner countries on Hybrid CoE's activities in February 2021. Hybrid CoE continued to work in close cooperation with the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch monthly. The two staffs prepared three new Parallel and Coordinated Assessments.[52]

According to the seventh progress report on implementing the common set of proposals in 2021 and 2022, the EU and NATO staffs continued to participate in activities organised by the Hybrid CoE. Both staffs participated in its Steering

[48] NATO 2018.
[49] Hybrid CoE s. a.
[50] NATO 2019.
[51] NATO 2020: 2–3.
[52] NATO 2021.

Board meetings. The Centre had 32 NATO Allies and EU Members States: "The Hybrid CoE hosted the main exercise for the 'Resilient Civilians' project, which brought together senior-level government officials and experts from EU Member States and NATO Allies." The number of staff-to-staff meetings increased, and the exchange of information between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch continued. Four new Parallel and Coordinated Assessments were published.[53] The eighth progress report emphasised that staff interactions on countering hybrid threats remained in the framework of the Hybrid CoE. Staffs of the EU and NATO participated in the Steering Board meetings and in the third High-Level Retreat, in October 2022. The Hybrid CoE organised a scenario-based discussion on hybrid threats from Russia and China and possible EU and NATO answers. A pilot course on *The Contribution of Cyber in Hybrid Conflict* was organised by the European Defence Agency (EDA) with the support of the NATO Cooperative Cyber Defence Centre of Excellence. The cooperation between the NATO Joint Intelligence and Security Division Hybrid Analysis Branch and the EU INTCEN Hybrid Fusion Cell further developed preparing assessments on various topics.[54]

Conclusion

The deteriorating security environment created a breeding ground for increased cooperation between the EU and NATO. 2016 marked as a turning point and significant steps has been made since then. As a consequence, effective cooperation between the EU and NATO has become a daily routine, the two organisations are complementing each other in the field of countering hybrid threats. Both member states and the two international organisations put emphasis on the effective implementation of the common guidelines and measures.

[53] NATO 2022: 2–3.
[54] NATO 2023: 3.

Questions

1. Please describe the main reasons behind the closer cooperation between the European Union and NATO.
2. When was the European Centre of Excellence for Countering Hybrid Threats established?
3. Please summarise the main roles of the European Centre of Excellence for Countering Hybrid Threats.
4. Which are the participating states of the European Centre of Excellence for Countering Hybrid Threats?

References

Balcaen, Pieter – Du Bois, Cind – Buts, Caroline (2022): A Game-theoretic Analysis of Hybrid Threats. *Defence and Peace Economics,* 33(1), 26–41. Online: https://doi.org/10.1080/10242694.2021.1875289

Council of the European Union (2022): *A Strategic Compass for Security and Defence. For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security.* Brussels, 21 March 2022 (OR. en), 7371/22. Online: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

Droin, Mathieu (2023): NATO and the European Union: The Burden of Sharing. *Center for Strategic and International Studies,* 17 January 2023. Online: www.csis.org/analysis/nato-and-european-union-burden-sharing

European Commission (2016): *Joint Communication of the European Commission and the High Representative Presented to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union Response.* JOIN/2016/018 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission (2018): *Joint Communication to the European Parliament, the European Council and the Council Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats.* Online: www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

European Commission (2020): *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM/2020/605 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605

European External Action Service (2016): *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* June 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European Parliament (2022): *Exchange of Views with the NATO StratCom Centre of Excellence.* 1 February 2022. Online: www.europarl.europa.eu/committees/en/exchange-of-views-with-the-nato-stratcom/product-details/20220121CHE09881

Hoffman, Frank G. (2006): Complex Irregular Warfare: The Next Revolution in Military Affairs. *Orbis,* 50(3), 395–411. Online: https://doi.org/10.1016/j.orbis.2006.04.002

Hybrid CoE (2017a): *The Common Set of Proposals for the Implementation of the Joint EU–NATO Declaration.* Online: www.hybridcoe.fi/wp-content/uploads/2017/08/Common-set-of-proposals-for-the-implementation-of-the-Joint-Declaration-2.pdf

Hybrid CoE (2017b): *Memorandum of Understanding on the European Centre of Excellence for Countering Hybrid Threats.* 11 April 2017. Online: www.hybridcoe.fi/wp-content/uploads/2017/08/Hybrid-CoE-final-Mou-110417-1.pdf

Hybrid CoE (2017c): *The Establishment.* Online: www.hybridcoe.fi/establishment/

Hybrid CoE (2018): *Hybrid CoE Supports Informal NAC–PSC Discussion.* 28 September 2018. Online: www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/

Hybrid CoE (s. a.): *What Is Hybrid CoE?* Online: www.hybridcoe.fi/who-what-and-how/

Johnson, Robert (2018): Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies,* 29(1), 141–163. Online: https://doi.org/10.1080/09592318.2018.1404770

Molnár, Anna (2019): The Renaissance of EU–NATO Relations in Light of the EU's Attempt at Autonomy. In Baranyi, Tamás Péter – Stepper, Péter (eds.): *NATO in the 21st Century. A Central European Perspective.* Budapest: Antall József Tudásközpont, 239–256.

NATO (2016a): *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Online: www.nato.int/cps/en/natohq/official_texts_133163.htm

NATO (2016b): *NATO–EU Relations.* North Atlantic Treaty Organization, Fact Sheet, July 2016. Online: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/ 20160630_1607-factsheet-nato-eu-en.pdf

NATO (2017a): *Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 14 June 2017. Online: www.google.com/search?client=firefox-b-e&q=Progress+report+on+the+implementation+of+the+common+set+of+proposals+endorsed+by+NATO+and+EU+Councils+on+6+December+2016%3B+14+June+2017

NATO (2017b): *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 29 November 2017. Online: www.nato.int/nato_static_fl2014/ assets/pdf/pdf_2017_11/171129-2nd-Joint-progress-report-EU-NATO-eng.pdf

NATO (2018): *Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 31 May 2018. Online: www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf

NATO (2019): *Fourth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 17 June 2019. Online: www.nato.int/nato_static_fl2014/assets/pdf/ pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO (2020): *Fifth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 16 June 2020. Online: www.nato.int/nato_static_fl2014/assets/pdf/ 2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf

NATO (2021): *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016.* 3 June 2021. Online: www.nato.int/nato_static_fl2014/assets/pdf/ 2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

NATO (2022): *Seventh Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 20 June 2022. Online: www.consilium.europa.eu/media/57184/eu-nato-progress-report.pdf

NATO (2023): *Eighth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 20 June 2023. Online: www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/230616-progress-report-nr8-EU-NATO.pdf

NATO Watch (2017): *European Centre of Excellence for Countering Hybrid Threats opens in Helsinki.* Online: https://natowatch.org/newsbriefs/ 2017/european-centre-excellence-countering-hybrid-threats-opens-helsinki

Renz, Bettina (2016): Russia and 'Hybrid Warfare'. *Contemporary Politics,* 22(3), 283–300.

Sweeney, Simon – Winn, Neil (2022): Understanding the Ambition in the EU's Strategic Compass: A Case for Optimism at last? *Defence Studies,* 22(2), 192–210. Online: https://doi.org/10.1080/14702436.2022.2036608

Wijnja, Kim (2022): Countering Hybrid Threats: Does Strategic Culture Matter? *Defence Studies,* 22(1), 16–34. Online: https://doi.org/10.1080/14702436.2021.1945452

Dany Shoham[1]

Chemical and Biological Weapons

Given the variability in defining hybrid warfare, perhaps the most simple and decent form would rely on the definition of 'hybrid', namely, "something that is a mixture of two very different things" (Cambridge Dictionary), meaning that hybrid warfare is plainly a mixture of two (or more) very different warfares. The pertinent scope is broad. Alongside conventional warfare, unconventional warfare is one main vector within this context, and includes, i.a. chemical and biological weapons (CBW). In similarity to radiological weapons, and unlike nuclear weapons, CBW constitute weaponry of mass destruction having no physical impact. CBW may expectedly be used in parallel to any other type of warfare, particularly together with information warfare aiming to deny or, conversely, take responsibility and advantage of, or just threaten their employment; otherwise, as another example, together with cyber warfare aiming to paralyse hospitals or pharmaceutical producers, and thus hinder medical treatment and preventive measures. Many parameters account for remarkable flexibility in employing CBW, thereby shaping a wide range of tasks/tentative achievements, as well as adjustability, in relation to the contemporarily employed other type(s) of warfare, being it conventional or an additional type of unconventional warfare. Especially notable among those parameters – together with actual instances – are:

- the user – a state (Syria, during the civil war) or non-state actors – an organisation (ISIS, in Iraq and in Syria)
- the contemporaneously conducted warfare – during the civil war in Syria, CW were often used by Syria parallel to conventional warfare; at times lethal (sarin nerve agent) and at times non-lethal (chlorine, basically an incapacitant); also, nearby hospitals were attacked at the same time, so as to hamper treatment and/or obfuscate evidence
- the impact – intended to form, and thereafter last, in the short, medium, or long run; for example, the impact of a non-persistent nerve agent, as compared to an epidemic virus (having a period of incubation, and prolonged effect)

[1] Bar-Ilan University.

DOI: https://doi.org/10.36250/01236_05

- the objective – the direct impact may be the ultimate objective, or may propel the occurrence of the ultimate objective; the CW employment in Syria was meant, alternately, to afflict and/or terrorise Syrian citizens and ISIS warriors
- the target – humans, livestock or crops; also, logistic targets, such as fuel pools, can be contaminated by fuel-eating germs, as one instance
- the mode – through commando operations (assassinations with toxic substances by Russia and North Korea) or through standardised munitions (Iraq, Syria)

On the whole, CBW are highly consistent with the increasing global trend of combining conventional and unconventional warfares. A substantial spectrum of hybrid warfare modes is thereby accentuated, at large, serving for the attainment of noticeably diversified outcomes. The main problem marking the menace described here, hence, is the complicatedness of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers. This problem is intended to be handled through typologically and detailedly expounding this coupling, so as to enhance preparedness and countering capacities. At its basic level, hybrid warfare represents the coupling of conventional and unconventional warfares, while chemical and biological weapons (CBW) are included within the unconventional vector. At its utmost, namely under the category termed 'Unrestricted Hybrid Warfare' – foremost conceptualised and upgraded by China and Russia – there are three sub-categories: non-military, transitional and military. Both approaches are being followed in the present chapter, within a spectrum of CBW events and scenarios. The chemical and biological warfare agents (CBA) and weapons mentioned in this chapter are not all prohibited under the CB conventions. The purpose of mentioning the CBW discussed here is to broadly present a variety of such agents and weapons that might be effectively employed within the context of hybrid warfare, whether or not included in those conventions. Alongside classic CBW, the nearly existing horizon of hybrid warfare is apt to combine conventional warfare modes together with new generations of a variety of CBW, as detailed below. A variant of hybrid warfare can include two vectors (or more), of which one is a CBW vector, and the second one (either an additional CBW or a conventional element) serves to prevent attention to, detection and identification (by the opponent) of the first one; or brings about a synergistic effect together with the first one. An example is simultaneous employment of CW munitions together with conventional munitions that

look entirely the same. Or simultaneous employment of CW munitions containing one type of a CWA together with another type of CWA-containing munitions that look entirely the same. The element of misleading is hence prominent, alongside. In sum, this chapter is intended to meet pertinent questions and issues as follows:

- the singularities of CBW as weapons of mass destruction
- the meaningfulness of CBW as a vector within the doctrine of hybrid warfare at large
- within that context – the consequentiality of the category termed 'Unrestricted Hybrid Warfare', foremost conceptualised and upgraded by China and Russia
- the actuality of events and feasible scenarios, which expound the complicatedness and impacts of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers
- typologically and detailedly expounding this coupling, so as to enhance preparedness and countering capacities
- the utilities of CBW in hybrid warfare beyond anti-human effects, namely for attacking farm animals, crops, wild vegetation (defoliants), and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare
- the weight of a nearly existing horizon of hybrid warfare apt to combine conventional warfare modes together with new generations of a variety of by far advanced CBW

Delivery and dispersion

Operationally, the effectiveness of CBW is mainly shaped by the efficiency of its delivery, or dissemination, to a target. The most common techniques include munitions (such as bombs, projectiles, warheads) that allow dissemination at a distance and spray tanks which disseminate from low-flying aircraft. Developments in the techniques of filling and storage of munitions have also been important in shaping the effectiveness of CBW. The dissemination is highly dependent on atmospheric conditions because many CWAs act in gaseous form. Thus, weather observations and forecasting are essential to optimise weapon delivery and reduce the risk of injuring friendly forces. Practically, dispersion is placing the CBA upon or adjacent to a target immediately before dissemination, so that the material is most efficiently used, and would at its maximum reach

the opponent. The act of dispersing takes place as a result of explosion of the munition, or otherwise thanks to collateral mechanical devices that generate air, inert gas or liquid propellant. Concomitant aerosolisation of the concerned CBA would enhance its dispersal and effectuality. Basically, CBW delivery methods fall into two broad categories: line sources and point sources. Line source delivery involves dispersing an agent from a moving source that can cover a much larger area than point source delivery would. Line source delivery systems include sprayers attached to moving aircraft, vessels, or vehicles. Point source delivery involves dispersing an agent from a single location. Point source delivery systems include grenades, mines, artillery shells, aerial bombs, rockets and warheads delivered via missiles. Basically, CBW delivery methods fall into two broad categories such as line sources and point sources:

- Line source delivery – involves dispersing an agent from a moving source that can cover a much larger area than point source delivery would. Line source delivery systems include sprayers attached to moving aircraft, vessels, or vehicles.
- Point source delivery – involves dispersing an agent from a single location. Point source delivery systems include grenades, mines, artillery shells, aerial bombs, rockets and warheads delivered via missiles.

In dissimilarity to the above described delivery modes, commandos or terrorists can use CBWA via standardised or improvised small devices, at times quite simple and yet effectual, or even just contaminate directly water and food consumed collectively or by certain persons. Aerial contamination, whether in a closed space or environmentally would chiefly rely on spraying devices, while the latter can serve for assassinations as well. Such operations may be carried out clandestinely or overly, including by suiciders. Chemical weapons[2] include toxic and non-toxic agents that have the purpose to kill or severely injure. Toxic agents are nerve agents such as sarin, soman, tabun, VX, GF, novichok agents, choking or lung-damaging agents such as chlorine and phosgene, blood agents also called asphyxiants such as hydrogen cyanide, cyanogen chloride, arsenic compounds and blister agents or vesicants such as sulfur mustard, nitrogen mustard, lewisite, phosgene oxime. Non-toxic agents impair human functioning and can be grouped into incapacitating agents aiming to temporarily incapacitate such as central nervous system stimulants, like amphetamines, central nervous

[2] USAMRICD 2000.

system depressants like opioids, psychedelics like LSD-25 and deliriants like BZ. Malodorants are disgusting and smelly odorants. The idea behind is to combine several stinking substances that are largely based on sulfur, as one example, along with a sniffing factor that will spray and cause nausea and escape. The difficult military experience of the U.S. military in Somalia has led to the use of such substances. Another example is the mixture named 'Skunk', which contains an organic and non-toxic blend of baking powder, yeast and other ingredients. There are also partially incapacitating agents such as vomiting agents like adamsite, and irritant agents also called lacrimators like CS or tear gas. Exposure or contact with an agent does not necessarily lead to absorption, namely penetration of the epithelial barrier. Contact with epithelial tissues may include skin, lungs, eyes and gut, and may lead to percutaneous absorption, inhalational absorption, ocular absorption, or enteral absorption, respectively. When absorption does occur, consequential effects might be limited to the site of contact, or much wider, due to systemic distribution of the toxic molecules in the body. An area denial weapon or anti-access/area denial weapon system is a defensive device or strategy used to prevent an adversary from occupying or traversing an area of land, sea or air. Alongside, the massive use of defoliants or herbicides such as Agent Orange, which contains the toxic element dioxin known from the Vietnam War, can be regarded as an effectual interdiction measure, because they leave areas empty of any form of vegetation cover. In the desert-like terrain that ensues, it is impossible for the enemy to travel without being seen, and there is little cover in case of an attack, especially from the air. White phosphorus munitions may cause significant toxic effects in high concentration, hence can at time be used as a substitute. CWA constituting power multipliers through attacking non-living targets during hybrid warfare might include a variety of substances that:

- block vital openings
- eat away the insulating materials of electrical wires
- are corrosive towards rubber
- can betray the vehicles to the radar
- cause vehicles to slip; neutralise essential lubricants

The domain of biological weapons (BW) is more complex than the domain of CW, although there are various significant common denominators. The way BW are presented hereafter is hence rather different from CW. BW are most outstanding in general, in that technologically the needed a shift from producing defensive biologicals, in that case vaccines to offensive biological

weapons agents (BWA) is minimal, an attribute bearing multiple implications, including in the dimension of hybrid warfare. Moreover, BW are the only weapons either within the context of unconventional or conventional warfare that in principle mimic natural phenomena in the form of infectious diseases, hence are highly disguisable, potentially, when employed clandestinely. BWA include, basically, pathogens and toxins that may be classified into live, hence reproducing agents/pathogens and nonviable agents/toxins:

- toxins – include ricin, botulinum, mycotoxins
- viral diseases – include SARS, Marburg and smallpox
- bacterial diseases – include anthrax, cholera and brucellosis
- fungal diseases – include histoplasmosis
- lethal or sub-lethal agents – that do not present themselves to a clear-cut classification, since mortality rate may widely vary
- transmissible or contagious agents – also called epidemic pathogens or non-transmissible pathogens

Natural or modified/engineered pathogens and toxins abruptly in the case of toxins or gradually in the case of pathogens affect the target such as humans, husbandry, crops, or materials. The vehicle may be natural (infected insects, animals, or human beings) or artificial (warheads, aerial bombs, artillery shells, man-made disseminators, i.e. sprayers, including through guerrilla warfare). The route of penetrating the body is the respiratory system, alimentary tract, eyes or rarely skin. It seems, then, as if the most significant distinctions can be made between epidemic and non-epidemic agents on the one hand and independently, between treatable and untreatable agents, on the other. Although the former distinction relates equally to bacterial and viral pathogens, the latter reflects a fundamental difference between those two major classes. Regardless of anti-sera, antiviral preparations are of limited efficacy, although they are expectedly being upgraded. Vaccines, as prophylactic measures, are in principle efficient against viruses, bacteria and protein toxins. The impact of BW employment is appreciably varied, both spatially and temporally. Its variability is shaped by the following factors:

- initial area coverage – the primary area contaminated, via air, water supplies, food supplies, or animal vectors/carriers
- contagiousness – is vital to attain epidemicity and thereby a much wider affected area, for example plague

- demographic conditions – population density would significantly extend the chain of infection range
- climatic conditions – sunlight in the form of ultraviolet light would usually damage the BWA, but wind might enlarge affected area
- duration of pathogenetic course – from hours in the case of toxins to weeks in the case of SARS, or even longer periods
- curability – by antisera if available against toxins, bacteria, or viruses or by antibiotics against bacteria
- environmental stability of the pathogen/toxin – of utmost stability are anthrax and mycotoxins
- conduction and effectiveness – of preventing measures before and after the act of BW employment

Beyond BWA affecting humans, should be mentioned BWA attacking husbandry such as foot and mouth disease virus and BWA attacking crops such as stem rust fungus. BWA attacking non-living objects are bacteria naturally or genetically engineered able to feed and eat various key substances. The latter include plastics, rubber, asphalt, fuel and oil. Area denial BW are spores that can contaminate the ground for lengthy periods of time, thanks to their superb endurance, thus providing a form of area denial. Other biotic force multipliers are cybernetic organisms, and bio-robots are being developed as components of hybrid warfare that have meaningful impacts. Notably, such fighting vectors were recently underscored by far in a RAND report prepared for the Pentagon.[3]

Preparedness and precautionary measures

CBW preparedness is a research-based set of actions that are taken as precautionary measures in the face of CBW threats and impacts. The latter include:

- personal illness that may lead to death of soldiers and/or civilians
- incapacitated manpower
- logistic efforts needed to medically support and isolate the infected/sickened victims
- meticulous, extremely demanding managing of the apparently unaffected population

[3] Matthews et al. 2024.

- demoralisation that may ascend to total panic
- economic crisis
- overall instability[4]

CBW preparedness is a major phase of CBW emergency management and an important quality in achieving related goals and in avoiding and mitigating damaging impacts. A fundamental distinction would be needed between CBW threats that concern civilian targets or military targets. The most developed type appears to be 'disaster preparedness', defined by the UN as involving "forecasting and taking precautionary measures before an imminent threat when warnings are possible".[5] CBW preparedness is initially propelled by an intelligence assessment posing either a potential or concrete CBW threat. The methodology of creating CBW preparedness includes the exploration of theoretical, possible and feasible scenarios of threat materialisation, intelligence monitoring, potential or concrete threat assessment of adversaries' efforts, capabilities and intentions, planning of the corresponding emergency management alignment, education, practising and periodical training. Within that context, a potential threat is observed as an actual effort to procure CBW, whether through a domestic program of research, development and production, or from extraneous sources. A concrete threat is observed as an existing CBW already possessed by an adversary that might have intentions to employ them. At that point, an intelligence endeavour to explore whether and in what modes a given CBW threat is prone to materialise in whatever form of hybrid warfare is crucial. Afterwards, persistent intelligence aiming at continuously monitoring the adversary's doctrine that involves CBW within hybrid warfare scenarios is vitally needed. The intelligence components involved include:

- analysis of exports and imports of single-use and dual-use chemicals and equipment
- human intelligence such as diplomatic, refugee and spying reports (HUMINT)
- photography from satellites, aircraft and drones (IMINT)
- examination of captured equipment (TECHINT)

[4] Shoham 2007.

[5] Kent 1994: 11.

- communications intercepts (COMINT)
- detection of chemical manufacturing and chemical agents themselves (MASINT)

Thus once established, a certain CBW threat would imperatively lead to a phase of threat management. Beyond the cardinal component of intelligence, that phase may include efforts to defy the forming of threat, a counter-doctrine of retaliation in kind or otherwise, and the orderly resultant construction of an emergency management alignment. The latter would usually be divided into an upon-threat-materialisation-crisis management sub-alignment, and a post-threat-materialisation management sub-alignment. It would rely on practical capacities of detection of chemical attacks ideally preceded by intelligence warning, specific identification of CBAs, individual protection such as gas masks, clothing, antidotes, anti-sera, vaccines, anti-microbial drugs, collective protection, building/shelters protection, decontamination, evacuation, hospitalisation and medical treatment. As a principle, particular military procedures, which are usually the model for civilian procedures, depend on the equipment, expertise and personnel available. The United States' (U.S.) approach is essentially whole community preparedness (in reference to the civilian sector): "By working together, everyone can keep the nation safe from harm and resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics."[6] CBW threats either within the context of terrorism or military unconventional attacks are equivalents. The U.S. Federal Emergency Management Agency, individuals, families, businesses, faith-based and community groups, profitable groups, schools and academia, media outlets, and all levels of governments are to take an active role in preparedness efforts. A disaster will affect the whole community, so everyone must be ready, by making a plan, being informed, and taking action to mitigate the effects of future crises. A most grand program aiming to scale up preparedness to bioterrorism was based on the U.S. Project Bioshield Act, which was passed by the Congress in 2004. The Act called for $5 billion to purchase vaccines that would be used in the event of a bioterrorist attack. In its full amplitude, the program was designed to acquire medical countermeasures to biological, chemical, radiological and nuclear agents for civilian use. Actually, since the 2001 terrorist attacks against the Twin Towers and the anthrax letters,

[6] *GeoCONOPS Alignment to Federal Doctrine: PPD-8* s. a.; U.S. Department of Homeland Security 2015.

the U.S. has allocated nearly $50 billion to address the threat of biological weapons. The U.S. funding for bioweapons-related activities focuses primarily on research for and acquisition of medicines for defence. Funding also goes toward stockpiling protective equipment, increased surveillance and detection of biological warfare agents, and improving state and hospital preparedness.[7] The corona pandemic and the possibility that the virus was developed as a BWA and accidentally leaked in Wuhan added an amplified dimension. Thus, the U.K. established in 2023 the *UK Biological Security Strategy.*[8] Further, underpinned by the UK Biological Security Strategy and the U.S. Biodefense Strategy, the U.S.–UK Strategic Dialogue on Biosecurity took place in January 2024 and reflected a shared ambition to protect against a growing and diverse spectrum of biological threats. These threats include future pandemics, antimicrobial resistance, a deliberate bioweapon attack, as well as those that might arise from the misuse of biotechnology.[9] Moreover, the World Economic Forum recently launched the Biothreat and Disease Surveillance Initiative to catalyse the establishment of public–private collaborations that improve the capacity to prepare and respond to biological threats.[10]

Hybrid warfare with CBW

During the eight-year Iran–Iraq War (1980–1988), more than 350 large-scale Iraqi chemical attacks were reportedly conducted since 1982 in the border areas, and took place until the last day of war. Most of the chemical attacks were combined with conventional Iraqi attacks, and played a highly important role in Iraq's military success. Essentially, the Iranian forces were most of the time unprotected, and Iran did not possess any CBW at that time, to retaliate with. Hybrid warfare is low risk, low cost and provides an adversary the opportunity to obfuscate, throwing doubt on who is responsible for gray zone actions. Thus, the Syrian regime's use of CW during the Syrian Civil War (since 2012) has been a lasting illustrative example in that an indicator that the regime might be about to use CW would be planting information that the opposition has CW. Then,

7 Gottlieb 2013.
8 Cabinet Office 2023.
9 East–Regan 2024.
10 Shapiro – Du Moulin 2024.

when there is chlorine in some Syrian village, who is to say it came from a barrel bomb? This type of tactic might be a particular problem with consensus-driven organisations, such as NATO.[11] Moreover, after the Syrian-declared CW arsenal was destroyed, the Syrian regime persistently claimed it does not possess CW while concurrently hiding and often employing significant portions of the real arsenal as a disinformation line aiming to refute Syrian CW employment. An additional line of Syrian disinformation warfare has been the concurrent elimination of evidence indicating that CW were used.[12] The concrete mechanism of Assad's decision-making in relation to the transition from conventional to CW is not clear. It can be assumed that he is the authority approving that transition, at least in those cases where sarin was employed, which is not necessarily the case with chlorine. The Syrian regime's desire to use CW has stemmed largely from its inability to achieve or major difficulty in achieving, various tactical, operational and strategic goals either military or demographic by means of conventional weapons. This was a chief drive behind Syria's retention of sarin.[13] Thus, the Syrian regime was highly predisposed to employ CW in numerous occasions during the war, but considerable international pressure as opposed to concurrent backing, if indirect yet solid lent by the Russians and the Iranians posed unignorable restrictions. Obviously, the Syrian CW arsenal has not been dismantled. Thus, the Syrians once and again had two decisions to make: whether to employ CW and what type of CWA to choose given that the Islamic State of Iraq and Syria, better known as ISIS or any other group never possessed nerve agents, hence cannot be accused of using such CWA. Therefore, the Syrian Army mostly used chlorine gas and only in a few cases sarin, still endeavouring though to trickily obfuscate, contemporarily. Within that context, the first employment of sarin by the Syrian Army in Khan al-Asal in March 2013, was a typically complicated event of hybrid warfare.[14] Several further employments of sarin by the Syrian Army were conducted until 2018. The last one in Douma in April 2018, was followed by American–British–French retaliatory raids against Syrian CW facilities. Interestingly, in a statement condemning the 2018 Western raid, Russian Foreign Minister Lavrov said: "We told the USA where our red lines were, including the geographical red lines, and the results have shown that they

[11] Garamone 2019.
[12] Shoham 2015a.
[13] Shoham 2017.
[14] *Khan al-Assal Chemical Attack* s. a.; René–Domingo 2014.

haven't crossed those lines."[15] Beyond, however, disinformation warfare did follow the U.S. strike. On 11 April 2018 Putin suggested the chemical attack was a false flag operation intended to discredit the Syrian Government. On 13 April 2018 President Assad said the attack was "100 per cent fabrication" by the United States "working hand-in-glove with the terrorists", intended to provide a pretext for the airstrike on the Shayrat Airbase.[16] In an unprecedented television interview, on *Russia Today* in May 2018, Syrian President Assad posed detailed argumentation (ostensibly) for his army's alleged non-use of CW. Referring to the (confirmed) employment of sarin in Duma and the subsequent American–British–French retaliatory raid, Assad claimed that CW had not been used by anyone, (rather than by the rebels or other groups) as has usually been contended by Syria.[17] The Russo–Ukraine War, which started in February 2022 is a conventional warfare conjoined with concomitant CBW-related elements. Since the beginning, a remarkably eventful information and intelligence dialogue evolved between Russia and the U.S., marking a hybrid warfare that involved Russian moves in Ukraine connected with significant concomitant CB elements, though not concrete employment of. On 24 February, the day the Russian invasion started Lieutenant General Igor Kirillov, Chief of the Nuclear, Biological and Chemical Protection troops of the Russian Army said that documents uncovered by the Russian military in Ukraine "show that the Ministry of Health of Ukraine has set the task of completely destroying bio-agents in laboratories. The Pentagon knows that if these documents fall into the hands of Russian experts, then it's highly likely that Ukraine and the United States will be found to have violated the BW Convention." China subsequently backed the Russian claims.[18] The U.S. said in response that its pertinent program does the opposite and in fact aims to "reduce the threat of biological weapons proliferation". Contemporaneously, the WHO "has strongly recommended to the Ministry of Health of Ukraine and other responsible authorities to destroy the dangerous pathogens in order to prevent any possible leakage".[19] Some days earlier, within a CW context, a Russian Ministry of Defence briefing on 11 May asserted that Ukrainian forces had "carried out an explosion of a tanker with fertilizer, presumably ammonium nitrate, which

[15] Shoham 2018a.
[16] Shoham 2020.
[17] Shoham 2018a.
[18] Rising 2022.
[19] Lanese 2022.

resulted in a cloud of orange smoke that dissipated after some time". According to Moscow, the aim of the explosion, which occurred in the Kharkov region, was to accuse Russia of using CW in order to "extract additional military aid from the West by the Kyiv regime".[20] Besides, on several occasions during the war, the Russian Army was accused of using white phosphorus munitions such as toxic smoke not defined as CW and it is likely that at least in one case it was indeed used. Nevertheless, multiple cases in which riot control and irritant chemical agents – possibly including novel versions – were employed by the Russian military, have apparently been evidenced.[21] All in all, the context at large, and the chronology detailed, are emblematic of a modern conflict that is hybrid in nature, and potentially harboured imminent CBW-related threats.

Chemical and biological terrorism

Since its emergence ISIS has sought CW and has used them, mostly chlorine and rarely mustard, against its opponents, namely Syrian government forces, the Syrian opposition groups, Kurds and Iraqis. Usually, CW employment was synchronised with conventional warfare in a bordering territory.[22] The Sarin attack in the Tokyo Metro was an act of chemical terrorism perpetrated in March 1995 by members of the domestic Japanese cult movement Aum Shinrikyo, a basically religious group. In five coordinated attacks, the perpetrators released nerve agent sarin on three lines of the Tokyo Metro during the rush hour, killing 14 people, severely injuring 50 some of whom later died, and causing temporary vision problems for nearly 1,000 others. The attack was directed against trains passing close to the location of the Japanese parliament headquarter. The nerve agent was produced by the cult in Japan. It was released inside the train by puncturing plastic bags containing it and carried by the perpetrators. The perpetrators were caught later on. The attack was regarded by the attackers as an "act of salvation".[23] St. Luke's International Hospital in Tsukiji was one of very few hospitals in Tokyo at that time to have the entire building wired and piped for conversion into a 'field hospital' in the event of a major disaster. This

[20] Coleman–Devlin 2022.
[21] Kyiv Post 2023.
[22] Shoham 2015b.
[23] *Tokyo Subway Sarin Attack* s. a.

proved to be a very fortunate coincidence as the hospital was able to take in most of the 600+ victims, resulting in no fatalities. As there was a severe shortage of antidotes in Tokyo, sarin antidote stored in rural hospitals as an antidote for herbicide/insecticide poisoning was delivered to nearby stations, where it was collected by a Ministry of Health official on a train bound for Tokyo.[24] Russian ex-intelligence Colonel Sergei Skripal and his daughter Yulia were found in March 2018 unconscious on a public bench in London, due to Novichok nerve agent intoxication, conducted by Russian secret agents. Skipal has been recruited to British intelligence, and passed on state secrets and blew the cover of numerous Russian agents.[25] Well characterised, "the event in Salisbury wasn't an isolated incident. It was part of a wider coordinated strategy to exert power and influence in a new era of warfare. Often termed 'hybrid warfare', the strategy sits outside of the typical rules-based system of traditional foreign policy. It is a doctrine that is highly flexible and adaptive; it uses a variety of covert tools at its disposal to achieve strategic political objectives."[26] In this specific case thus, the poisoning task was but one quite drastic element within a broad range of Russian intelligence plus counterintelligence warfare. The Russian foreign ministry's denials were implausible. This was an example of Vladimir Putin's hybrid warfare, or probably what's better described as 'hybrid politics'. He's willing to use Russian power in transparent ways and trust that responses will be ineffective or require long processes that he can frustrate. The initial Russian response to the U.K.'s request for an explanation has been to deny any knowledge or involvement, and to request more details. Russian spokespeople have also started to provide 'alternative facts' about the attack, even speculating that it could have been conducted by U.K. authorities to discredit Russia.[27] Typically Russian disinformation warfare that followed an event combining intelligence warfare and chemical terrorism warfare. And yet, this assassination attempt was just one of multiple cases combining individual chemical terrorism warfare, intelligence warfare and disinformation warfare, as follows. Viktor Yushchenko, President of Ukraine from 2005 to 2010 was poisoned in Ukraine, likely by Russian agents during his election campaign in September 2004. He was flown to Vienna for treatment and diagnosed with several syndromes, due to a serious viral infection

[24] Smithson–Levy 2000.
[25] Shoham 2018b.
[26] Balson 2021.
[27] Shoebridge 2018.

and a toxic chemical substance called dioxin, which is not normally found in food products. After the illness, his face was greatly disfigured. A former Russian Federal Security Service officer who specialised in tackling organised crime, Litvinenko publicly accused their superiors, in November 1998, of ordering an assassination of a Russian tycoon. Litvinenko was arrested and afterwards fled in 2000 to London, where he was granted asylum. There, he worked as a journalist, writer and consultant for British intelligence. During his time in London, he wrote two books, wherein he accused the Russian secret services of staging several acts of terrorism in an effort to bring Vladimir Putin to power. In November 2006, Litvinenko suddenly fell ill and was hospitalised in what was determined to be a case of a lethal poisoning by radioactive Polonium-210. The intoxication was conducted by Russian secret agents. Notably, the methods of infiltrating the poisons from Russia into the U.K. and Ukraine constitute their own separate issue, which is of paramount importance. The political assassination with nerve agent VX in February 2017 of North Korean ruler Kim Jong-un's estranged half-brother Kim Jong-nam in Malaysia, by North Korean agents warrants attention. Kim Jong-un most probably backed the murder.[28] Examples of biological terrorism are also remarkable. One week after the Twin Towers plus Pentagon events, five regular letter envelopes containing anthrax (Ames strain) spore powder were mailed from New Jersey (NJ) on 18 September 2001 to news media reporters in the U.S. and two additional anthrax letters were mailed from NJ on 9 October 2001 to two Senators. Most of the envelopes were opened without control. Twenty two people were infected and five died. According to the FBI, the ensuing investigation became "one of the largest and most complex in the history of law enforcement".[29] Overall, dozens of buildings were contaminated with anthrax due to the upgraded floatability of the structured powder as a result of the first five mailings, which contained, altogether about 18 gr. of the sabotage spore powder. The decontamination of the Brentwood postal facility took 26 months and cost US$130 million. The Hamilton, NJ postal facility remained closed for 41 months (its cleanup cost US$65 million). The Environmental Protection Agency spent US$41.7 million to clean up government buildings in Washington, D.C. One FBI document said the total damage exceeded US$1 billion. The 22 cases that comprised the American Anthrax Outbreak of 2001 likely had contact with one or more of seven spore-laden envelopes.

[28] Shoham 2018c.
[29] Shoham 2007.

But the anthrax letters affair was not limited to the U.S. The American embassy in Vilnius, Lithuania was likewise concurrently targeted. For the time being, the culmination of bioterrorism worldwide has been this act of distributing mail envelopes containing anthrax spore powder. It reflected noticeable supremacy of a simple act of bioterrorism irrespective of preparing the anthrax powder in itself, which was very sophisticated in several senses:

- uncontrollable preparing of the postal envelopes containing the anthrax powder
- uncontrollable, repeated mailings
- undetectable conveying of the mailed envelopes until reaching their various destinations

An intermittent Pentagon report said "the anthrax attacks revealed weaknesses in almost every aspect of U.S. bioterrorism-preparedness. As simple as these attacks were, their impact was far-reaching."[30] It provided a detailed and informative but hardly unsuspected inventory of shortcomings in emergency preparedness and response. Following a zigzag investigation the FBI concluded that Bruce Irvine, an anthrax scientist from the U.S. Army Medical Research Institute of Infectious Diseases was the culprit. However, this assertion has been widely doubted while a feasible alternative pointed to Iraq being the provenance of remarkably advanced sabotage spore powder and al-Qaeda being the implementer. A highly potent biotoxin, ricin can easily be derived from castor beans, which was indeed the case in actuality with reference to various terrorist groups, including al-Qaeda. On two occasions in the U.S., envelopes containing ricin were mailed to the White House in November 2003, and to the U.S. Senate Office of the Majority Leader in February 2004. Much earlier in 1978 Georgi Markov, a Bulgarian regime opponent, was assassinated in London with ricin through collaboration between Soviet and Bulgarian secret services. In the Moscow Theater in October 2002 an incapacitating agent was used and markedly decreased alertness and clarity, caused drowsiness, deep loss of consciousness, and even fatal coma in a closed space. It happened after Chechen terrorists took over the Moscow Theater. Between 40 to 50 armed Chechen terrorists seized about 800 hostages and ended with the death of at least 150 people, mostly due to intoxication.[31] The Russian security services pumped an aerosol anaesthetic, later stated by

[30] Shoham 2007.
[31] CNN 2002.

Russian Health Minister Yuri Shevchenko to be based on fentanyl, into the theater through the air conditioning system. The discovery caused panic in the auditorium. Fentanyl is a powerful opioid used as a pain medication. Actually, an undisclosed incapacitating agent was used by the Russian authorities in order to subdue the Chechen terrorists who had taken control of the crowded theater. A later meticulous investigation revealed that the agent used was a mixture that contained two fentanyl derivatives much stronger than fentanyl itself, sprayed in an aerosol mist, namely the opioids carfentanil, which is a large animal tranquilizer and remifentanil, a surgical painkiller).[32] The pertinent chemical warfare agent has been designated by the Russians Kolokol-1. The event was potentially catastrophic, in that it seems likely that the 800 hostages were about to be killed by Chechen rebels. To rescue them, the Russian military used a calmative agent in an attempt to subdue the rebels. Overall, the case is highly demonstrative of a commercially distributed substance which may be, or is readily adopted as a typical CW. Hybrid threats of indirectly induced CB impacts can include destruction/sabotage by conventional warfare of domestic CB facilities including completely civilian ones in order to cause leakage and environmental CB contamination. Cyber operations aimed to generate uncontrolled above-standard CB contamination happened in May 2020, when an Iranian cyberattack on Israel's drinking water systems aimed to destabilise the chlorine level and poison the country's citizens. Iran was behind the attack, with hackers using American servers to carry out the breach, which somewhat affected several water facilities throughout Israel. Intensive disinformation warfare by Iran followed the event.[33] Particularities of the SARSCoV2 pandemic within the context of hybrid warfare are linked to the complexity of the debate over the origin of the pandemic virus, whether it was a natural scenario or a lab accident. Accidental leak of a lab-designed virus could take place during a scientific public health program and/or a military program. The debate is challenging, and is at any rate conjoined with hybrid warfare. Connectedly, one intriguing possibility which is here inquired into, among others, is the approach posed by a former U.S. State Department principal investigator who officially dealt with this matter, Dr. David Asher, in reference to China's strategy at large: "The Chinese have made it clear they see biotechnology as a big part of the future of hybrid warfare.[34] […] We didn't

[32] Riches et al. 2012.
[33] I24 News 2020.
[34] Birrell 2021.

come at this saying: Let's go blame the Chinese. But we […] had to appreciate the nature of the Chinese government. This is a government that since 2007 has been writing publicly about genetic warfare. […] The Chinese government, at the leadership of the People's Liberation Army (PLA), and even at Xi Jinping's level himself, have at least suggested that bio war is the future of war in some ways, even going beyond nuclear war. I don't know quite what that means, but when I start to read that in publications which are not classified but not well read because they're in Chinese and they're aimed at a Chinese audience, you start to say, "What are they talking about?" […] On Chinese national TV [in 2017], there was an interesting media commentary by their lead PLA commentator about that, [saying] "we have entered into an area of Chinese bio warfare, including using things like viruses." I mean, they made a public statement to their people that this is a new priority. […] You need to understand the context of Chinese hybrid warfare. You need to understand the nature of the communist state in China, and its secretive dual use approach to everything military, to be able to appreciate it."[35] Practically, China has been accused of:

- gain of function experimentation much beyond the norms
- responsibility for an accidental pandemic virus leakage
- reporting about the epidemic outbreak much after real time
- reporting that the virus is non-transmissible among humans
- allowing flights from China outwards as usual
- hiding data concerning the genomic origin of the virus and direct source of the initial human infection

In connection to the above, and referring to the Annual Threat Assessment of the U.S. Intelligence Community of 7 February 2022, it is worth noting within the BW dimension the following:[36]

- "Global shortcomings in preparedness for the pandemic and questions surrounding the origins of the Covid-19 virus and biosecurity may inspire some adversaries to consider options related to biological weapons developments.
- As China, Iran, and Russia continue to publicly tout individual or collaborative efforts to improve biosecurity, they have pushed narratives that further drive threat perceptions, including linking U.S. laboratories

[35] Asher–Yu 2021.

[36] Office of the Director of National Intelligence 2022.

abroad to Covid-19 origins, breaches in biosafety, untrustworthy vaccines, and biological weapons. This messaging probably will be amplified in the lead up to the once-every-five-years Review Conference of the Biological and Toxin Weapons Convention, tentatively slated to convene in mid 2022.
– Rapid advances in dual-use technology, including bioinformatics, synthetic biology, and genomic editing, could enable development of novel biological weapons that complicate detection, attribution, and treatment."

Connectedly, if in a collateral manner, it is of note that since the Covid-19 period, health sectors have become a favourite target for all types of cyberattacks in the entire world.[37] Further, the dimension of unrestricted hybrid warfare within the context of militarily manipulated biotechnology – combined with formation of solid footholds in the territory of the adversary (or ostensible partner), as well as with massive scientific espionage – has been materialised by China in effect, in the U.S.,[38] Canada[39] and Europe.[40] Far beyond, the issue of ethnic/biogenetic weapons is intriguing; the excludability of its feasibility appears to be uncertain. It so happened that in 2007, when China institutionalised its doctrine in that uncanny arena (as mentioned above) it was reported that the Russian Government banned all exports of human biosamples, while the reason for the ban was allegedly an account by the head of the FSB Nikolay Patrushev presented to Vladimir Putin. The account claimed about on-going development of "genetic bioweapons" targeting the Russian population by American and Polish institutions, including the Institute of Genetics and Biotechnology, Warsaw University and the Department of Medical Biotechnology, Jagiellonian University;[41] seemingly an earlier version of the bio-information warfare that reappeared 15 years later around Ukraine, as described. On the whole, China, Russia, Iran and North Korea certainly possess stockpiles of BW, and pose potentially serious biothreats. Particularly, China's conduct is implicative of unexplained peculiarities prior to, especially towards, and after the start of the pandemic, joined together with a variety of disinformation and misinformation warfare.[42]

[37] Remarks by the Head of the National Cyber System Gabi Portnoy at the Ministry of Justice; notification by the National Cyber Array, Israel, 26 October 2022.
[38] Sellin 2022a; Sellin 2022b.
[39] Shoham 2019.
[40] Sellin 2022c.
[41] Kommersant 2007.
[42] U.S. Senate 2022; Office of Senator Marco Rubio 2023.

Conclusion

The sphere of CBW, although representing mighty weapons of mass destruction on their own, constitutes a highly meaningful vector within the doctrine of hybrid warfare. A diversified spectrum of CBW is liable to meet that was presented in this chapter, together with a variety of actual events and feasible scenarios. This expounds the complicatedness and effectiveness of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers. Such modes, both tactically and strategically, have already been repeatedly implemented in reality as detailed, and are prone to expand. CBW may typically constitute a game changer in hybrid warfare either as a meaningful force multiplier of another main effort warfare, or as a main effort in itself amplified by another concurrent warfare serving as a force multiplier. A significant characteristic is the considerable modularity marking the pertinent interfaces, in that the lowest level of purposive coupling of CBW is with another warfare mode serving to facilitate or amplify the CBW effect, such as concurrently destroying warehouses storing protective CBW equipment. A higher level of purposive combining is with simultaneous invasion of CBW-protected infantry forces destined to defeat the CBW-afflicted enemy, occupying the territory held by the enemy. And so forth can be added at the same time or slightly later further layers of other warfares aiming either to increase the effectiveness of the three above mentioned elements, or to serve for a far higher broader purpose, which is still being assisted by those three elements as well. In a way, it is possibly an orchestration scaled up, contemporaneously, from tactic levels to strategic levels. Alongside, intelligence warfare is fundamentally a unique type of permanently ongoing warfare, including the CBW domain in terms of both intelligence and counterintelligence. Thus, CBW intelligence warfare is being conducted continuously on a basic level, as well as towards CBW employment, hybridly, during CBW employment, and increased when CBW defensive preparedness is heightened. Disinformation warfare and deception are often conducted verbally and/or practically together with CBW employment, aiming to obfuscate evidence, suspicions, or assessments related to the employer identity. Such a hybrid warfare might be sophisticated, challenging and at times entirely effective. Moreover, natural occurrences of toxins and of pathogens may serve as camouflage for BWA employment, thereby enabling efficient hybrid warfare. Remarkably, as shown, CBW are not designed against humans merely. A variety of CBWA are intended for attacking farm animals, crops, wild vegetation or defoliants,

and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare. On the whole, the CBW dimension of hybrid warfare is highly consequential. It has already proved as such along a wide diversity of events that took place in effect as detailed, while further, various scenarios embody considerable feasibility to happen in actuality. Basically, they might be implemented hybridly and flexibly as impactful components, through a wide range of options.

Questions

1. What are the singularities of CBW as weapons of mass destruction?
2. How can you explain the meaningfulness of CBW as a vector within the doctrine of hybrid warfare at large?
3. What is the consequentiality of the category termed 'Unrestricted Hybrid Warfare', foremost conceptualised and upgraded by China and Russia?
4. What is the actuality of events and feasible scenarios, which expound the complicatedness and impacts of coupling CBW with other forms of warfare that would conjointly comprise, mutually, powerful force multipliers?
5. How can one typologically and detailedly expound this coupling, so as to enhance preparedness and countering capacities?
6. What are the utilities of CBW in hybrid warfare beyond anti-human effects, namely for attacking farm animals, crops, wild vegetation (defoliants), and non-living objects of logistic importance, altogether comprising additional modes of hybrid warfare?
7. What is the weight of a nearly existing horizon of hybrid warfare apt to combine conventional warfare modes together with new generations of a variety of by far advanced CBW?

References

Asher, David – Yu, Miles (2021): Transcript: The Origins of Covid-19: Policy Implications and Lessons for the Future. *Hudson Institute,* 17 March 2021. Online: www.hudson.org/foreign-policy/transcript-the-origins-of-covid-19-policy-implications-and-lessons-for-the-future

Balson, David (2021): Tackling Hybrid Warfare: The Salisbury Poisoning Three Years On. *Ripjar,* 8 March 2021. Online: https://ripjar.com/blog/tackling-hybrid-warfare-the-salisbury-poisoning-three-years-on/

Birrell, Ian (2021): Worrying New Clues about the Origins of Covid: How Scientists at Wuhan Lab Helped Chinese Army in Secret Project to Find Animal Viruses. *The Mail on Sunday,* 24 April 2021. Online: www.dailymail.co.uk/news/article-9507749/How-scientists-Wuhan-lab-helped-Chinese-army-secret-project-animal-viruses.html

Cabinet Office (2023): *UK Biological Security Strategy.* Policy Paper by the U.K. Government, 12 June 2023. Online: www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html

CNN (2002): Chechen Gunmen Seize Moscow Theater. *CNN,* 24 October 2002. Online: https://edition.cnn.com/2002/WORLD/europe/10/23/russia.siege/index.html

Coleman, Alistair – Devlin, Kayleen (2022): Ukraine Conflict: Russian Chemical Attack Claim Fact-checked. *BBC News,* 15 May 2022. Online: www.bbc.com/news/61439398

East, Christopher – Regan, Dan (2024): Event Summary: the U.S.–UK Strategic Dialogue on Biosecurity. *Council on Strategic Risks,* 22 January 2024. Online: https://councilonstrategicrisks.org/2024/01/22/event-summary-u-s-uk-strategic-dialogue-on-biosecurity/

France 24 (2022): Ukraine Accuses Russia of Using Phosphorus Bombs in Fresh Strikes on Snake Island. *France 24,* 1 July 2022. Online: www.france24.com/en/europe/20220701-live-russian-missile-strike-on-apartment-building-in-odesa-kills-10

Garamone, Jim (2019): Military Must Be Ready to Confront Hybrid Threats, Intel Official Says. *U.S. Department of Defense,* 4 September 2019. Online: www.defense.gov/News/News-Stories/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intel-official-says/

GeoCONOPS Alignment to Federal Doctrine: PPD-8 (s. a.). Online: https://emilms.fema.gov/is_0060b/groups/17.html

Gottlieb, Scott (2013): Ricin, Domestic Bioterrorism, and the Lessons Learned After 9/11: Are We Safer Today Than We Were 10 Years Ago? *Forbes,* 17 April 2013. Online: www.aei.org/articles/ricin-domestic-bioterrorism-and-the-lessons-learned-after-911-are-we-safer-today-than-we-were-10-years-ago/

I24 News (2020): Report: Iran Behind Recent Cyberattack on Israel's Water Supply. *I24 News,* 7 May 2020. Online: www.i24news.tv/en/news/israel/1588852463-report-iran-behind-recent-cyberattack-on-israel-s-water-supply

Kent, Randolph (1994): *Disaster Preparedness.* Geneva: United Nations Disaster Management Training Program.

Khan al-Assal Chemical Attack (s. a.). Online: https://https://en.wikipedia.org/wiki/Khan_al-Assal_chemical_attack

Kommersant (2007): Russia Observes the Human Model. *Kommersant,* 29 May 2007.

Kyiv Post (2023): Ukraine Reports 465 Chemical Attacks by Russia Since Start of Full-Scale Invasion. *Kyiv Post,* 27 December 2023. Online: www.kyivpost.com/post/26011#:~:text=In%20December%20alone%2C%20Russian%20troops,grenades%20with%20unknown%20new%20agents

Lanese, Nicoletta (2022): Ukraine Should Destroy 'High-Threat' Pathogens, WHO Says. *Live Science,* 11 March 2022. Online: www.livescience.com/ukraine-labs-destroy-pathogens-who-advises

Matthews, Luke J. – Lee, Mary – De Bruhl, Brandon – Elinoff, Daniel – Eusebi, Christopher A. (2024): *Plagues, Cyborgs, and Supersoldiers. The Human Domain of War.* Santa Monica: RAND. Online: www.documentcloud.org/documents/24376031-rand_rra2520-1-1

Office of Senator Marco Rubio (2023): *A Complex and Grave Situation. A Political Chronology of the SARS-CoV-2 Outbreak.* 1 May 2023. Online: www.rubio.senate.gov/wp-content/uploads/_cache/files/4f6bb786-504e-443d-8904-974dafc1cd0e/CD3BC3317D197A25E9FF01EBFB869357.rubio-covid-origins-report-final.pdf

Office of the Director of National Intelligence (2022): *Annual Threat Assessment of the U.S. Intelligence Community.* Online: www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

René, Pita – Domingo, Juan (2014): The Use of Chemical Weapons in the Syrian Conflict. *Toxics,* 2(3), 391–402. Online: https://doi.org/10.3390/toxics2030391

Riches, James R. – Read, Robert W. – Black, Robin M. – Cooper, Nicholas J. – Timperley, Christopher M. (2012): Analysis of Clothing and Urine from Moscow Theatre Siege Casualties Reveals Carfentanil and Remifentanil Use. *Journal of Analytical Toxicology,* 36(9), 647–656. Online: https://doi.org/10.1093/jat/bks078

Rising, David (2022): China Amplifies Unsupported Russian Claim of Ukraine Biolabs. *AP News,* 11 March 2022. Online: https://apnews.com/article/russia-ukraine-covid-health-biological-weapons-china-39eeee023efdf7ea59c4a20b7e018169

Sellin, Lawrence (2022a): *The Great Link between the Netherlands and China.* Online: www.youtube.com/watch?v=D6SKBPFAJ0s

Sellin, Lawrence (2022b): *The Laboratory Origin of Covid-19 and the Ongoing Cover-up of its Origin, the Structure of China's Biowarfare Program and China's Massive Infiltration of U.S. Virus Laboratories.* Online: https://lawrencesellin.substack.com/p/the-laboratory-origin-of-covid-19

Sellin, Lawrence (2022c): *Chinese Biotech Firm with Deep Links to China's Military and Its Covid-19 Program just Bought Land in Florida for a Massive Research Complex.* Online: www.thegatewaypundit.com/2022/09/chinese-biotech-firm-deep-links-chinas-military-covid-19-program-just-bought-land-florida-massive-research-complex/

Shapiro, Molly – Du Moulin, Lora (2024): Lessons from Rwanda: Building Systems to Protect against Infectious Diseases and Biothreats. *World Economic Forum,* 22 January 2024. Online: www.weforum.org/agenda/2024/01/systems-infectious-diseases-biothreats-rwanda/

Shoebridge, Michael (2018): Russia, Novichok and the future of the Chemical Weapons Convention. *The Strategist, Australian Strategic Policy Institute,* 15 March 2018. Online: www.aspistrategist.org.au/russia-novichok-future-chemical-weapons-convention/

Shoham, Dany (2007): Bioterrorism. In Cox Gad, Shayne (ed.): *Handbook of Pharmaceutical Biotechnology.* Hoboken: John Wiley and Sons, 1525–1651.

Shoham, Dany (2015a): Syria's Chemical Weapon Obfuscations. *BESA Center Perspectives Paper,* (305), 7 August 2015. Online: https://besacenter.org/syrias-chemical-weapon-obfuscations/

Shoham, Dany (2015b): Does ISIS Pose a WMD Threat? *BESA Center Perspectives Paper,* (322), 13 December 2015. Online: https://besacenter.org/9562/

Shoham, Dany (2017): The Syrian Sarin Attacks of August 2013 and April 2017. *BESA Center Perspectives Paper,* (452), 26 April 2017. Online: www.jstor.org/stable/resrep04591

Shoham, Dany (2018a): Assad Addresses the Chemical Weapons Issue. *BESA Center Perspectives Paper,* (879), 1 July 2018. Online: https://besacenter.org/assad -chemical-weapons/

Shoham, Dany (2018b): Russia's Toxic Legacy. *BESA Center Perspectives Paper,* (792), 10 April 2018. Online: www.jstor.org/stable/resrep16934?seq=5

Shoham, Dany (2018c): The Peculiar Chronology of Persistent Nerve Agents. *BESA Center Perspectives Paper,* (912), 3 August 2018. Online: https://besacenter.org/persistent-nerve-agents/

Shoham, Dany (2019): China's Biological Warfare Programme and the Curious Case of Dr. Xiangguo Qiu. *CBW Magazine,* 12(4), Online: https://idsa.in/cbwmagazine/chinas-biological-warfare-programme

Shoham, Dany (2020): Syria's Chemical Arsenal: Obama's Failure, Trump's Mixed Success. *Middle East Quarterly,* 27(2), 1–8.

Smithson, Amy E. – Levy, Leslie-Anne (2000): *Ataxia: The Chemical and Biological Terrorism Threat and the US Response.* Online: https://cryptome.org/ataxia.htm

Tokyo Subway Sarin Attack (s. a.). Online: https://en.wikipedia.org/wiki/Tokyo_subway_sarin_attack#Attack

USAMRICD (2000): *Medical Management of Chemical Casualties Handbook*. U.S. Army Medical Research Institute of Chemical Defense.

U.S. Department of Homeland Security (2015): *National Preparedness Goal*. Online: www.fema.gov/sites/default/files/2020-06/national_preparedness_goal_2nd_edition.pdf

U.S. Senate (2022): *An Analysis of the Origins of the Covid-19 Pandemic*. Senate Committee on Health Education, Labor and Pensions, Minority Oversight Staff, October 2022. Online: www.help.senate.gov/imo/media/doc/report_an_analysis_of_the_origins_of_covid-19_102722.pdf

Andrew Dolan[1]

Hybrid Warfare and Nuclear Weapons

It would be unusual to examine the nature of hybrid warfare and omit consideration of the potential role, if any, that nuclear weapons might play in this form of conflict. Nuclear weapons, both traditional and the imagined, is a constant feature of the global security order and as such could have a role to play in any current or future conflict, should a protagonist possess them. The important point, however, is to try and avoid far reaching speculation and keep to the realms of what is known about nuclear weapons, the context surrounding their use and if they would make sense, if deployed in a hybrid context. This chapter will therefore seek to explore what nuclear weapons might bring to a hybrid conflict, examining what role they could play, if either used or threatened to be used, and to consider what additional factors, if any might shed light on how effective their deployment might be. It recognises that much of this type of thinking is fraught with uncertainty and hesitancy due to a lack of empirical evidence and a lack of clear definition. However, as this chapter will reveal, there are issues worth examining and questioning even if the outcome of our investigation remains barren and abstract.

Traditional nuclear security environment

It is often forgotten that nuclear weapons have featured prominently in classical military thinking since the final days of World War II. The development of atomic and then thermonuclear weapons has spawned a virtual industry in a certain strand of strategic studies that has not lost any of its intensity with the passage of time. Traditional calculations concerning the use of nuclear weaponry such as deterrence, first strike, counter force and survivability are as live today as they were under the gaze and calculations of nuclear theorists such as Bernard Brodie, Herman Kahn or Henry Kissinger. There will always, it seems, be room for the Rand Corporations, the RUSIs and SIPRIs and the Military Balances of

[1] Centre for the Study of New Security Challenges.

DOI: https://doi.org/10.36250/01236_06

the world.[2] Most commentators today would still agree that by and large, nuclear weapons remain a symbol of massive military firepower. The United States and Russia remain 'primus inter pares' so to speak but even middle ranking nuclear powers, such as the U.K., France and to a lesser extent, China, possess nuclear capabilities quite capable of wreaking havoc on any enemy should they choose to do so.[3] Familiar also is the traditional 'triad' of capabilities, based on land, sea and air delivery systems. Over the years, technological improvements in areas such as sea-launched ballistic capabilities or enhanced guidance systems or payload or propulsion features have ensured that nuclear capabilities do not remain static. Numbers might be reduced through arms control and negotiation but the issue of firepower, flexibility and prestige continues to retain a currency even after seventy or so years of development and deployment.[4] Of course it would be pointless to maintain and develop such forces at no little cost to a nation's wealth if no thought was given to the use of such capabilities. Therefore, it should not be a surprise that the integration of nuclear forces into general calculations of modern conflict remains a major feature of those government and militaries that possess them. Indeed, it is unsurprising that the strategic thinking about the potential utility of nuclear weapons remains unabated in serious strategic planning circles and their associated academic 'Think Tanks'.[5] Part of such discussions is very much of a technical nature. For example, the potential of hypersonic delivery systems that seemingly can penetrate even the most sophisticated missile defence system has been highlighted as a result of the current conflict in Ukraine. Similar technical discussions have also taken place regarding new forms of delivery platforms, missile guidance systems and vitally, control.[6] However, the other part of nuclear discourse focuses on another traditional aspect of nuclear weapons and arguably more akin to asymmetrical conflict, which itself is seen as a likely element of hybrid conflict – the rise of the nuclear outlier or so-called rogue state.[7] As much as one could argue that traditional superpower nuclear policies have been more or less

[2] The USA and the U.K. have long-established security studies NGOs focusing on the development and use of nuclear weapons – which is a reflection of their early development in these countries.

[3] See the IISS annual Military Balance audit.

[4] Cirincione 2020.

[5] Cirincione 2020.

[6] See booth SIPRI and Janes Defence Group for a number of excellent discussions on nuclear weapon technologies.

[7] Venter 2018.

stable since the days of détente, highlighting the significant strides in nuclear disarmament, there are isolated states in the international order that have a different perspective on the so-called nuclear 'balance of power'. Regional powers from about the 1970s began to recognise the potential of nuclear capabilities as a factor in their own security calculations and strove – often in the face of stiff opposition by the traditional powers – to acquire such weapons. Recognising the significant technical and financial challenges to developing such weapon systems, these states often sought to acquire the precursors to weaponry through illegal and dubious methods in the face of regulatory prohibition.[8] One could argue that such policies on the part of states like India, Pakistan and eventually Libya, Iraq, Iran and Syria to acquire such capabilities could be labelled 'hybrid'. The potential use of such weaponry, were it to be either acquired or developed, would need to be seen in the light of hybrid as the arsenals were likely to be sufficient to threaten or contribute to the destruction of a neighbouring rival but was never seriously going to deter a modern nuclear-armed enemy should they decide to engage in brinkmanship. However, you can clearly see, however, that the potential use of such limited capabilities could only make sense in a form of hybrid engagement if it were to have any chance to succeed. Unfortunately, international efforts to dampen such nuclear weapon proliferation has clearly failed and as such, the only realistic response seems to be the use of force to prevent the development of a 'rogue' nuclear capability or accommodation, including possibly deterrence. Economic sanctions, trade and financial, seem to make little impression on a determined state actor seeking to acquire nuclear weapons and it is unsurprising that military planners do consider scenarios where rogue states do possess some rudimentary form of nuclear weapon and pursue a range of policies under the real or imagined security umbrella that they think nuclear weapons offer.[9] However, if such scenarios do suggest the potential for nuclear weapons to form a component of a hybrid strategy, one can equally introduce another more contemporary factor into the equation – the non-state actor seeking or possessing such a capability. Nuclear terrorism is generally recognised as a potential element in various forms of hybrid conflict, either as a stand-alone factor or a proxy for a traditional state actor. This fear has been greatly accentuated by the events of 9/11 and it is fair to say that nuclear

[8] Albright 2010.
[9] Venter 2018.

terrorists armed with so-called 'dirty bombs' have been a mainstay of counter-terrorist risk assessments and exercises for many years. The utility and benefit of the possession of such weapons that accrues for the terrorist is arguably not that different from the benefits assumed by so-called rogue states, including self-empowerment, strength and power, a possible deterrent and leverage through fear and blackmail. It also appeals to ego but in reality, it often reflects fear. The activities of the nuclear terrorist, as far as one can judge, is also pretty similar to those of the rogue state; deceit, concealment, acquisition and barter. Theft will also come in handy but by and large this is not an overwhelmingly important factor and certainly less so than having an 'insider' accomplice embedded in the acquisition process.[10] Of course it is problematic to speculate overly about whether or not a nuclear-armed terrorist group would value playing a subordinate role in a larger hybrid conflict directed by the aims and objectives of others. However, should the terrorist group be a 'proxy' for a state or even a body of state posing as a 'terrorist', the calculations of risk are possibly not far from each other. Certainly, expecting a traditional terrorist group to think on classical strategic conflict lines – for example about using their limited nuclear capability as a deterrent or a rudimentary form of 'extended deterrence' is unlikely but not far fetched, depending on the cause and perspective of the group. It is unlikely that such calculations would detain a 'lone wolf' actor. It would give a false impression of the nuclear security world if one were to ignore the global efforts to prevent or dampen the desire by some states or non-state actors to acquire nuclear weaponry. International efforts to prevent such proliferation have been with us for years, a reflection perhaps that more traditional, diplomatic efforts to secure and contain the growth of nuclear arsenals has been only partly successful and that there exists a flourishing 'black market' or 'proliferation pathway' which sustains efforts to circumvent these controls.[11] At the top of this apex of countermeasures and limitations are – as already mentioned – a network of arms control agreements. In addition to these, however, attempts were made to restrict access to those materials and expertise that would facilitate a clandestine nuclear weapons programme. Arguably, it has been the international community's willingness to prevent such activities that has led, in extremis to the use of

[10] Bunn–Sagan 2017.

[11] The concept of the 'Proliferation Pathway' is often used in government counter proliferation agencies to describe the range of activities undertaken to ensure the smuggling of goods or weapons to support an illegal WMD development programme.

military force to thwart or stall a so-called 'rogue state's' weapon development programme. Notable examples of such intervention in recent times have included the Stuxnet cyber operation against an Iranian nuclear facility, the invasion of Iraq and of course the Abdul Qadeer Khan case. Yet it is this subterranean counter proliferation conflict that could easily lend itself to being or becoming an element of a hybrid conflict. It is frequently difficult to appreciate how an export control violation or the illegal sale of dual use technologies could be a vital component of an aggressive proliferation operation. Similarly, the sophisticated dispersal and concealment of large sums of money in and out of the global financial system, which is necessary to underpin large-scale – usually state-sponsored – proliferation is really akin to 'white collar crime' and quite clearly a hybrid activity of sorts.[12] Whilst trying to address such 'strategic' forms of proliferation, the international community must also strive to stifle and prevent lower level activities most commonly associated with gaining access to radio-active materials – much of it from unlikely sources such as medical facilities or industry – and which could be associated with efforts to create a radiological dispersal device, often touted as the terrorists' weapon of desire. Such efforts to prevent this theft or transport of illegal and hazardous materials – like the efforts at the global and regional level – depends on a combination of reactive and static surveillance and more proactive intelligence-led surveillance and interdiction. Often the most appropriate form of prevention lies in the overlay of several types of activity, which ultimately draw their mandate and method from international frameworks such as the UN 1540 arrangement or the Proliferation Security Initiative (PSI).[13] However, despite the possible similarities between the efforts of rogue states or terrorist groups to acquire a nuclear weapon capability, one should beware of reading too much into this. Proliferation networks – absent outright theft of a nuclear weapon – can operate clandestinely for a number of years but still fail to deliver the sought-after end result. This is most likely to be a lack of certainty that would complicate the more complex choreography of planning that would be necessary in developing a hybrid strategy.[14] What this does suggest, however, is that to effectively discern the role of nuclear weapons in a hybrid context requires a significant investment in early warning architecture, which can provide solid and reliable indicators and warnings.

[12] Zetter 2015.
[13] PSI – Proliferation Security Initiative s. a.
[14] PSI – Proliferation Security Initiative s. a.

Beyond traditional thinking

Despite seeming popular apathy and lack of thinking about nuclear weapons today, it still seems fair to say that there is an absence of sophisticated speculation as to where nuclear weapons might fit into hybrid conflict. Methods of procurement or development aside, it has been difficult to perceive a genuine debate on the role of such weapons on hybrid strategies, although some commentators believe that this is due to change as a result of the current conflict in Ukraine. Yet, this apparent lack of debate is more likely to be the result of knowing where best to position new thinking within the traditional nuclear strategy realm. Look hard enough and you will actually see some fascinating considerations of new thinking about the potential impact of nuclear weapons, although the focus rarely if ever mirrors current forms of analysis. For example, the loss of command and control of nuclear weapons through the hacking of codes and communications architecture. Such a scenario of course is not unique to hybrid conflict if at all but it does bring into focus some new forms of risk and generates new thinking on how best to address the problem. Cyber threats and challenges is a massive security subject and within it, the protection of critical systems features large. Arguably, no military system is more decisive than nuclear arms control, especially on the issue of release. Over the last few years, however, it is possible to speculate, based on an extrapolation of data arising from global cyberattacks, that national control systems might be vulnerable. It is a fact that the private sector is more likely to attract the most creative and gifted coders to commerce than they are to be attracted by government service. This imbalance of talent could suggest that the balance of capability – if used maliciously – might lie with a determined or financially empowered enemy.[15] Should the most critical of communication and authorisation codes relating to nuclear weapon systems be compromised, one could be looking at a factor that might easily fit into a concept of hybrid conflict. Issues such as strategic stability or predictability could be significantly degraded and reading intentions could become more challenging. Indeed, even the short-term disarming or hindering of a state's nuclear alert posture is clearly advantageous to a participant in a crisis whereby nuclear intent might be crucial.[16] An equally disturbing scenario might be the loss of control of an active weapon and facilitating its release onto

[15] Unal–Afina 2020.
[16] Unal–Afina 2020.

its owner or its owner's allies or even onto its owner's enemy. The deliberate release of a nuclear missile onto a densely packed civilian population centre would also have a similar effect. The key question is purpose. To what end would such a scenario make sense? Tragically, such a response is not too difficult to imagine, especially in a context where concealment, clandestine movement, deniability and fake news are prominent features of asymmetrical challenge.[17] Given that imagination is often at a premium in the consideration of forms of activity that might constitute hybrid conflict, it would be foolish to ignore the lessons of recent history in suggesting that the use of specific nuclear facilities could quite easily, if they were to fall out of the control of their operators, become weapons in their own right. There is perhaps no better example in recent years than the hijack and use of civilian aircraft as 'missiles' smashing into civilian targets.[18] It would be inappropriate, however, to assume that such acts, whether it was the attack on the World Trade Center or a future assault to take over control of a nuclear facility would necessarily envisage the callous disregard of civilian casualties. Depending on the author of such an act, it might be the threat of further escalatory acts, which seek to influence an opponent's behaviour that is the purpose of the exploitation of nuclear power and not any particular desire to generate a nuclear explosion. It also has to be noted that the role that cyber weapons might play could be crucial, which suggests that cyber weapon policy is equally as potent in any hybrid conflict. The prime reason why this potential utilisation of a nuclear facility might be attractive to a state engaging in hybrid conflict is obvious. Suddenly, from a position of no nuclear capability, there lies the promise of activating powerful equivalents already prepositioned around the world. Clearly any strategy based on exploiting civilian nuclear facilities has significant limitations. These 'weapons' – if they can be called that – are not yours, by and large not familiar to you, require sophisticated handling, cannot be directed and remain situational. This might lead one to speculate that the aim of turning a nuclear plant into a weapon might only work or be carried out successfully in fairly limited circumstances and that should it be successfully achieved, might suggest a sophisticated and technical opponent who sees the strategic value in blackmail.[19] A repetitive feature of discussions on hybrid

[17] The 9/11 attacks demonstrated a capacity to 'weaponise' traditional forms of technology to support forms of hybrid terrorist attacks.

[18] Clark 2012.

[19] Allison 2006.

conflict is the acute consideration given to the use of some form of rudimentary weapon of mass destruction. Nuclear or radiological material of course features highly by dint of the fact that significant volumes of material are present in a world supported by nuclear energy and aided in key societal sectors, such as medical or engineering, with radioactive materials. In short, it is a short thought from materials available to making some form of improvised explosive device or better still, radiological dispersal device.[20] It is fair to point out that no such terrorist or state sponsored activity has been undertaken using such methods. One can draw the preliminary conclusions that for whatever reason, it has been too difficult to develop such a weapon or there is no intent to do so. Perhaps the return on investment for the perpetrator is insufficiently rewarding. However, in a war situation or major conflict, especially a hybrid conflict, would such calculations remain valid? Undoubtedly the sheer volume of such material would lend itself to the potential development of a small number of devices, so-called 'dirty bombs'. One has the technical expertise to craft such weapons. Yet, in terms of sheer destructive power, the effect is more likely to be less than a similar device using conventional explosive such as Semtex or unconventional mixtures such as the use of fertiliser. If it is appreciated that the destructiveness of such a device is limited, how else might such a weapon become useful? More likely, the exploitation of small quantities of nuclear or radioactive material lies in the shock and fear value that is likely to arise from their use. The typical terrorist generation of fear and panic, usually aimed at generating a certain form of response by the authorities is a valuable and proven weapon and arguably it is the fear factor of the willingness to use this form of nuclear weapon that might credibly add credibility to a hybrid strategy. Arguably the least speculated dimension of nuclear policy in a hybrid contest could be the deployment and eventual use of forms of nuclear weapons in space. Such weapons might figure in forms of warfare ranging from support in destroying competing space assets such as satellites to possibly being launched against targets on earth. Admittedly, much of this seems more akin to science fiction literature than staid global warfare planning but in reality, the decision by major military powers to create Space Commands is a recognition that space-based operations, including in support of nuclear command and control operations, anti-satellite operations and possibly the deployment of some form of nuclear weapon in space cannot be ignored. What could be more hybrid that a strategy that straddles terrestrial and

[20] Allison 2006.

space operational theatres? One would anticipate that only significant military powers will occupy this space but the advent of aggressive cyber operations and the potential small state exploitation of civilian satellites, particularly commercial micro satellites have the potential to impact how one might actually use nuclear weapons in the future. This is an element of potential hybrid strategy that clearly demands further 'horizon scanning'.

Nuclear weapons and recent conflict

The current conflict in Ukraine – arguably an example of hybrid warfare – has been replete with examples of the nuclear question. Perhaps the earliest manifestations of the nuclear dimension arose from comments from Moscow about its possession of a considerable nuclear arsenal, possibly as a way to warn off too direct western or NATO intervention but also as a timely reminder to Ukraine that this was an unequal context.[21] Such sabre rattling was noted but on reflection, it seems to have done little positive for Moscow's position. NATO certainly played down these reminders by reminding Moscow that it also possessed a massive and credible nuclear arsenal. Demonstrations of nuclear strength by Russia continue, ranging from the tests of new missile technology to sea-launched missile exercises. Added to this were the continuing flying of nuclear capable bombers along NATO's borders and the testing of the state of readiness of Russia's nuclear forces.[22] One might convincingly argue that this represents Russian nuclear strategic thinking and they would not be wrong. Nuclear forces are a vital and integral element of Russia's military capability and their thinking about engaging in conflict. Frankly, whether the warfare is classical or hybrid is neither here nor there. Other commentators, however, have highlighted the fact that this is not an engagement involving two nuclear powers due to the unilateral decision by Ukraine – under international diplomatic agreement – to give up its nuclear arsenal. With hindsight, was that a wise move or does the current situation lend itself to suggestions that possessing a nuclear weapon might have prevented the outbreak of hostilities in the first place.[23] Indeed, these deliberations about nuclear policy and in particular Russian nuclear policy have

[21] Cournoyer–Messmer 2022.
[22] Cournoyer–Messmer 2022.
[23] Much of this type of discussion is a mainstay of nuclear deterrence theory.

begun to broach the subject of Russian nuclear doctrine's acknowledgement that a limited tactical nuclear strike might be valuable in setting conditions conducive to ending a military engagement of the sort we see in Ukraine. One could argue that such a development might only be feasible under a hybrid warfare scenario and could not really be contemplated in a classical engagement between two nuclear-armed parties. However, like numerous conflicts across time, space and distance, it is events on the ground that often dictate the tempo and flavour of the conflict and in Ukraine, the Russian assaults and seizure of two critical nuclear power plants and the secondary action surrounding it has sparked another crisis. In engaging in military activity, including the shelling of targets in the vicinity of such nuclear facilities, the risk of some form of accident is increasing daily. In Chernobyl and Zaporizhzhia, Russian forces had occupied – albeit temporarily in the case of Chernobyl – the physical sites and crucially, seized operational control from the operators. In doing so, it exposed the systems to external interference, degraded the capabilities of the operational staff and more worryingly, disrupted traditional communication systems.[24]

Assessing the risk

Knowledge and insight into the operations of a vital system and the equipment and materials associated with it are out of regulatory control. What this might mean is that vital and sensitive knowledge of how to operate or disable such systems could be open to abuse or deliberately or inadvertently transmitted to people of concern. Furthermore, in such circumstances as it pertains at the moment in Ukraine around the Zaporizhzhia plant, there is unlikely to be certainty that all critical equipment or nuclear materials can be accounted for.[25] Why might this be relevant to hybrid conflict? A number of possible scenarios come to mind, not as certainties but simply to illustrate the potential that unfettered access to such materials afford an imaginative adversary. One such scenario might be the future use of materials to support a 'false flag' operation. For example, a release of nuclear material into the atmosphere adjacent to a nuclear facility

[24] It was the proximity of actual shelling and the subsequent seizure of the Zaporizhzhia nuclear power plant in Ukraine which led to the intervention of the IAEA.

[25] This was an important factor in EU energy security decisions developed in late 2022 and early 2023.

and containing a radioactive signature similar to the facility could lead to its closure and a subsequent disruption to national energy supplies and economic disruption. Another scenario might see the smuggling of materials into the hands of organised crime and from there to a particularly dedicated or wealthy terrorist group. Indeed, radioactive material from a site which had been occupied in time of conflict could also find its way to select proxy groups, the future use of which could be clearly linked to a hybrid conflict agenda.[26] As it stands, the intervention by the International Atomic Energy Agency (IAEA) in Ukraine seems the most obvious route for the nuclear conundrum to be resolved but this cannot be guaranteed nor would it solve all the potential risks associated with Russia's current activities.[27] Nuclear specialists would be the first to admit that despite the apparent stability that nuclear weapons can bring to a balance of power, the history of nuclear strategy clearly indicates that there have been times when the world tottered on the brink of a nuclear clash.[28] The most well-known and pertinent example would be the Cuban Missile Crisis in October 1962, when the U.S. and the Soviet Union confronted each other over the Kremlin's decision to deploy tactical nuclear missiles to the small communist state off the United States. Such a decision was unlikely to stand, given the U.S.'s determination to see the weapons removed. The question most people asked at the time was how to prevent escalation amid crisis management?[29] Diplomacy – much of it secret – did in the end create the conditions for a resolution but as historians have revealed since then, the situation was not only fraught with high-stakes geopolitical gambling but was also frames to an extent by faulty analysis and appreciation of the actual state of play concerning the weapons and tactics themselves. The most disturbing historical revelation was the acknowledgement by the Soviet Union that the local commander on the ground had release authority should the situation escalate and hostilities break out. Since then, other instances of nuclear risk emerged, including at the time of a stand-off in the late 1960s between the Soviet Union and China, the 1973 Yom Kippur War and the infamous systemic error in the Soviet system, in the late 1980s, had the Soviet Nuclear Command almost convinced that the U.S. had launched a surprise nuclear attack on the Soviet Union. On that occasion, human intervention by a Soviet officer overruled

[26] See IAEA s. a.
[27] IAEA s. a.
[28] Plokhy 2022.
[29] Hoffman 2011.

the technical alert system and led to a satisfactory outcome to the crisis. Why are such examples important? The examples above occurred during a period of confrontation that was sensitive to the enormity of the power of nuclear weapons and as such, an arrangement of sorts about both their use and threat of use had been created. Not only was the mantra of 'mutually assured destruction' a sobering thought but the choreography of 'last resort' graduated response clearly signalled that although nuclear weapons were an integral element of national power, they were not really weapons to brandish at the drop of a hat.[30] Hybrid warfare on the other hand, holds out the potential of a more complex, constantly shifting and indeterminate phases between preparation, planning, action, resolution, de-escalation and bluff. Indeed, once set in motion, can one predict with any certainty that events by their nature and location are just that, disparate and unlinked activities or part of a mosaic or jigsaw that will eventually mushroom into a focused act of aggression? In essence, trying to gain early warning of a potential nuclear component to a hybrid strategy is a significant task. It isn't that we lack indicators and warning of threats and in particular, the specific threats of nuclear deployment, threat or attack. It isn't the risk matrix that is likely to be challenged but our ability to see such incidents as part of a sophisticated and multi-level, organic challenge. How do we create such analytic systems but arguably more important, how do we refine our decision-making culture in the face of quite unusual future nuclear risks? That perhaps signals one of the most attractive or frightening aspects of a nuclear empowered hybrid challenge.

Conclusion

As the short review above seeks to demonstrate, nuclear weapons still retain their importance and some would say their centrality in modern military doctrine. There is nothing to suggest that this situation will not persist for many years to come. Therefore, it would be a mistake not to consider that those states that have nuclear weapons have considered their deployment and even possible use in a range of eventualities. Some of these eventualities would have included speculation and discussion on the contours of hybrid conflict. What then might be the features of a hybrid conflict that might lend itself to a nuclear option? This can only be answered properly if we try and distinguish between those

[30] Hoffman 2011.

with nuclear weapons and those without. It might appear a fallacious distinction but in terms of scoping out options, it is not unreasonable. For a nuclear power, therefore, using weapons in a hybrid conflict will always be an option, especially when one takes into consideration real or likely adversaries. Options for using or threatening to use such weapons could depend on prior planning or simply reflect strategic considerations during a campaign. On balance, perhaps the most advantageous way for a nuclear power to behave is to threaten their use, thereby creating strategic ambiguity, perhaps encouraging confusion or simply trying to simply frighten an enemy into submission or acting in a certain way. One way or another, possessing nuclear weapons offers options and flexibility that a non-nuclear adversary cannot match. Such a disadvantage might be the catalyst required by a protagonist to either acquire a nuclear capability through a dedicated weapons programme or to set out to structure a tactical capability based on low level acquisition or theft. This development time would largely depend on circumstances but again the contour of potential exploitation of a rudimentary capability lies in the ability to either threaten to use such a weapon in order to influence events or use it to inflict some form of asymmetrical response. It is hard to see how the damage of a 'dirty bomb' for example could significantly damage a nuclear opponent but it might have a more meaningful impact against another non-nuclear power. At this level of engagement, nuclear weapons in a nominally nuclear free environment could significantly alter the balance of power but again, if the weapon be a simple radiological dispersal device, would it really count for much in a hybrid conflict? Arguably, the most obvious role for a non-traditional nuclear power in a hybrid conflict is to avoid conflict unless the threat is existential. However, should deterrence fail, threatening to use a nuclear capability previously undeclared and not described in any detail would create that sense of ambiguity that might be useful in a hybrid setting. Should it prove necessary to follow through on the threat and absent anything other than an improvised weapon and delivery platform, the protagonist would in all likelihood be advised to create fear and panic or any other destabilisation action that could possibly influence the course of an aggressor. That, frankly, is a significant gamble. A much wider consideration might be the notion that any state that has serious regional intentions would seek to acquire a nuclear capability of some sort, preferably one that looks and feels like a traditional weapon system and which could fit seamlessly into a hybrid strategy. If this becomes likely and there are few good reasons why it should not then western strategists might have to invest greater effort into planning the management of

a hybrid conflict, which could include nuclear weapons. Such considerations might become the staple fare of war college studies and strategy symposia but it would also force a review of hybrid countermeasures and the framing of new risk analysis paradigms. By implication, this might suggest that in the future, nuclear proliferation might become an underlying feature of hybrid posture and might require the international community to recalibrate its global counter proliferation posture. Not only would materials and processes associated with nuclear proliferation become objects of enhanced control and surveillance but so also would the spectrum of emergent technologies. Finally, hybrid conflict and its unpredictable nature might force greater efforts to be undertaken by determined actors to use cyber means to disrupt the nuclear capabilities and operations of a nuclear armed opponent. Hacking and cyber disruption operations are likely to increase in intensity and unfortunately it will not take too many hijackings of a nuclear weapon and its subsequent detonation to significantly alter some of the strategic calculus of nuclear powers. A careful and prudent surveillance of technical developments in fields such as artificial intelligence and quantum computing might throw light on the future vulnerability of nuclear weapon systems and their associated command and control systems. The fear will be that under hybrid conditions, launch authority is devolved to smart intelligent machines in order to hasten and reinforce responses from external interference and reaction times that are counted in seconds. Nuclear weapons in a future hybrid warfare scenario might be difficult to predict but there is no doubt that they would not reduce concerns but possibly complicate what has been hitherto a fairly stable arrangement as far as modern conflict is concerned. If that is the case, then perhaps we have to explore more deeply what a hybrid concept of modern conflict might develop into, in the not too distant future.

Questions

1. Describe the benefits of incorporating nuclear weapons into a national hybrid warfare strategy and what the potential drawbacks might be of this approach?
2. How might cyber capabilities used under a hybrid conflict scenario influence the behaviour of a nuclear state?
3. Explain how stolen or illegally procured radioactive material could be used in a hybrid conflict situation?

4. How effective could a 'false flag' nuclear release event be in influencing the outset of a hybrid warfare campaign?
5. Do concepts of hybrid warfare and the nuclear dimension encourage proliferation? Discuss.

References

Albright, David (2010): *How the Secret Nuclear Trade Arms America's Enemies. Peddling Peril.* New York: Simon Spotlight Entertainment.

Allison, Graham (2006): *Nuclear Terrorism. The Risks and Consequences of the Ultimate Disaster.* London: Constable and Robinson.

Bunn, Matthew – Sagan, Scott D. eds. (2017): *Insider Threats.* Ithaca–London: Cornell University Press.

Cirincione, Joseph (2020): *Bomb Scare. The History and Future of Nuclear Weapons.* New York: Columbia University Press.

Clark, Richard A. (2012): *Cyber War. The Next Threat to National Security and What to Do About It.* New York: Ecco.

Cournoyer, Julia – Messmer, Marion (2022): *Ambiguous Nuclear Threats Heighten Catastrophic Risks.* Online: www.chathamhouse.org/2022/09/ambiguous-nuclear-threats-heighten-catastrophic-risks

Hoffman, David E. (2011): *The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy.* London: Icon Publishers.

IAEA (s. a.): *Nuclear Safety, Security and Safeguards in Ukraine.* International Atomic Energy Agency. Online: www.iaea.org/nuclear-safety-security-and-safeguards-in-ukraine

Plokhy, Serhii (2022): *Nuclear Folly. A New History of the Cuban Missile Crisis.* London: Penguin.

PSI – Proliferation Security Initiative (s. a.). Online: www.psi-online.info

Unal, Beyza – Afina, Yasmin (2020): *How to Deter Cyberattacks on Nuclear Weapons Systems.* Online: www.chathamhouse.org/2020/12/how-deter-cyberattacks -nuclear-weapons-systems

Venter, Al J. (2018): *Nuclear Terrorism. The Bomb and other Weapons of Mass Destruction in the Wrong Hands.* Barnsley: Pen and Sword Military.

Zetter, Kim (2015): *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon.* New York: Broadway Books.

Further reading

Abbasi, Rizwana (2020): *New Warfare Domains and the Deterrence Theory Crisis.* Online: www.e-ir.info/2020/05/13/new-warfare-domain-and-the-deterrence-theory-crisis/

Abid, Amber Afreen (2022): Hybrid Warfare: A New Face of Conflict in South Asia. *Eurasia Review,* 29 July 2022. Online: www.eurasiareview.com/29072022-hybrid-warfare-a-new-face-of-conflict-in-south-asia-oped/

Blackham, Jeremy – Graydon, Michael (2020): No Short Cuts to Deterrence in a World of Hybrid Warfare. *Briefings for Britain,* 18 September 2020. Online: www.briefingsforbritain.co.uk/no-short-cuts-to-deterrence-in-a-world-of-hybrid-warfare/

Boulton, Frank (2022): The Nature and Consequences of a Nuclear War: Lessons for Prevention from Ukraine 2022. *Medicine, Conflict and Survival,* 38(3), 184–202. Online: https://doi.org/10.1080/13623699.2022.2093571

Brozowski, Alexandra (2021): NATO to Focus on Hybrid Warfare, How to Deter Russia. *Euractiv,* 21 October 2021. Online: www.euractiv.com/section/defence-and-security/news/nato-to-focus-on-hybrid-warfare-how-to-deter-russia/

Cabot, Adam (2021): *China's Nuclear Threat against Japan: Hybrid Warfare and the End of Minimum Deterrence.* Online: www.realcleardefense.com/articles/2021/08/06/chinas_nuclear_threat_against_japan_hybrid_warfare_and_the_end_of_minimum_deterrence_788893.html

Hinton, Megan (2022): Russia Accuses West of 'Total Hybrid War' despite Threatening to Nuke UK in Seconds. *LBC News,* 14 May 2022. Online: www.lbc.co.uk/news/russia-threatens-uk-nuclear-satan-2-hypersonic-missile/

Kucharski, Lesley (2018): *Russian Multi-Domain Strategy against NATO: Information Confrontation and U.S. Forward-deployed Nuclear Weapons in Europe.* Online: https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_ NATO_nuclear_posture.pdf

Latiff, Robert H. (2017): *Future War. Preparing for the New Global Battlefield.* New York: Alfred A. Knopf.

Mbodouma, Victor (2021): Is the US Nuclear Strategic Deterrent Fully Adequate to Dissuade Today's New Threats. *Strategic Studies Quarterly,* 15(3), 3–5.

Najzer, Brin (2022): *The Hybrid Age. International Security in the Era of Hybrid Warfare.* London: I. B. Taurus.

Nichols, Michelle (2022): West Could Trigger Nuclear War over Ukraine, Russia Says at U.N. *Reuters,* 3 August 2022. Online: www.reuters.com/world/europe/west-could-trigger-nuclear-war-over-ukraine-russia-says-un-2022-08-02/

Rautenbach, Peter (2019): The Subtle Knife: A Discussion on Hybrid Warfare and the Deterioration of Nuclear Deterrence. *The Journal of Intelligence Conflict and Warfare,* 2(1), 34–54. Online: https://doi.org/10.21810/jicw.v2i1.951

Reach, Clint (2022): *Escalation and Deescalation of Crises, Armed Conflicts, and Wars.* Online: www.ndc.nato.int/research/ research.php?icode=751

Roushan, Anurag (2022): Russia Says US Steps to Engage in Hybrid Warfare with Moscow over Kyiv Raise Nuclear Risks. *Republic,* 16 August 2022. Online: www.republicworld.com/world-news/russia-ukraine-crisis/russia-says-us-steps-to-engage-in-hybrid-warfare-with-moscow-over-kyiv-raise-nuclear-risks-articleshow.html

Sechser, Todd S. – Fuhrmann, Matthew (2017): *Nuclear Weapons and Coercive Diplomacy.* Cambridge: Cambridge University Press.

Shishkin, Mikhail (2022): The West Is Trying to Quietly Forget the War in Ukraine. It Does So at Its Own Peril. *The Guardian,* 22 August 2022. Online: www.theguardian.com/commentisfree/2022/aug/21/the-west-war-ukraine-vladimir-putin-russia

Smith, Charlie (2022): Putin Would 'Use Nuclear Weapons' against Xi in Chinese Invasion of Siberia: 'Fair Chance'. *Express,* 23 August 2022. Online: www.express.co.uk/news/world/1658620/putin-news-nuclear-weapons-xi-jinping-china-invasion-siberia-spt

Tagarev, Todor (2019): Theory and Current Practice of Deterrence in International Security. *Connections: The Quarterly Journal,* 18(1–2), 5–10. Online: https://doi.org/10.11610/Connections.18.1-2.00

Tham, Gabriel – Wong, Edward – Kuo Kai Ming, Kelvin (2017): Technologies in Hybrid Warfare: Challenges and Opportunities. *Pointer, Journal of the Singapore Armed Forces,* 42(1), 12–24.

Wilkie, Robert (2009): Hybrid Warfare: Something Old, Not Something New. *Air & Space Power Journal,* 23(4), 13–17.

Woodroofe, Jason (2021): *War in a Time of Peace – Is Hybrid Warfare the New Norm?* Online: https://theowp.org/war-in-a-time-of-peace-is-hybrid-warfare-the-new-norm/

Andrew Dolan[1]

Biosecurity State: Responding to Malicious Biosecurity Risks

Quite early on in the current Ukraine conflict, the Russian Authorities claimed, with very little supporting evidence, that the United States (U.S.) had been developing biological weapons in Ukrainian laboratories. Observers highlighted the so-called 'fake news' angle to these claims – a key facet of modern hybrid conflict. However, coming hard on the heels of the global Covid pandemic, it generated a more than passing interest in the possibility of future conflict being linked to biowarfare.[2] Such suggestions are easy to make but the question remains – how likely is the use of biological weapons in a future hybrid conflict scenario? Do the circumstances exist, which suggest that states might deliberately seek to create or acquire biological weaponry and worse, actually consider their use?

Biological weapons and conflicts

Fortunately, the world has been spared – so far – the scourge of a major global conflagration using biological weapons. A major factor in this situation is the fact that so few states have actively sought to develop a viable and significant biological weapons programme and those who have traditionally considered them as a feature of a rounded military capabilities posture, such as the former Soviet Union and the United States, have gradually eliminated their stockpiles.[3] One might argue that the description above is partial, however. Various states have claimed that they adhere to the Biological Warfare Convention (BWC), which prohibits the development, production, acquisition, transfer, stockpiling and use of biological agents or toxins as outlined by the Convention. However, there is a lingering suspicion that some states might have attempted to circumvent the prohibition and have sought to develop a workable weapons programme or

[1] Centre for the Study of New Security Challenges.
[2] Inskeep–Yousef 2022.
[3] See UNODA s. a.

DOI: https://doi.org/10.36250/01236_07

at least conducted the research that might allow them to do so quickly. Given that the BWC has no inspection or verification mechanism, then such suspicions are difficult to either confirm or deny.[4] There is also a significant concern that non-state actors might seek to acquire or develop their own stock of biological weapons. The use of simple pathogens or toxins has been associated with the occasional terrorist attack, although again, the incidences have been thankfully low.[5] The attraction of having or using a biological weapon remains relevant and multi-faceted. Depending on the type of biological weapon, it is possible to inflict a range of suffering or hardships on an adversary. Traditional concerns tend to focus on death and illness and the generation of significant societal dislocation associated with a public health emergency. For some advocates of the use of such weapons, this dislocation and disruption could be an end in itself and not simply an element of a larger operational assault. For others, the ability to create panic and sow public distrust might be enough to degrade a state's ability to respond in a crisis or effectively build up a willingness to actively resist an adversary.[6] Certainly, it is also more than likely that the effective, targeted and graduated use of biological weapons could lead to severe economic shock and significantly alter the calculus of engaging in conflict. Other observers are becoming more alarmed at the potential environmental damage that such a conflict might engender if there is a widespread use of toxins that in extremis, could lead to food shortages or spiralling prices. If such events can happen in relation to energy shocks, then why not in relation to disruptions in the food chain? Such 'shocks' to global stability clearly suggest that 'scale' matters – if a biological weapons strike were of sufficient magnitude, it could, given time, have a massive disruptive effect. One need only examine the current global Covid pandemic to witness the effect of the world's relative inability to halt the spread of a highly contagious biological risk and the recent medical barriers have taken months to develop by which time millions of people have died in the interim. Therefore evidence, if evidence was needed, that biological threats, if 'weaponised' can wreak havoc on an unprotected and unsuspecting global population. Yet under a traditional conflict scenario, the originator of such a weapon would presumably have a purpose for using such weapons and as such would wish to have a degree of control over both use and the resulting consequences. Would this remain the

4 UNODA s. a.

5 Kaplan–Marshall 1997.

6 Chan–Ridley 2022.

case in relation to hybrid conflict? Can we assume that the use or possession of biological weapons will be conceived in a hybrid conflict as that of a traditional conflict? Do the circumstances under which one might posit the adoption of a hybrid strategy continue to lend themselves to the identification of an advantage through biological weapons? The answer to this question depends largely on the conception you might have of what constitutes a hybrid strategy. Indeed, it might depend more on whether or not you can acquire a biological weapon than whether or not you might like to consider its use.[7] By and large, acquiring a nuclear weapon is akin to the acquisition of a nuclear capability – it clearly can be a weapon of mass destruction, it can be developed in such a way to calculate the scale and form of destructiveness and it might lend itself to various forms of 'delivery'. Indeed, one might argue that it is the issue of 'delivery', which might be a distinguishing feature of both the weapon and the form of conflict.[8] Therefore, in a traditional form of conflict calculus, possessing a biological weapon offers a form of capability, which can be exploited in various ways. Of course this recognition of capability or strength only works if you are willing to communicate this fact to an adversary. The leverage such a weapon might afford you is commensurate with the level of concern its announcement generates on the intended recipient of the news.[9] Yet clearly, the hesitancy and unpredictability that might arise from the mere suspicion that a state possesses such a weapon cannot be ignored and would undoubtedly impact any risk assessment within an adversarial relationship. Even the hint that a state has been researching or trying to develop a biological weapon and a delivery platform to go with it is difficult to plan against other than the adoption of a 'worst case scenario' posture.[10] Therefore, should it be in the interest of a state to acquire a reinforced sense of protection, especially within a hybrid setting, then in that case, acquiring a biological weapon might make sense. There is another scenario, however, within a set of hybrid considerations, that needs to be explored and that could be the use of a proxy or non-state actor to either acquire or deploy such a weapon. The use of proxy forces or terrorists within a hybrid conflict setting is frequently cited in professional literature exploring the subject. The attraction of conducting operations, which are either deniable or unattributed, is often cited as a force

[7] Mangold–Goldberg 1999.
[8] Mangold–Goldberg 1999.
[9] Mangold–Goldberg 1999.
[10] Alibek 2000.

multiplier in a hybrid conflict and certainly one can see the value, especially if it secures strategic or operational surprise. Using biological weapons under such circumstances could be worth the effort, especially if one could control the strike and delivery and crucially, the outcome. However, one can also identify some drawbacks. Using biological weapons would require, depending on the nature and scale of an attack, very precise planning. A limited biological event is not beyond the capabilities one would assume of a proxy force with all the likely support of the sponsor state that would go with it and even a dedicated and professional terrorist group. One could even imagine, depending on the nature of the pathogen or toxin, a so-called 'lone wolf' event. Yet such planning by definition might open up the originator of the attack to scrutiny – perhaps due to an adversary's indicator and warning system – or simply due to missteps in the preparation stage, such as the need to test the weapon or the delivery system. Equally, should the planned attack fail to materialise for whatever reason or become compromised, the repercussions might trigger an immediate reaction or alter a well-rehearsed plan of hybrid pressure within an overall hybrid concept of operations. Indeed, given that biological weapons are considered weapons of mass destruction, it is feasible that a botched attack or indications of an impending attack could trigger an asymmetrical response and one, which might include the use of other forms of weapons of mass destruction. If a biological strike against a nuclear power were to unfold, one considered by them to be an 'existential threat' – then it is quite conceivable that the retaliation might unleash an unanticipated strategic response.[11] It is clearly possible, therefore, to speculate that a hybrid strategy could easily include a biological element but before a more valued assessment might be made, it is worth considering a much more fundamental question and that is the question of how likely is it today that a non-superpower or possible proxy or terrorist group might acquire a biological weapon?

Biotechnology and biosecurity

An interesting feature of the Covid pandemic has been the need to discover the origins of the outbreak and as much detail as possible about the pathogen. This has led to numerous investigations into the origins of Covid and interestingly, it

[11] Chan–Ridley 2022.

throws light on how such outbreaks occur, how they develop and where the scientific community fits in.[12] For many months after the outbreak, the international public health community was minded to frame the outbreak as a natural zoonotic occurrence, not much different from SARS or MERS. That early view was never fully accepted by all in the medical or scientific community and as more evidence and data came to light, the consensus opinion was forced to change. A significant body of opinion began to dissent from the 'public' narrative and even though debate continues to persist, the general public has been provided with an insight into some of the contours of current cutting-edge biotechnology research and development. This activity, much of it conducted under less than transparent conditions and in a network of global laboratories could understandably be abused by those harbouring malicious intent of having a clearly dual purpose. A major problem regarding all forms of weapons of mass destruction proliferation is this very problem of the use assigned to so-called 'dual use technologies'. The issue therefore within the ambit of hybrid conflict and biological weapons is possibly that any attempt to develop a biological weapons programme would lean heavily towards the illegal acquisition of biological material, specialist research data and perhaps more intriguingly, acquisition of experts.[13] Most public discourse on biosecurity risks tend to focus less on the use of bioweapons in a state on state conflict and more towards a possible dystopian future resulting from some form of natural or intentional man-made pandemic. Much of this angst is more likely than not to be a result of the fear generated globally by the Covid pandemic and speculation regarding its origin, although one can make a plausible case for saying that mass media and entertainment outlets have exploited such fears, through both TV and film. It would be unwise, however, to dismiss such fears as being forms of unthinking paranoia. Given that surprise is a traditional ingredient of conflict, hybrid or otherwise, then the factors behind lethal pandemics cannot and should not be dismissed as either a form of deliberate attack or simply an accident. If there is one thing that Covid has demonstrated is the need to determine how and where the deadly pathogen emerged – not only for purposes of attribution but also to prevent baseless accusations. If it had not been for the drive to find the cause of the Covid outbreak, most of us would be unaware of the scale of cutting-edge international biotechnology development that goes on in many of our countries, the very acute risks associated with gain of function

[12] Chan–Ridley 2022.
[13] Kaplan–Marshall 1997.

experimentation and the vast financial rewards linked to significant medical or pharmaceutical breakthroughs.[14] Could this be attractive to a hybrid conflict adversary? If this adversary is sufficiently weak in a power relationship and wishes to eliminate or rebalance this supposed weakness, then clearly having access to some pretty lethal and nasty pathogens or toxins for example is not outside the bounds of possibility. Whether the actor that deliberately seeks to acquire such material or the results of the experimentation is a state or non-state, the risk of a deliberate 'release' could be globally consequential depending on the lethality of the agent released. It is unfortunate but occasionally, aspersions are cast against scientists or technicians or medical practitioners as being either excessively secretive or even deceitful in the conduct of their research, especially in those fields which form part of life sciences and biotechnology or bioengineering. Yet equally, a blanket clean bill of health cannot be assumed. Covid investigations have unearthed a range of worrying practices, including poor health and safety and security protocols in laboratories, unnecessary risky experimentation where the risk of failure could have significant consequences and human frailty. All of the above could, under certain circumstances, be exploited in a deliberate attempt to acquire or manufacture a bioweapon. Furthermore, it would be unwise also to dismiss the sums of money, which support biotechnology research and development – a beacon for corrupt individuals within the sector to exploit their access or be susceptible to corruption. However, is the public perception accurate or meaningful or insightful? Is there any relevance here to hybrid conflict? Unfortunately, the answer must be yes – albeit a qualified yes. The potential negative outcomes and possibilities of the above can lead to or support an attempt to acquire or release a lethal virus or toxin. The medical and biotechnology community is only too aware of such risks, although by and large the research community is more likely to view these risks through the prism of accident. Nevertheless, the outcome might be somewhat similar. That these risks have become accentuated since the global pandemic is witnessed through the significant enhancement of state preparedness for a future global biological event. Encouraging as this is, however, the desire to enhance safety and security at sites or facilities, which might attract a higher level of risk can only really be achieved in stable, well-functioning states. The level of confidence in the security of medical or pharmaceutical research in weak or so-called failed

[14] See The Economist 2021.

states inspires less confidence.[15] Additionally, the nature of global academic research and technological research is such that transparency and sharing of results of research is the default setting. For example, controlling sensitive research data is difficult within a transnational setting and if there is a clear commercial interest involved, governments are far less well placed to keep an eye on significant technical developments, including those linked to bio and life sciences.[16] As a result of these marketplace developments, governments are being forced to recognise that some of this activity could very well be used to support a hybrid conflict activity and the question is, how do you identify the potential indicators and warnings, especially when the understanding of hybrid conflict is so shallow and fragmented? Undoubtedly, traditional security specialists are being pushed towards having a more inclusive view of the potential threats, risks and challenges associated with these emerging and evolving issues. Indeed, one could argue that what needs to develop is a new risk calculus. That novel forms of bioweaponry are likely to emerge sooner rather than later, then it might be prudent to gauge what form such weapons might take, how they might be used against a range of hybrid targets and where they might fit into a hybrid strategic, operational or tactical setting. Furthermore, by making such assumptions, or simply seeking to develop a 'tout azimuth' approach to security, one must ask if the current and traditional forms of early warning and risk assessment can be of much use in these bio technology settings? Public Health and National Security are not natural bedfellows when it comes to strategic priorities and methodologies but under a hybrid context, we might need to consider how well or otherwise such a biohazard partnership might emerge in the future.[17]

Implications of the evolving biothreat

It is far from easy to speculate if the use of bioweapons in a hybrid conflict is more or less likely. Those who point to the Covid pandemic tend to emphasise the potential widespread reach of the public health crisis and therefore anyone with a malicious intent might be tempted to create or use a bioweapon if they had

[15] De Bretton-Gordon 2020.

[16] House of Commons 2021.

[17] This will possibly lead to a new type of investigator that has both a law enforcement and public health remit, which also implies specialist recruitment and training.

access to it. However, equally, one might highlight the fact that the actual ability to control such a pathogen's spread – ensuring no 'blowback' so to speak – is tenuous at best. Current levels of globalisation challenge such considerations. If the idea of using bioweapons in a hybrid context was to achieve surprise, then arguably this might be possible but to view it as a flexible and measured weapon of strategic significance could be a step too far. Equally, however, developing a new bioweapon programme based on current cutting-edge bioengineering is most certainly within reach of both a state and a non-state actor. Even under hybrid conflict conditions, the limited application of a targeted biowarfare capability could accrue significant advantages, ranging from weakening a particular target or target group to instilling general fear and panic should the weapon be linked to other information warfare elements of hybrid strategy.[18] Yet, actually one of the major unintentional risks of developing an active biosurveillance system is that it impinges on a fundamental aspect of a democratic society – privacy. The potential friction and stress that a constant biosurveillance environment might generate could in itself be a desired outcome for an adversary that 'flags up' in some way their access to bioweapons and a willingness to use it. Such claims can be investigated to an extent but just how effective would such auditing be? Short of significant levels of proof that such a capability exists and that it is either pre-deployed or could be readily deployed against you, how does a state react? How do you assess if such a risk is real but is located in another territory? If all you can realistically do is to deploy sophisticated surveillance systems, including, in extremis, periodic 'lockdowns' in response to isolated or coordinated disease outbreaks, then the fundamental concept of an 'open society' could be put in jeopardy. Indeed, in a society where biotechnology and life sciences is a significant part of the fabric of that society, there is likely to be precious little consensus even on were we place our security: do we put academic and technical life science development under surveillance? Do we vet bioengineers? Should laboratories be policed? Should foreign students across a range of technical studies be banned? Fears of hybrid conflict involving bio-weaponry are not necessarily unfounded but they certainly do impact on a wider slice of life. Perhaps the obvious point of departure for a consideration of how best to deter or defend against bioweapons in a hybrid context is to engage in

[18] Consider the fear and panic created in the USA as a result of anthrax terror attacks, which although resulted in a small number of deaths, the response generated was significant on the part of the U.S. authorities.

some philosophical investigation. Considering bioengineering or life sciences as a so-called 'dual use' activity might be as good a place as any to start. Unfortunate as it might be, it is impossible not to recognise the lethal potentiality of activities that exploit life sciences and associated technologies, such as artificial intelligence or nanotechnology, in the process of creating bioweapons. One has only to look at the scale of Soviet 'Cold War' era bioweapons programmes to understand how thousands of scientists could dedicate their professional careers to cutting-edge research and development in pursuit of weapons.[19] It is essential therefore that such an approach be embedded into a wider scheme of information and educational outreach to the target scientific and technical audience. The security community should be encouraged to join with the public health community in working alongside the biotechnology community in order to provide adequate warning of the potential hazard that might emerge or develop as a result of research, the outcome of which might not even be known let alone understood.[20] It will also be necessary to enhance the security of those materials and processes, which are integral to work on this challenging field. This should not be considered as a new departure related to hybrid conflict – it clearly is not. What is new, however, is the scale of development in this field and the clear overlapping of various disciplines, ranging from microbiology and toxicology to algorithm design and development and cloud computing. Efforts must also be made to better guide and regulate those who work in this field, not only in terms of regulatory frameworks – perhaps based on international norms but also in respect of developing legislation – a not unexpected outcome of the levels of concern relating to biosecurity that has emerged in the wake of the Covid pandemic.[21] Clearly such developments will inevitably lead to more intrusive vetting of key scientists, researchers and students working in this sector and with it perhaps a more stringent control regime for gaining access to those materials needed to develop the vaccines and other pharmaceuticals that society so plainly relies upon. The unstated or understated concern here is not simply access to physical 'precursors' – for the want of a better description but a requirement to dampen or completely eliminate the risk of intangible technology transfer.

[19] Alibek 2000.

[20] Such a solution will be far from simple to structure but it seems a logical progression in terms of government responses to biosecurity threats.

[21] The Global BioLabs Report of King's College, London is an excellent tool for examining the potential risks facing the biosecurity communities in labs. See King's College London 2023.

Obviously to do this effectively impacts on the association of cybersecurity and 'insider threats', two methods commonly used to illegally gain access to research, material and personnel.[22] In the years ahead, this concept of greater transparency and regulation – which might be contested by interests within the sector and which, although partisan, are not unaware of the hazards linked to the science and research of the life sciences and biotechnology community – there might come a time when this sector is placed on an equal footing with the nuclear energy community and even more severe, as an aspect of national security.[23]

Conclusion

All of the above considerations and explanations are not unique to concepts of hybrid conflict. They might apply to a future hybrid clash but equally might be just as likely to support a traditional clash or even support the tactics of a so-called 'lone wolf' terrorist or technologically capable non-state actor group, including organised crime. The potential attraction of bioweapons might lie in the shock and surprise associated with its release and the resultant panic. This inculcation and generation of fear clearly has an asymmetrical value if nothing else. Furthermore, events in the Middle East have demonstrated that deploying chemical weapons might suggest that doing something similar with bioweapons is not in any way and act 'beyond the pale' or beyond calculation of gain and loss. What seems different today is the perception that novel weaponry is a 'norm' and that if an actor in a clash with a superior power can acquire or develop even a rudimentary form of bioweapon, the chances are that use might be considered. Realigning the way we try and control the bio sector might eventually lead to tighter and less advantageous area in which to short circuit the development of a weapon of mass destruction programme and by association, make the sector more resilient to abuse. The key question, however, is who will lead the way in calling for such a 'realignment' at a time when 'novelty' in our post-modern context is considered a sign of 'cleverness' and sophistication.

[22] King's College London 2023.
[23] King's College London 2023.

Questions

1. Explain how a bioweapon – if released in an urban environment – could contribute to strategic surprise in a hybrid conflict?
2. What could be the main disadvantages of using bioweapons in a major conflict?
3. In terms of gaining access to controlled information within a biotechnology environment, would cyber penetration or a so-called 'insider threat' be more effective?
4. What forms of deterrence would be most effective against a bioweapons threat?
5. Should the EU acquire a bioweapons capability? Discuss.

References

Alibek, Ken (2000): *Biohazard. The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told from Inside by the Man Who Ran It.* New York: Arrow.

Chan, Alina – Ridley, Matt (2022): *Viral. The Search for the Origin of Covid-19.* London: Fourth Estate.

De Bretton-Gordon, Hamish (2020): Biosecurity in the Wake of Covid-19: The Urgent Action Needed. *CTC Sentinel,* 13(11). Online: https://ctc.westpoint.edu/biosecurity-in-the-wake-of-covid-19-the-urgent-action-needed/

House of Commons (2021): *Biosecurity and National Security: Government Response to the Committee's First Report of Session 2019–21,* 1 March 2021. House of Commons – House of Lords, Joint Committee on the National Security Strategy. Online: https://committees.parliament.uk/publications/4870/documents/49008/default/

Inskeep, Steve – Yousef, Odette (2022): Russia Claims U.S. Labs across Ukraine Are Secretly Developing Biological Weapons. *NPR,* 22 March 2022. Online: www.npr.org/2022/03/22/1087991730/russia-claims-u-s-labs-across-ukraine-are-secretly-developing-biological-weapons

Kaplan, David – Marshall, Andrew (1997): *The Cult at the End of the World. The Incredible Story of Aum.* Stratford-Upon-Avon: Arrow Books.

King's College London (2023): *Global BioLabs Report.* Online: www.kcl.ac.uk/warstudies/assets/global-biolabs-report-2023.pdf

Mangold, Tom – Goldberg, Jeff (1999): *Plague Wars. A True Story of Biological Warfare.* London: Macmillan.

The Economist (2021): What Is "Gain-of-Function" Research? *The Economist,* 1 November 2021. Online: www.economist.com/the-economist-explains/2021/11/01/what-is-gain-of-function-research

UNODA (s. a.): *Biological Weapons Convention.* United Nations, Office For Disarmament Affairs. Online: https://disarmament.unoda.org/biological-weapons/

Further reading

American Academy of Family Physicians (2020): *Bioterrorism.* Online: https://family-doctor.org/bioterrorism/?adfree=true

Australian Government (2023): *Commonwealth Biosecurity 2030.* Department of Agriculture, Fisheries and Forestry. Online: www.agriculture.gov.au/biosecurity-trade/policy/commonwealth-biosecurity-2030

Australian Government (2024): *Biosecurity Risk Analysis.* Department of Agriculture, Fisheries and Forestry. Online: www.agriculture.gov.au/biosecurity-trade/policy/risk-analysis

Australian Government (s. a.): *Biosecurity in Australia.* Department of Agriculture, Fisheries and Forestry. Online: www.agriculture.gov.au/biosecurity-trade/policy/australia

Bennett, Kerry (2022): Disease Ecologist Investigates 'Stealthy' Pathogen in Iraq. *The NAU Review,* 14 September 2022. Online: https://news.nau.edu/foster-brucella/

Boyle, Francis A. – King, Jonathan (2005): *Biowarfare and Terrorism.* Atlanta: Clarity Press.

Cummings, Christopher L. – Volk, Kaitlin M. – Ulanova, Anna A. – Lam, Do Thuy Uyen Ha – Ng, Pei Rou (2021): Emerging Biosecurity Threats and Responses: A Review of Published and Gray Literature. In Trump, Benjamin D. – Florin, Marie-Valentine – Perkins, Edward – Linkov, Igor (eds.): *Emerging Threats of Synthetic Biology and Biotechnology. Addressing Security and Resilience Issues.* Dordrecht: Springer, 13–36. Online: https://doi.org/10.1007/978-94-024-2086-9_2

Dando, Malcolm R. (2006): *Bioterrorism and Biowarfare. A Beginner's Guide.* London: Oneworld Publications.

Duong, Thi Tam – Brewer, Tom D. – Luck, Jo – Zander, Kerstin K. (2019): Understanding Biosecurity Threat Perceptions across Vietnamese Smallholder Farmers in Australia. *Crop Protection,* 117(3), 147–155. Online: https://doi.org/10.1016/j.cropro.2018.11.022

Gillman, Stephen (2015): Fighting Bioterrorism – Europe Works on Master Plan. *Horizon,* 23 July 2015. Online: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/fighting-bioterrorism-europe-works-master-plan

Green, Manfred S. – Le Duc, James – Cohen, Daniel – Franz, David R. (2019): Confronting the Threat of Bioterrorism: Realities, Challenges, and Defensive Strategies. *The Lancet Infectious Diseases,* 19(1), e2–e13.

Hawaii State Department of Health (2018): *Bioterrorism, Chemical, Radiological, and Nuclear Emergencies.* Online: https://health.hawaii.gov/docd/prevention/bioterrorism/

Hinrichs, Eric B. (2020): *Chinese Biowarfare and Cyberwarfare. Military Force Multipliers for the 21st Century.* Chicago: Independent Publishers.

Kenigsberg, Ben (2022): 'The Anthrax Attacks' Review: Strange Behavior and an Incriminating Flask. *The New York Times,* 8 September 2022. Online: www.nytimes.com/2022/09/08/movies/the-anthrax-attacks-review.html

Maynard, Richard M. – Tetley, Terry D. (2004): Bioterrorism: The Lung under Attack. *Thorax,* 59(3),188–189. Online: https://doi.org/10.1136/thx.2003.016659

Miranda, Tatiana (2022): The Anthrax Attacks – A Dramatic Documentary Analyzing the Government and Bioterrorism. *The Disappointment Media,* 7 September 2022. Online: www.disappointmentmedia.com

Morris, Anthony (2022): Bioterrorism and Betrayal Have Poland's Spies on a Knife Edge in 'Illegals'. *SBS News,* 15 September 2022. Online: www.sbs.com.au/guide/article/ 2022/09/15/bioterrorism-and-betrayal-have-polands-spies-knife-edge-illegals

NSW Government (2017): *Protect Your Property from Biosecurity Threats.* Department of Primary Industries. Online: www.dpi.nsw.gov.au/biosecurity/plant/reporting,-diagnostics-and-biosecurity-collections/emergency-plant-pest-reporting-and-what-happens-next/protect-from -biosecurity-threats

NSW Government (s. a.): *Identify the Risks.* Department of Primary Industries. Online: www.dpi.nsw.gov.au/biosecurity/your-role-in-biosecurity/primary-producers/identify-the-risks

Prakash, Nilima (2010): Bioterrorism: Challenges and Considerations. *Journal of Forensic Dental Sciences,* 2(2), 59–62. Online: https://doi.org/10.4103/0975-1475.81283

Project Syndicate (2022): Biosecurity Is National Security. *Project Syndicate,* 8 August 2022. Online: www.gavi.org/vaccineswork/biosecurity-national-security

Riedal, Stefan (2004): Biological Warfare and Bioterrorism: A Historical Review. *Baylor University Medical Center Proceedings,* 17(4), 400–406. Online: https://doi.org/10.1080/08998280.2004.11928002

Sawyer, Charlie (2022): The Anthrax Attacks: Inside the Bioterrorism Events that Tormented the US Shortly after 9/11. *Screenshot,* 9 September 2022. Online: https://screenshot-media.com/culture/entertainment/the-anthrax-attacks-9-11/

Sharples, Frances – Husbands, Jo – Mazza, Anne-Marie – Thevenon, Audrey – Hook-Barnard, India et al. (2015): *Potential Risks and Benefits of Gain-of-Function Research. Summary of a Workshop.* Washington, D.C.: National Research Council – Institute of Medicine of the National Academies. Online: https://doi.org/10. 17226 /21666

The College of Physicians of Philadelphia (s. a.): *Biological Weapons, Bioterrorism, and Vaccines.* Online: https://historyofvaccines.org/vaccines-101/ethical-issues-and-vaccines/biological-weapons-bioterrorism-and-vaccines

Tin, Derrick – Sabeti, Pardis – Ciottonea, Gregory R. (2022): Bioterrorism: An Analysis of Biological Agents Used in Terrorist Events. *American Journal of Emergency Medicine,* 54, 117–121. Online: https://doi.org/10.1016/j.ajem.2022.01.056

Urbigkit, Cat (2022): Pandemic Demonstrated Connections between Humans, Animals, and Environment. *Cowboy State Daily,* 20 September 2022. Online: https://cowboystatedaily.com/2022/09/20/cat-urbigkit-pandemic-demonstrated-connections-between-humans-animals-and-environment/

Walsh, Patrick F. (2018): *Intelligence, Biosecurity and Bioterrorism.* London: Palgrave Macmillan. Online: https://doi.org/10.1057/978-1-137-51700-5

Ionuț Alin Cîrdei – Lucian Ispas[1]

Friendly Force's Projection, Training and Engagement

Hybrid warfare is a different kind of warfare than the conventional one that militaries have become accustomed to and trained for over time. In order for the armies to be able to deal with this particular type of conflict, it is necessary, first of all, for them to understand the context in which it appears and manifests itself and to know its particularities, since no two hybrid conflicts are alike. Combating hybrid warfare requires a comprehensive approach that combines all the instruments of power as effectively as possible, and that actions take place in a coordinated manner in all confrontational environments, both physical and informational, cyber or virtual. Countering an adversary using hybrid tactics or strategies requires understanding that the adversary is using the environment and context to its advantage, and that the adversary is trying to exploit the other side's vulnerabilities and create new vulnerabilities, while simultaneously trying to reduce its own vulnerabilities and transform them to its advantage. The nature of hybrid warfare determines how to counter it. Fighting a hybrid adversary requires flexible and adaptable forces capable of operating in a complex, ambiguous, ever-changing environment characterised by a high degree of uncertainty, where situations cannot be catalogued in nuances of black and white, but different shades of grey must be distinguished, which can render a conventional force ineffective and overexposed. Fighting a hybrid adversary involves developing a new, unconventional way of thinking and putting yourself in the attacker's role to better understand their perspective. Fighting means not only the use of force but, above all, increasing the ability to identify the mode of action of hybrid attackers and increasing the resistance capacity, developing the resilience of people and systems, which can be done through intensive, realistic training, through complex and dynamic exercises.[2]

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] Violand 2015.

DOI: https://doi.org/10.36250/01236_08

Training of forces

In order for an armed force to be able to counter a hybrid threat, it is necessary to develop specific mechanisms for training the military, but also tools that allow it to identify the threat as early as possible, to understand it in order to determine its mechanism of manifestation, to identify its strengths and vulnerabilities and to act effectively to neutralise the threat with the least possible use of brute force and the least possible use of kinetic, destructive actions. The training of modern forces, capable of operating in varied and difficult operational contexts, in environments characterised by volatility, unpredictability, complexity and ambiguity, must focus on the formation of military structures and leaders capable of conducting full-spectrum operations, in a multinational, joint, intergovernmental and interagency architecture, to combine all the instruments of power available to achieve the objectives.[3] Training of soldiers, commanders, commands and units must be as intensive, realistic, standardised and performance-oriented as possible to enable forces to conduct full-spectrum military operations in diverse areas where adversaries will use both conventional and hybrid means of warfare. After the formation of basic individual and collective skills, the training needs to diversify to include the training of the skills necessary to identify, analyse and combat hybrid threats, of a military and non-military nature. Training in this direction must be generalised to all levels of military art and all military arms/services and include interagency cooperation in the higher phases of training. All structures must benefit from complex training, based on realistic and challenging scenarios to create a basis both at individual and especially at collective level to act in difficult environments, in hybrid contexts. This is all the more necessary today, when it is found that the evolution of a crisis can be galloping, and the transition from the state of normality to the state of conflict can be very fast, which leaves very little time for the preparation of forces. It is also noted that the operational pace is increasingly high, due to the use of modern technologies, and the preparation and adaptation of the forces to the increasingly changing situation is difficult to achieve.[4] The basis of the preparation of the forces that are going to participate in a potential hybrid conflict must be the knowledge and understanding of the threat, which generically can be represented by a combination of regular forces, non-regular

[3] Department of the Army 2008a.

[4] Congressional Research Service 1998.

forces, criminal groups acting jointly to obtain common advantages. It is highly likely that conventional armed forces will face in a future confrontation space an adversary that uses "conventional and irregular tactic, techniques and procedures, all manner of terrorist acts targeting not only military but also civilian populace, and to witness an increase use of crime as a weapon system, an emphasis placed on cyber war, and an exploitation of the media".[5] To prepare the forces to fight an adversary that uses unconventional tactics of a hybrid nature, it is necessary for them to train in conditions as close as possible to the reality of the operational environment, conditions that must be replicated in the training process. Replicating this environment and context during individual training or exercises is extremely difficult, but planners and commanders must make continuous efforts to adapt training scenarios and incorporate lessons learned from recent conflicts, especially those from Syria and Ukraine, in the process of training the forces. The reason behind this approach is that the more the military are exposed during the training phase to stimuli of a hybrid nature, the more they face complex situations, characterised by ambiguity, the more they are used to make decisions under conditions of uncertainty, in consequence the more easily they will be able to adapt to the real challenges of the hybrid battle space and fulfil their missions, integrate the most diverse effects to achieve the desired end state, including those effects that exceed the military dimension of the confrontation and which are the result of a comprehensive approach. In the process of preparing the forces to participate in military actions in the context of the existence of hybrid threats and, subsequently, during the participation in this type of operations, it must be taken into account that the adversary or potential adversary is very adaptable, it is a good observant and has a high capacity to learn and self improve. That is why it is recommended that in any activity, template-ism, the use of predetermined solutions for a specific set of problems, the use of patterns of thinking and action should be avoided, and creativity, initiative, unconventional thinking and innovation should be encouraged, in order not to allow the adversary to create patterns of the actions of our forces and to identify ways to combat them. The hybrid actor will always try to hit the opponent's weak points and exploit any weakness in their combat functions,[6] and to avoid this, a commander must ensure that his forces are able to identify these weak points and reduce their exposure, the key being

[5] Hoffman 2007: 17–35.
[6] Hoffman 2009.

preparation, anticipation and adaptation.[7] The preparation of forces to operate in a hybrid context is very important and has the ability to shape how future actions will be conducted. Detailed and thorough planning followed by thorough implementation of the plan can create favourable conditions for military action. Starting from Napoleon Bonaparte's thoughts on the importance of preparing for future actions "if I always appear prepared, it is because before entering an undertaking, I have meditated long and have foreseen what might occur. It is not genius which reveals to me suddenly and secretly what I should do in circumstances unexpected by others; it is thought and preparation",[8] we can extrapolate about the importance of training the forces, the importance of planning their deployment in a new and challenging theatre of operations, and the need to establish clear rules regarding the engagement of forces in military actions to avoid their premature attrition and failure to accomplish their missions and strategic objectives of the operation. The irregular conflict, which favours the use of hybrid tactics, will complicate the way of conducting operations for forces that predominantly use conventional strategies and tactics and will condition the preparation and engagement of forces in operations, requiring the emergence of a new way of thinking and acting, which favours the initiative, independent action, creativity, flexibility and critical thinking at the expense of classic characteristics such as conformity, obedience, etc. The new generations of soldiers, both those at the base level and those at different decision levels, will adapt more easily to these new conditions because their education and way of being allows them to ask themselves more questions, to question decisions and doubt much more easily than in the case of the old generations, and they are also more receptive to the use of new technologies and the implementation of innovations, which allows them to adapt to the hybrid confrontation environment. All this happens because they have greater mental agility and greater tolerance for ambiguity, which allows them to adapt more easily in the face of the unknown and unpredictable. Consequently, in addition to decision-making competencies and tactical leadership skills, the military organisation must focus on creating a conducive training environment that prepares warfighters to face various situations specific to the hybrid combat environment and develop their capacity for resistance, shock absorption and adaptation so as to preserve as

[7] Murray 2009.
[8] Jeffrey 2020.

much as possible their freedom of action and fighting capacity. To succeed in this endeavour, we must not only change our way of thinking and relate to new situations, but we must develop our ability to adapt both at the individual and institutional level.[9] In the training phase of individuals, commands and forces, emphasis must be placed on the development of personal and collective skills and competences, on the knowledge and efficient use of new military and civilian technologies, but above all on the development of resilience, which allows them to recover back to normal in the shortest possible time after facing unexpected and unconventional threats. Building resilience is necessary because no training system can adequately replicate the complex reality and anticipate the characteristics of the hybrid combat environment, bearing in mind that each environment is unique and hybrid tactics are in constant evolution. In order to survive the challenges of the hybrid combat environment, it is imperative to develop resilience as it enables the military to survive in complex, hybrid threat environments and complete their missions with minimal exposure to potentially lethal risks.[10] Training is carried out mainly in base units or in joint training centres, individually, by units, joint and even interagency, using dynamic inputs to challenge the entire force to the maximum and open the way to unconventional approaches to various classic or hybrids threats. Training may continue after forces are deployed to the area of operations, particularly if immediate engagement in military operations is not anticipated, with forces having the advantage of training in the same environment and under the same conditions in which they will conduct future missions rather than in the artificially replicated environment from their peace location. In the situation where during the participation in the missions certain deficiencies in the training of the forces, in the synchronisation of the actions are found or new challenges arise that prevent the effective application of the elements of combat power, especially in relation to hybrid threats, the training of the forces can continue for the entire duration of the operations, for the improvement of techniques, tactics and procedures of action or for the identification of new techniques, tactics and procedures, suitable for the newly identified situations, provided that the additional training does not interfere and does not affect the combat capability and the degree of operationalisation and the force response ability. In order for individuals and military

[9] Daskalov 2018.
[10] Nindl et al. 2018.

structures to be able to adapt to the specifics of the hybrid confrontation environment, it is necessary for the military, and especially the leaders, to prepare themselves in the physical, intellectual and moral domains,[11] realistically, under conditions as harsh as possible and close to the requirements of the modern and real battlefield. By training in different scenarios, officers can learn how to be flexible and make difficult decisions. Leaders need education and strong intellectual training to meet the challenges of war, of changes and different cultures in the world.[12] Hybrid warfare is not only a confrontation of brute force, a clash of men and weaponry, but also a philosophy of warfare, in which not the strongest wins, but the most patient, the most adaptable, the most resilient and the most innovative. The hybrid combat environment raises many challenges that cannot be fully forecasted, but the soldiers who will be exposed to this environment must be prepared from all points of view. Therefore, they must benefit from a solid education[13] and a specialised training that will develop their cognitive, cultural, communication and action skills, that will allow them to adapt to the ever-changing environment, to understand the cultural peculiarities of the population and potential adversaries, to approach missions in a comprehensive way, which strictly goes beyond the military approach. They must be able to act in conditions of uncertainty, in a continuous change, in the conditions of an information vacuum and of intense manipulation, carried out both in the physical and in the virtual environment, to adapt quickly to the new conditions and to use the new technologies to facilitate mission accomplishment. All these attributes can be developed through a comprehensive training process aimed at not only the accumulation of knowledge and skills as a fighter, but also the development of critical and unconventional thinking and the development of skills that allow them to act and survive in a hybrid, discontinuous and multidimensional environment.[14] No matter how complex the training system and no matter how much time is allocated to training, militaries and commands cannot be fully prepared to face the threats from a hybrid confrontation environment.

[11] Thomas 2004.
[12] Thong 2019.
[13] Anton 2016.
[14] Anton 2016.

Projection of forces

Projecting forces to participate in a military operation is not just about moving them from their peacetime location to where they will perform a combat mission. Force design means more than that, it means activating forces, training them, transporting them, participating in conflict, etc. Combat power projection can be defined as "the ability of a nation to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability".[15] According to the U.S. doctrine of employment of forces in operations, force projection comprises eight stages,[16] starting and ending on the national territory. Thus, the complex process of force projection begins with their mobilisation and continues with the following stages: pre-deployment activities, force deployment, insertion operations in the theatre of operations, main operations, ending the conflict and conducting post-conflict operations, redeployment of forces and their demobilisation. Each stage is of great importance to the success of the whole operation, requiring the necessary support to be given to the forces participating in this projection process. In the context of participating in a hybrid conflict, the forces will have to carry out this projection process taking into account the particularities of the new area of operations and the hybrid tactics used by the adversary, who may target the forces from the very first phases in which they aim to activate and increase combat capacity by intensifying training in a hybrid scenario and influencing, shaping the internal and external environment in order to support the intervention and make the actions of the armed forces more efficient. The mobilisation of forces to participate in a military operation consists of a series of activities aimed at bringing the forces to a level of operationalisation that will enable them to meet future challenges. Mobilisation can mean activating some units, filling them with personnel, intensifying training to deal with a hybrid operating environment, but primarily preparing personnel, commands, equipment for future operations. The activities that precede the deployment of the forces are very important and aim to perfect the preparation of the forces taking into account the specifics of the future operation, but also to increase the cohesion of the military and structures and to test techniques, tactics and action procedures specific to participating in a hybrid conflict and combating hybrid threats.

[15] U.S. Marine Corps 2011: 2–21.
[16] Department of the Army 1994.

The pace and intensity of the actions carried out in the preparation phase of the deployment of the forces are influenced by the level of training of the forces, the security situation and the objectives set for the forces in question. After the completion of the preparations and the realisation of the stocks of materials, fuel, equipment, weapons and ammunition, but also after the identification of the forces and means that will facilitate the projection of the forces, we will proceed to the deployment phase, the projection of the forces in the area of operations, most often outside the national territory. The actual deployment of forces is conditioned by the existence of land, air or naval transport capabilities and the analysis of operational factors, such as the mission, the enemy, the terrain, the time available, etc.[17] At NATO level this process of deployment of forces in an area of operations is known by the acronym of RSOM-I[18] standing for reception, staging, onward movement and integration, which captures the essence of this process. Thus, the armed forces, after being trained, evaluated, after being equipped with all the necessary means to successfully carry out the future mission, even in the context of an operations area where there is a risk of using hybrid tactics, used both in the physical, as well as in the cyberspace are moved to the future area of operations where they will find a permissive environment that allows them to easily insert, or a hostile environment, which involves the conduct of forcible entry operations. Forces to be inserted into a hostile environment and immediately engaged in combat must be transported with intact combat capability and must receive intensive support from all supporting forces and services. If the insertion area is already under the control of the own forces or the threat level is low, the forces will be moved without aiming to maintain the combat capacity, most of the time separating the personnel from the equipment, weapons and ammunition, to increase the speed of deployment and to reduce the risks of accidents. In this case it is necessary to go through the stage of reception, i.e. receiving forces and equipment, storing them and keeping them safe from threats until the forces are sufficiently numerous and meet the conditions to be engaged in operations. After the reception of the forces and equipment, the phase of staging follows, when the units are formed, when the equipment is checked and the personnel are integrated into the units according to the order of battle, and the headquarters are prepared to lead and coordinate the forces. From this moment on the forces will execute the movement to the area of

[17] Department of the Army 2022.
[18] Ministry of Defence 2021.

responsibility, where they will carry out combat actions, having the full combat capability and being able to react to any threat, of a conventional or hybrid nature, using all elements of the specific combat power. Once in the area of operations, the forces will integrate with forces already present there, host nation forces, or other elements with whom they will have to cooperate in the future. In the integration phase, the forces will have the opportunity to familiarise themselves with the characteristics of the area, with the existing threats, but also to identify the optimal options that allow them to combat these hybrid threats.[19] The most intense phase of force projection in an area of operations where conventional actions are conducted in parallel with hybrid actions, where threats do not come only from armed groups and do not only target the armed forces, but come from paramilitary groups, groups of organised crime, partisan organisations, etc., and which not only conduct kinetic actions against the armed forces, but plan and conduct actions aimed at reducing morale and the will to fight, creating and maintaining a climate of insecurity, sowing doubt about the effectiveness and legality and legitimacy of actions, reducing operational efficiency through actions carried out online and offline, in the physical and virtual space, etc. is represented by the phase of operations conduct. Having all the resources at his disposal, having the possibility of knowing the real operational situation and timely identifying conventional and hybrid threats, the commander will focus his attention on obtaining decisive effects that will contribute to the achievement of the objectives and the creation of the conditions for the successful conclusion of the operation. In this phase the commander must take the most appropriate measures to ensure the protection of the forces and to ensure military actions and to decisively engage the adversary and to gain and maintain the initiative at all levels.[20] The key to success in any type of military operation, but even more so in one where there is a risk of facing an adversary using hybrid tactics, is to successfully mobilise, focus, project, deploy and engage forces before the adversary can be ready for this by maintaining the initiative, thus avoiding time pressure and the obligation to react to the opponent's actions. Projecting forces in a theatre of operations is a very complex, resource-intensive action that involves a concentrated effort from several services and categories of forces, being a joint operation by definition. The success of force projection depends on the ability to use all available resources to control the battlespace, occupy and control key

[19] Ministry of Defence 2018.
[20] Department of the Army 2019.

insertion points and facilities, and sustain military operations in a hostile operating area where hybrid threats can take different forms and may act in unexpected ways against conventional armed forces. In order for the projection operations to be carried out successfully, it is necessary that the physical confrontation space be under the full control of the own forces in order to reduce the risks to the forces, especially in the moments when they are most vulnerable: during transport, disembarkation, the establishment of the devices and the initiation of the movement. Efforts will be focused on controlling the airspace and securing a bridgehead large enough to allow the initial concentration of forces, the establishment of initial combat formation, but also the accumulation of consistent logistical support to provide the necessary support for operations. Maintaining a ring of security can be done by initially deploying forces capable of identifying and eliminating the direct enemy threat with kinetic attacks and creating a multidimensional protective bubble for own forces. However, it will be very difficult to eliminate all threats, especially those of a hybrid nature that manifest in the physical or cyber environment. Protecting forces from these non-conventional threats requires them to be prepared in advance to recognise a hybrid threat and identify optimal countermeasures, which can range from ignoring to observing, deterring, engaging and neutralising.[21] Armed forces involved in projection operations must be prepared for opposed or unopposed entry operations. Projecting forces in a hostile environment with a strong hybrid component implies a force with sufficient full-spectrum immediate adversary engagement capabilities and advanced force protection capabilities that must be ready for combat from the moment of insertion. Projecting forces in a permissive environment allows them to continue to build and strengthen their combat capability against conventional and hybrid threats and after insertion into the area of operations, allows them to train, acclimatise and acculturate to the place. When considering force projection one must consider the combat power requirement that must be present in the area of operations, the type of capabilities needed to accomplish the objectives, and how to use those capabilities to make the force sufficiently credible, lethal and able to operate in the specific conditions of hybrid warfare. Commanders must be prepared to deploy in the field sufficient forces, characterised by a high level of combat power, to resolve the crisis situation or conflict under the conditions established by them, in the shortest possible time and with the least possible losses. Projected force composition must be established

[21] Cîrdei 2016.

in advance of their deployment to allow for the early accumulation of forces, assets, capabilities and skills and to enable force training and integration. The field-deployed force package must be strong enough to meet threats and accomplish objectives without oversizing the force package, which entails additional exposure.[22] The implementation of new technologies has the potential to increase the range and resilience of deployed forces, and the refinement of long-range strike systems, the multiplication of sensor networks, emerging and disruptive technologies that are becoming more accessible, the generalisation of multidimensional approaches, with an emphasis on the increasing cyber dimension; the use of hybrid techniques and technologies will favour the defender who will be able to strike the attacking forces at any point, at any distance,[23] generalising the risk and forcing the forces to adopt complex and expensive protective measures and will increase the state of tension and anxiety at the level of the forces. The use of unmanned and autonomous air and ground vehicles, as well as other weapon systems that combine human and artificial intelligence, increases the hybrid character of the confrontation and changes the way in which forces can be projected and engaged in combat and gives rise to new options for design and employment of forces.[24]

Engagement of forces

The hybrid threat is a combination of regular, irregular forces and means, criminal groups operating in the physical or virtual environment, which join forces to achieve favourable effects, and their basic characteristics are the ability to innovate, adaptability, the ability to network, using a mix of old and new technologies to create dilemmas and challenges for opponents,[25] both physical, cognitive and moral, through actions carried out by a network of people, capabilities and systems, which combine in actions carried out across the entire spectrum of operations and in all dimensions of the operational environment, affecting or influencing all operational variables.[26] Knowing that

[22] Joint Chiefs of Staff 2017.
[23] Smith–Palazzo 2016.
[24] Commonwealth of Australia 2016.
[25] Department of the Army 2010b.
[26] Department of the Army 2010a.

the adversary operating in the hybrid environment will try to gain the advantage using decision and action speed, agility and versatility, the major challenge will be to reduce his ability to use the aforementioned advantages. Conventional forces will do their best to win the war in the shortest possible time, with the least human and material costs, and in doing so will plan and execute decisive actions directed against the adversary's centres of gravity. When facing a hybrid type opponent this is no longer possible due to his characteristics, the way of organising and conducting the fight. The objective of the hybrid adversary is not necessarily to win the battle, but rather to prevent conventional armed forces from regaining victory and maintaining a narrative that they have lost or will lose the conflict, while waiting for them to make mistakes and wear out their fighting capacity and the support of the national and local population, as happened during the war between Israel and the Hezbollah group in Lebanon in 2006. More often than not, time is on the side of the warfighter who uses hybrid tactics to compensate for certain deficiencies and correct certain asymmetries, which allows him to establish a convenient operational rhythm and thus affect the ability of forces to engage and to support a military action in the hybrid environment. Once inserted into the area of operations, conventional forces will most likely be under constant pressure in both the physical and virtual environment, with the hybrid adversary having the freedom to choose both the place and time of the confrontation, its scale and the means used to create and maintain a state of tension, of uncertainty among conventional forces, to reduce their fighting capacity and damage their image and credibility. For conventional forces to be able to accomplish their mission, they must act across the entire spectrum and target both adversary combatants and public opinion in home countries, in the host country, while taking all measures to protect critical civilian and military infrastructure, to achieve force protection and to maintain its combat capability at the highest possible level for as long as possible. The participation of forces in a hybrid conflict implies the application of new rules, new concepts and strategies. In a classic conflict, most strategies focus on engaging and destroying the adversary, be it an insurgent group, a terrorist organisation, or a state, so that it no longer poses a threat and can no longer carry out attacks against its own forces and affect its own interests and objectives. When acting in a hybrid context, using the military tool to achieve objectives is no longer sufficient. A new approach is needed, setting objectives that go beyond the military dimension and identifying a complex, comprehensive strategy that goes beyond the military sphere and that also involves other institutions or organisations. In hybrid

conflict, a holistic interinstitutional approach is needed to lead to the elimination "of the military, logistical and ideological support of the groups within the hybrid conflict",[27] by integrating the effects of other instruments of civil power, such as political, diplomatic, economic, informational and by involving other national or international actors. Depending on the type and intensity of the conflict, the armed forces may have the primary role in countering hybrid threats, the leading role or a secondary, supporting role.[28] Given the complexity of the threat, it is necessary to employ a comprehensive approach that combines political, socio-economic, information and military tools to identify, mitigate, counter, and failing all else, recover from the effects of hybrid warfare.[29] The comprehensive approach to military operations carried out in a hybrid context involves the sharing of efforts, the coordination of actions, the most efficient use of resources, the effective exercise of command and control of all available forces, regardless of the field of action and the institution/agency to which they belong, the integration of effects to achieve common final goals, etc. NATO's strategy for countering hybrid threats[30] and which also has implications for how forces prepare and operate in a potentially hybrid environment is based on a comprehensive approach that considers multiple steps on the scale of military escalation, such as building partnerships and developing knowledge, deterring hybrid actions against NATO states, engaging the threat and stabilising. Depending on the stage in which the NATO forces are, in relation to the evolution of the crisis, the focus must be either on actions carried out in the non-military fields, or on actions carried out in the military field, whether they are kinetic or non-kinetic. In the partnership development phase, the emphasis is on the intensive use of political, diplomatic and economic instruments, in the knowledge development phase, attention is focused on specific intelligence activities, which prepare future actions. In the deterrence stage of hybrid actions, emphasis can be placed on carrying out demonstrations of force in the military field, organising exercises, activating the forces and increasing their level of training, but also on intensifying political and diplomatic actions or even on putting pressure in the economic or financial field to deter the threat. Threat engagement is the most intense and dynamic phase, in which the necessary resources are allocated for the operation

[27] Ioniță et al. 2017: 40–41.
[28] Monaghan 2019: 91.
[29] Kremidas-Courtney 2020.
[30] NATO 2010.

and forces are projected into the theatre of operations and engaged in combat actions, based on the mandate received, the specific rules of engagement, so as to fulfil their mission, by engaging and neutralising the hybrid threat, with the adapted means, aiming more at achieving the desired effects than the physical destruction of the adversary. The reconstruction phase focuses on rebuilding the infrastructure and institutions of the host state and creating the right security climate for the transfer of authority.[31] The hybrid adversary can act to force conventional forces to disperse their resources, forces, combat assets and attention, limit their freedom of action and initiative, etc. and to create and maintain economic instability, to amplify the lack of trust in defaulters, to attack information networks, to cause humanitarian crises, etc. The armed forces must have an organisation and equipment, but also a command and control system that allows them to be as supple as possible, more agile in training and employment, to have a proactive posture, which can be achieved in peacetime by carrying out complex, realistic exercises that take soldiers and commanders out of their comfort zone and expose them to the greatest possible challenges and force them to have a comprehensive approach, to recognise the need to understand the operating environment and cooperate with other agencies, institutions and organisations to achieve the objectives.[32] The further the operations are conducted from the country of origin, the greater is the effort of the country sending the forces and the longer is the time required to provide support and the duration of their support in the operations. Also the extended distance and duration of operations "tends to tire soldiers out and weaken their morale as a result of exhaustion. In addition, the further the forces are from the home country, the longer the logistics line becomes; defense capabilities will thus become depleted as a result of the need for security."[33] The effort of the attacking or expeditionary country is all the greater as the resource consumption of a highly mechanised and technological force is greater these days, requiring impressive amounts of fuel, spare parts and other equipment to fuel the machinery of war and to provide soldiers with the necessary means of combat, survival and morale. The impact of distance can be reduced in hybrid cyber conflicts because distance is no longer an essential factor in this equation, and "information technology has demolished

[31] Department of the Army 2008b.
[32] Joint Chiefs of Staff 2016.
[33] Sakaguchi 2011: 83.

time and distance"[34] and "changing technology has reduced the value of propinquity".[35] The problem that arises is represented by the fact that a state actor in conflict with another state actor cannot limit himself only to the hybrid tactics of distance warfare, using the cyber environment, and cannot achieve victory in this way, being obliged to project, employ and sustain conventional forces to enable it to achieve its military and political objectives and to put continuous pressure on the adversary. In carrying out military actions, an important aspect that must be developed from the preparation phase is maintaining situational awareness in a hybrid environment, where the emphasis must be placed on monitoring "known unknowns" and discovering "unknown unknowns",[36] to reduce operational fog and be able to anticipate the evolution of events and find the right answers to complex questions regarding the opponent's mode of action and his objectives.[37] The evolution of society in all areas, the rapid integration of modern and emerging technologies into military actions have given rise to new threats and allowed old ones to manifest in new and unpredictable ways, which puts the armed forces in a great difficulty. Starting from these ideas, we can say that conventional conflicts between states will be replaced by new hybrid conflicts, which will require conventional forces to quickly adapt and force them to find new ways of dealing with both old and new problems and challenges, "this requiring a rapid change in existing warfare tactics and techniques so that security and military organizations can respond in a timely manner to the challenges of the modern security environment".[38] The engagement of forces in operations implies not only the preparation of forces to act and fulfil their missions in a hybrid, unpredictable and multidimensional environment, but also the development of new capabilities, which will improve the abilities of forces to obtain information, to analyse it, to identify and engage the threat, etc., as well as developing analysis algorithms that involve developing creative and unconventional thinking at all levels to understand and counter hybrid threats. As with countering hybrid threats, there is also likely to be a trade-off assuming limited resources between capabilities to counter hybrid warfare and those to

[34] Wriston 1997: 172.
[35] Bandow 2004.
[36] Monaghan et al. 2019: 64–65.
[37] Neag 2018.
[38] Vuković et al. 2013: 136.

counter leading conventional combat adversaries.[39] Combating hybrid adversaries or those using hybrid tactics must be done on multiple levels, as victory on the battlefield is not sufficient to eliminate the source of the hybrid threat. The engagement of forces in counter-hybrid threat operations can make a decisive contribution to shaping the environment and the area, facilitating the end of the conflict, but victory can only be achieved through the adoption of coordinated, multi-pronged measures based on a plan focused on the comprehensive and multi-dimensional approach.[40]

Conclusion

The complexity of hybrid warfare, and the fact that adversaries are everywhere and can take any form, can lead us to think that preparing forces to combat hybrid threats is an impossible task, involving training warfighters and commanders to fight anyone, anytime, with an omnipresent and invisible opponent at the same time, who can take different forms and act in extremely diverse ways. However, hybrid threats can be fought and even defeated, but for this the fighters, especially the commanders and planners of military actions, must fully understand the confrontation environment, their own forces, but also the nature of the threats they face. Only by understanding the adversary or potential adversary is it possible for it to be defeated, and for one's own forces to take the initiative, to act proactively, not just to react to the adversary's movements and try to limit the effects of his actions. The solution is to prepare leaders to understand that potential enemies may use different and innovative strategies, but that they are not infinite, and therefore can be anticipated, learned and countered. The current security environment is very complex, unpredictable and changing, and conflicts can no longer be classically defined, no longer have clearly defined three phases of evolution and are no longer fought only by military means, by identifiable adversaries.[41] There are many actions that can endanger the security of a state and which are far below the limit of a military attack, such as cyberattacks, campaigns carried out on social media, buying influence and creating currents of opinion, using Trojan horses among local politicians, supporting organised crime, etc.,

[39] Monaghan 2019.
[40] Elonheimo 2021.
[41] Rühle–Roberts 2021.

which can destabilise a state without the need for military intervention. These threats being undetectable and hard to attribute to a hostile state are impossible to fight by classical means. Armed forces can intervene only when a serious violation of international rules is found and when security and territorial integrity are threatened by an adversary that has moved to the next stage: the combined use of hybrid strategies and armed force to achieve objectives which cannot be accomplished without the use of military power. In this case, the armed forces will have to act to limit the effects of these actions but to be able to do this they must be properly prepared to face an unconventional adversary, who is everywhere and nowhere and who uses all the means at their disposal, trying to avoid the rules of armed conflict and trying to stay as much as possible in the gray area, where they can hide, take refuge and strike by surprise. This training must be carried out both in the action field, by intensifying complex exercises, based on realistic, adaptable and challenging scenarios, but also in the cognitive and intellectual field. In addition to specialised training, it is necessary that especially leaders, but also fighters, develop their critical thinking and broaden their horizons in order to better understand the particularities of other cultures, other societies, to be able to understand, know and even model the confrontational environment and to maintain situational awareness at the highest possible level, in parallel with the development and strengthening of individual and organisational resilience. Hybrid threats are increasingly diverse and manifest in all areas, with direct and indirect implications for the safety and security of individuals and states. Actors who use hybrid warfare-specific tactics aim to achieve their goals as quickly as possible, with the lowest possible human and material costs, and want to surprise the adversary in all areas and environments and exploit their vulnerabilities. Countering hybrid threats is done by various methods, in all areas of interest, but it is very possible that the use of armed force in this regard will also be necessary. Modern armies are prepared to deal with conventional adversaries and successfully conduct combat or stability and support operations, but are not so well prepared to act in an unconventional, hybrid conflict. In order to deal with opponents who use hybrid tactics on a large scale, it is necessary to change the way we think, to adapt our training and even to modify and adapt the rules of employment, in order to fight threats as effectively as possible, while respecting national and international law on the use of force. In hybrid warfare, the armed forces often have to adapt, anticipate and act unconventionally and this requires additional training, clear rules for insertion into the area of operation and concerning the mode of action.

Questions

1. Why is there a need for a special training of the forces in order for them to be able to deal with the hybrid confrontation environment?
2. Which are the essential elements to be taken in consideration when training a force to operate in the context of the existence of hybrid threats?
3. Which are the main steps in the force projection process?
4. Which are the key aspects of engaging forces in an environment with a hybrid operational component?
5. What does the comprehensive approach during the engagement in a hybrid threat environment consist of?

References

Anton, Mihail (2016): Hybrid Pedagogies for Hybrid War. *Scientific Research and Education in the Air Force, AFASES,* 18(2), 509–516. Online: https://doi.org/10.19062/2247-3173.2016.18.2.3

Bandow, Doug (2004): *Quick and Full Disengagement.* Online: www.cato.org/commentary/quick-full-disengagement

Cîrdei, Alin I. (2016): Countering the Hybrid Threats. *Revista Academiei Forţelor Terestre "Nicolae Bălcescu",* 21(2), 113–119.

Commonwealth of Australia (2016): *Future Operating Environment 2035.* Online: https://cove.army.gov.au/sites/default/files/08-09_0/08/Future-Operating-Environment-2035.pdf

Congressional Research Service (1998): *Military Readiness, Operations Tempo (OPTEMPO) and Personnel Tempo (PERSTEMPO): Are U.S. Forces Doing Too Much?* CRS Report for Congress. Online: www.everycrsreport.com/files/19980114_98-41_f1911e3025585281e1c684e4d4d7aa9cefc20cb9.pdf

Daskalov, Krassen (2018): Hybrid Warfare and the Challenge It Poses to Psychological Resilience Training in the Bulgarian Military. *Information & Security: An International Journal,* 39(3), 197–205. Online: https://doi.org/10.11610/isij.3917

Department of the Army (1994): *Intelligence and Electronic Warfare Operations. FM 34-1.* Online: https://irp.fas.org/doddir/army/fm34-1/ch3.htm

Department of the Army (2008a): *Training for Full Spectrum Operations. FM 7-0.* Online: www.hsdl.org/?view&did=233070

Department of the Army (2008b): *Stability Operations. FM 3-07.* Online: https://irp.fas.org/doddir/army/fm3-07.pdf

Department of the Army (2010a): *The Operations Process. FM 5-0.* Online: https://irp.fas.org/doddir/army/fm5-0.pdf

Department of the Army (2010b): *Hybrid Threat. TC 7-100.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100.pdf

Department of the Army (2019): *Operations. ADP 3-0.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf

Department of the Army (2022): *Operations. FM 3-0.* Online: https://irp.fas.org/doddir/army/fm3-0.pdf

Elonheimo, Tuukka (2021): Comprehensive Security Approach in Response to Russian Hybrid Warfare. *Strategic Studies Quarterly,* 15(3), 113–137.

Hoffman, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies. Online: www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hoffman, Frank G. (2009): Hybrid Threats: Reconceptualizing the Evolving Character of Conflict. *Strategic Forum,* 240, 1–8. Online: https://apps.dtic.mil/dtic/tr/fulltext/u2/a496471.pdf

Ioniţă, Dorin – Pînzariu, Sorin – Bârsan, Ghiţă – Raţiu, Aurelian – Moşteanu, Dan (2017): Interinstitutional Dimension Concerning Planning, Training and Force Engagement as Response to the Hybrid War. *Scientific Journal of the Military University of Land Forces,* 186(4), 38–48. Online: https://doi.org/10.5604/01.3001.0010.7217

Jeffrey, Steve (2020): *Questions to Plan & Make Decisions in a Crisis.* Online: www.stevejeffrey.co/7-questions-to-plan-make-decisions-in-a-crisis/

Joint Chiefs of Staff (2016): *Interorganizational Cooperation. JP 3-08.* Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08.pdf?ver=CqudGqyJFga9GaACVxgaDQ%3D%3D

Joint Chiefs of Staff (2017): *Joint Forcible Entry Operations. JP 3-18.* Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1.pdf?ver=A9WjEOdmKtKqabuKPDGu_g%3D%3D

Kremidas-Courtney, Chris (2020): *Building a Comprehensive Approach to Countering Hybrid Threats in the Black Sea and Mediterranean Regions.* Online: https://nmiotc.nato.int/wp-content/uploads/2020/02/Building-a-Comprehensive-Approach-to-Countering-Hybrid-Threats-in-the-Black-Sea-and-Mediterranean-Regions-by-Chris-Kremidas-Courtney.pdf

Ministry of Defence (2018): *Allied Joint Doctrine for the Joint Logistic Support Group. AJP-4.6.* Edition C, Version 1. December 2018. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778361/doctrine_nato_joint_logistic_support_group_ajp_4_6.pdf

Ministry of Defence (2021): *Allied Joint Doctrine for the Deployment and Redeployment of Forces. AJP-3.13.* Edition A, Version 1. May 2021. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085161/Allied_Joint_Doctrine_for_Deployment_and_Redeployment.pdf

Monaghan, Sean (2019): Countering Hybrid Warfare. So What for the Future Joint Force? *Prism,* 8(2), 82–98.

Monaghan, Sean – Cullen, Patrick – Wegge, Njord (2019): *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare.* A Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Murray, Williamson (2009): Military Adaptation in War. *Institute for Defense Analyses.* Online: https://apps.dtic.mil/sti/pdfs/ADA509781.pdf

NATO (2010): *BI SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.* Online: www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

Neag, Mihail M. (2018): Design of Military Actions in the Operational Environment Hybrid Type. *International Conference Knowledge-Based Organization,* 24(1), 157–162. Online: https://doi.org/10.1515/kbo-2018-0023

Nindl, Bradley C. – Billing, Daniel C. – Drain, Jace R. – Beckner, Meaghan E. – Greeves, Julie – Groeller, Herbert – Teien, Hilde K. – Marcora, Samuele – Moffitt, Anthony – Reilly, Tara – Taylor, Nigel A. S. –Young, Andrew J. – Friedl, Karl E. (2018): Perspectives on Resilience for Military Readiness and Preparedness: Report of an International Military Physiology Roundtable. *Journal of Science and Medicine in Sport,* 21(11), 1116–1124. Online: https://doi.org/10.1016/j.jsams. 2018.05.005

Rühle, Michael – Roberts, Clare (2021): *Enlarging NATO's Toolbox to Counter Hybrid Threats.* Online: www.nato.int/docu/review/articles/ 2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

Sakaguchi, Daisaku (2011): Distance and Military Operations: Theoretical Background toward Strengthening the Defense of Offshore Islands. *NIDS Journal of Defense and Security,* (12), 83–105. Online: www.nids.mod.go.jp/english/publication/kiyo/pdf/2011/bulletin_e2011_5.pdf

Smith, Chris – Palazzo, Al (2016): Coming to Terms with the Modern Way of War: Precision Missiles and the Land Component of Australia's Joint Force. *Australian Land Warfare Concept Series,* 1. Online: https://researchcentre.army.gov.au/sites/default/files/160819_-_concept_-_lw_-_australian_land_warfare_concept_series_1_-_unclas_0.pdf

Thomas, Joseph J. (2006): *Leadership for the Long War: Developing 21st Century Warriors.* The ADM James B. Stockdale Center for Ethical Leadership, United States Naval Academy. Online: www.usna.edu/Ethics/_files/documents/Leadership%20in%20the%20Long%20War%20Thomas.pdf

Thong, Calvin S. S. (2019): Combating the Modern War. *Pointer, Journal of the Singapore Armed Forces,* 44(1), 21–32.

U.S. Marine Corps (2011): *Marine Corps Operations. MCDP 1-0.* Online: www.trng-cmd.marines.mil/Portals/207/Docs/TBS/MCDP%201-0%20Marine%20Corps%20Operations.pdf

Violand, David E. (2015): Setting the Training Conditions to Win in a Complex World. *Small Wars Journal,* 22 September 2015. Online: https://smallwarsjournal.com/jrnl/art/ setting-the-training-conditions-to-win-in-a-complex-world

Vuković, Josipa – Matika, Dario – Barić, Slavko (2016): Hybrid Warfare Challenges. *Security and Defence Quarterly,* 12(3), 118–138. Online: https://doi.org/10.35467/sdq/103239

Wriston, Walter B. (1997): Bits, Bytes, and Diplomacy. *Foreign Affairs,* 76(5), 172–182.

Paul Tudorache – Ghiță Bârsan[1]

Designing Adversary Hybrid COAs

Different state and non-state actors use a wide range of strategies to take advantage of the opportunities ensured by hybrid warfare (HW). Regardless of the nature of escalation (vertical, horizontal), the adversary correlates instruments of power from the military, political, economic, civilian and information spheres, in a way that generates a non-linear direction, creating an ambiguous pattern, which is quite difficult to decipher and counter. Consequently, this non-linearity of hybrid aggression/attack (HA) requires an exhaustive analysis to be discerned. Starting from the idea that hybrid threats (HT) represent "force multipliers and/or a coercion tactic used to support a policy or strategy that is not delivering the desired results"[2] this chapter seeks to analyse the most representative conceptual models for understanding the framework of HT, as well as to determine a common denominator of the adversary's strategies, operations and tactics. These will be used to substantiate the design of the adversary's courses of action (COA) in the framework of HW. Furthermore, due to the fact that the most acute lethal effects of HA are felt at the lowest level of operations, a comprehensive approach to the various COAs that may be used by the adversary at tactical level of HW is required.

Conceptual models

The principle underlying the desired visualisation and understanding of the overall image of HT/HA requires, first of all, reporting to the representative conceptual models, which analysed and correlated accordingly, will provide the essential generic aspects, constituting a starting point in designing various COAs that may be used by the adversary in the HW framework. To eliminate any confusion from the beginning, it is appropriate to emphasise that the two concepts

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] Giannopoulos et al. 2021: 10.

DOI: https://doi.org/10.36250/01236_09

of HT and HW are used interchangeably. Even though HT is considered a hostile intent of a potential aggressor before his HA in the HW framework, both HT and HA are considered principle forms of offensive actions, and thus both can be considered inherent parts of the HW spectrum.[3] Also, other additional information that substantiates the usage of HW, no matter in what form (HT, HA), refers to the following key principles:

- Creating volatility, uncertainty, complexity and ambiguity (VUCA) – if the volatility consists in the high amplitude of the changes in a very short time, the uncertainty is given by the difficulty of predicting the hostile intentions of the hybrid adversary. Instead, the complexity arises from the diversity of domains and tools used to perform HT/HA, while the ambiguity manifests itself through the hidden and plausible negation, which creates real obstacles in understanding decision-making contexts.
- Generating asymmetry – is achieved by relating and leveraging various deceptive strategies and multi-domain instruments and capabilities against expanded target vulnerabilities. In this regard, the synchronisation of the HT/HA usage can be obtained by relating horizontal and vertical escalation of power instruments and tailored strategies.
- Having a multisource pattern – HT/HA can be used by "an actor or a network of actors willing to engage in hostile, usually covert activities […] may be controlled or influenced by a nation-state, proto-state, or a non-state actor such as large organizations, which often attempts to either circumvent or ignore international laws".[4]
- Achieving simultaneous or successive effects – they are multilevel guided, aiming at political, strategic, operational and tactical targets from all fields of societal security to degrade their normal functioning.
- Practising blended tactics – exemplifying at the tactical level, the adversary's operations are based on employing modular conventional military structures reinforced with guerrilla, paramilitary, insurgent or criminal elements.

[3] Monaghan et al. 2019.

[4] Balaban–Mielniczek 2018: 3711.

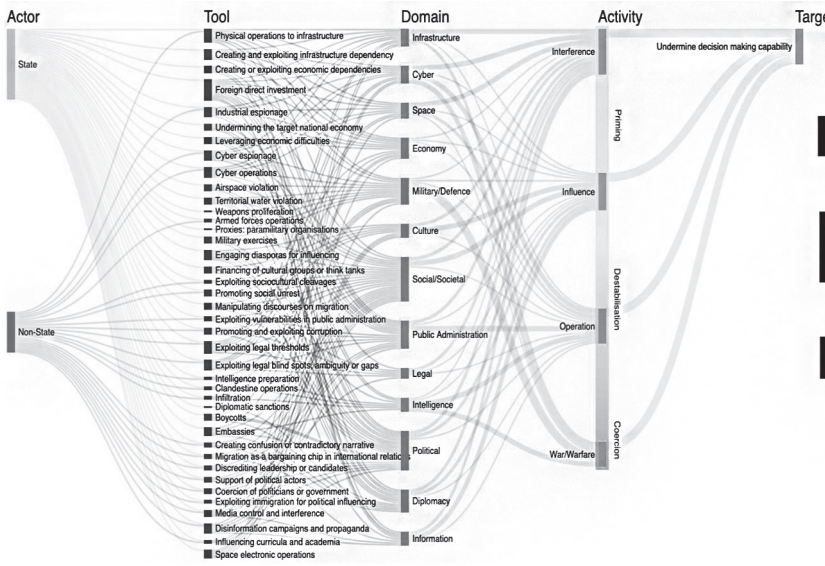

Figure 1: Conceptual model for HT/HA – EU JRC and Hybrid COE
Source: Giannopoulos et al. 2021: 13

A first conceptual model to which the authors refer and which portrays the principles mentioned above is the one developed by the mutual effort of the Center of Excellence (COE) for HW and the Joint Research Center (JRC).[5] As it can be seen in Figure 1, the conceptual model is based on five key elements such as actors, tools, domains, activities and targets. The principle of its operation is quite simple and is based on the progressive correlation of the constituent elements.

The comprehensive understanding of the conceptual model initially involves the proper analysis of each dedicated element. This consists in:

- Actors – can be of two types as state and non-state actors. State actors are considered different countries, which are also found with the name of 'nation-states' and are dominant in the hybrid spectrum. Also, state actors are divided in four main categories as "core states, transition states, rogue states, and failed or failing states".[6] Instead, non-state

[5] Giannopoulos et al. 2021.
[6] Department of the Army 2010: 2-1.

actors are represented by actors that "do not represent the [capabilities] of a particular nation-state […] include rogue actors as well as third-party actors".[7] Insurgents, mercenaries or guerrilla are some examples of rogue actors, while refugees, transnational corporations or news media falls in the category of third-party actors.

- Tools – are defined as "the ways in which an actor might bring about an effect".[8] The effects can propagate not only on one but on several domains, because they are strongly interrelated. For instance 'cyber operations' could impact military, infrastructure, space, public administration domains, while 'diplomatic sanctions' could influence economic, diplomatic or political domains.
- Domains – defines the vulnerabilities or opportunities against which the various tools and activities are directed for their targeting or exploitation; within the model shown in Figure 1, the domains are extremely diversified from infrastructure to diplomacy or information.
- Activities – are used to "harm, undermine or weaken the target"[9] and can manifest, according to the gradual escalation, in various forms such as interference, influence, operation or warfare. These activities are correlated with specific phases, consisting of priming, destabilisation and coercion. First phase, priming, also known as shaping or conditioning phase, can be acquired through interference and influence, destabilisation through operations, while coercion requires warfare strategies and tactics.[10]
- Targets – the objects of the tools and activities undertaken by the aggressor to generate desired effects, either lethal or nonlethal; as can be seen in Figure 2, they are extremely diversified, being correlated with various domains.

Relating to the elements above, the understanding of the conceptual model can be summarised as state or non-state actors, with certain defined objectives, but with a limited capacity of achieving them. They use various tools to engage multi-domain targets in order to create desired effects so that they are affected

[7] Department of the Army 2010: 2-1.
[8] Giannopoulos et al. 2021: 33.
[9] Giannopoulos et al. 2021: 36.
[10] Giannopoulos et al. 2021.

and shaped according to the desired end state. Furthermore, in relation to the aggressor's objectives, the tools will be used, escalating or de-escalating vertically and/or horizontally during priming, destabilisation and coercion phases of the HW. If in the priming phase, the aggressor uses the tools and activities to obtain certain advantages but also to test his own capabilities or to check the defender's readiness. In the stabilisation phase the goal is to achieve a deliberate objective, the use of tools and activities being much more visible and aggressive, thus challenging the limits of their acceptance or non-acceptance by the defender. Instead, in the last phase, coercion, the aggressor moves to the maximum escalation of aggression through the overt and covert use of the entire typology of strategies, tools and activities, resulting in a tailored mixture of military operations, subversive and propaganda activities, political and economic measures and so forth.[11] Another conceptual model, as representative as the previous one, but which portraits the attacker's behaviour depending on that of the defender is shown in Figure 2.

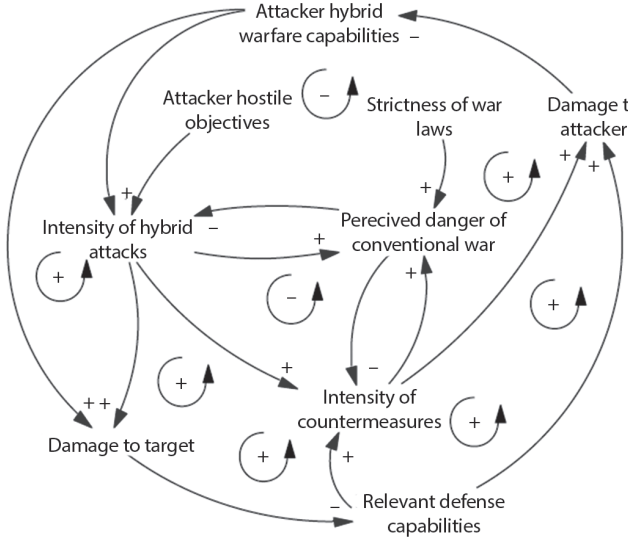

Figure 2: Designing attacker and defender's behaviours during HW
Source: Balaban–Mielniczek 2018: 3714

[11] Giannopoulos et al. 2021.

According to the model, the HA intensity is strongly correlated to the attacker's objectives and fluctuates depending on his HW capabilities. Also, the HA intensity influences in a positive way both the amplitude of the effect on target and the intensity of the defender's reaction. For this reason, it can be concluded that the higher the HA intensity, the more pronounced the effect on target and implicitly the defender's countermeasures will be. Thus, damaging the target through the effects obtained decreases its defensive capabilities, on the one hand, and on the other hand, it stimulates the defender's responsiveness capacity, which in turn limits the attacker's offensive capabilities.[12]

Adversary's tools used

From the information provided, it can be easily inferred that HW is an extremely complex and dynamic phenomenon, in which the opponents can use a wide variety of measures and capabilities to fulfil their objectives. For this reason, the HW is defined as "the synchronized use of multiple instruments […] tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects".[13] Practically, in this framework, the adversary tries to determine and use the most suitable formula for engaging the opponent, which is built using the harmonious integration of different tools such as those in Table 1.

Table 1: Adversary's tools used for HT/HA

Tools	Targeted domains
Kinetic operations against infrastructure	Infrastructure, Cyber, Economy, Space, Military, Information, Social, Public Administration
Building/exploiting economic dependencies	Economy, Political, Diplomacy, Public Administration
Building/exploiting infrastructure dependencies	Infrastructure, Economy, Cyber, Military, Space, Public Administration
Industrial espionage	Economy, Intelligence, Information, Infrastructure, Space, Cyber

[12] Balaban–Mielniczek 2018.

[13] Cullen – Reichborn-Kjennerud 2017: 3.

Tools	Targeted domains
Exploiting economic burdens	Economy, Political, Diplomacy, Public Administration
Undermining the national economy of the target state	Economy, Political, Diplomacy, Public Administration
Cyber operation/espionage	Cyber, Space, Infrastructure, Military, Public Administration
Territorial violation	Military, Political, Diplomacy, Social
Weapons proliferation	Military
Armed forces operations	Military
Rogue and third-party actors' activities	Military, Social
Military exercises	Military, Political, Diplomacy, Social
Supporting cultural groups	Culture, Social, Political, Diplomacy
Shaping/exploiting diasporas for own interest	Diplomacy, Political, Social, Culture, Intelligence
Building social disturbances	Social, Economy, Infrastructure, Political
Exploiting public administration's vulnerabilities	Public Administration, Social, Political
Promoting/exploiting corruption	Social, Public Administration, Legal, Economy
Exploiting law's vulnerabilities	Legal, Infrastructure, Diplomacy, Political, Intelligence, Information, Cyber, Space, Military, Economy, Culture, Social, Public Administration
Intelligence operations	Intelligence, Military
Clandestine operations	Intelligence, Military
Infiltration	Intelligence, Military
Disinformation and propaganda	Information, Political, Cyber, Culture, Social, Public Administration
Media and interference	Information, Social, Culture, Infrastructure
Electronic operations	Cyber, Space, Military, Economy, Infrastructure
Exploiting migration/immigration for political purposes	Social, Political, Diplomacy
Supporting/discrediting political actors/leaders	Political, Social, Public Administration
Coercion of governments/political leaders	Political, Legal, Public Administration
Diplomatic sanctions	Political, Diplomacy, Economy
Using embassies	Diplomacy, Intelligence, Political, Social

Source: Giannopoulos et al. 2021: 33–35.

It should be noted that only a few of the tools that can be used by the adversary for coagulating the HT/HA are scored in the table. Also, visualising these tools, it can be seen that their relationships can form the aggressor's hybrid behaviour, but not every combination of them can be considered hybrid. Normally, the hybrid character is given by the combination of tools from various domains, but here too there are exceptions. For instance, using 'exploiting economic burdens' together with 'undermining national economy of the target state' might not be hybrid, different from 'armed forces operations' combined with 'rogue actors activities' which should be considered hybrid.

Adversary's strategies, operations and tactics

Another aspect that must be clarified within this chapter refers to highlighting some of the strategies, operations and tactics that might be available to the hybrid adversary. All these, correlated with the previous information, substantiate the aggressor's probable COAs. Regarding the hybrid adversary's doctrine, other key principles underlying his aggressive behaviour are given by:[14]

- Centralising the decision-making capability – is achieved by integrating all civil and military decision-makers, necessary to coordinate the hybrid actions.
- Assuming hybrid actions as core missions – involves the adaptation of the traditional doctrine by including the necessity of carrying out missions/tasks in the HW framework.
- Carrying out long-term aggressive information campaigns – necessary to enhance the 'patriotic consciousness' for resurrecting the national fighting will; on the other hand, information operations (IO) are used to generate non-lethal effects on the target state's population and local administration bodies, as well as on the international community.
- Developing the expeditionary capabilities – necessary to achieve conventional strategic deployment and conduct HW actions anywhere and anytime.
- Improving the ability to use private security companies (PSC) or other proxies – in a HW spectrum the aggressor's operational success largely depends on his capacity to use conveniently PSCs or other proxies; by

[14] Clark 2020.

doing this the aggressor will improve his fighting power which will be directed against the defender's vulnerabilities.
- Prioritising the IOs and subordinating the kinetic operations to IOs – if in conventional warfare the lethal operations are more important than IOs, in case of HW contexts we witness a radical change, due to the fact that non-lethal effects are planned and generated more frequently, often proving more effective.

Generally speaking, the strategies that can be employed by an aggressor in HW are complex and multidimensional. According to literature review, a hybrid aggressor may use four types of strategic-level COAs triggered by his strategic objectives. These COAs are briefly described in Table 2.

Table 2: Aggressor's strategic-level COAs in a HW framework

COA type	**Particularities**
COA_1: Strategic operations	conducted for precluding an extraregional power to intervene in an interest region have a continuous character, being used during wartime and peacetime, as well as during the other types of operations (COAs) use all types of power instruments (tools) to engage the defender's centres of gravities (COG) previously use non-military means, and afterwards, depending on the situation, military means primarily target national will, public opinion, political decisions, leaders and warriors' morale
COA_2: Regional operations	directed against regional defenders or internal threats conducted both for countering threats and exploiting opportunities in order to maintain or expand the aggressor's regional influence have a pronounced conventional offensive pattern, aiming to disaggregate the defender's capabilities and diminish his resisting will by engaging armed forces, local population and critical infrastructure, limiting freedom of movement (FOM), destabilising control, retaining initiative, etc. depend on strategic operations in order to preclude an outside intervention
COA_3: Transition operations	directed with dual purpose for retaining the initiative and handling with an outside intervention; thus, are adopted when another actor, regional or extraregional, manifests his intention or actually intervenes in support of the defender used as a bridge between regional operations and adaptive operations, being able to expand in any of the two directions comprise specific elements of regional and adaptive operations

COA type	Particularities
COA_4: Adaptive operations	adopted for preserving the aggressor's combat power, degrading the opponents' fighting capabilities, gaining time for successful strategic operations conducted as a counteraction to the defenders' reaction, especially for countering the additional actor's intervention based on a defensive posture, correlating conventional and unconventional capabilities (last one more presented) to balance the combat power

Source: Department of the Army 2010: 4-1–4-4

All these COAs are sustainable and can be adopted depending on the strategic context, in relation to the defender's reaction and other considerations related to the operational environment. Normally, strategic-level COAs could be adopted successively with the development of the strategic and operational dynamics, which means that the aggressor should start with COA_1 and progressively could reach COA_4. Moreover, as we pointed out before, COA_1 should be correlated with the other COAs, because strategic operations are absolutely necessary for shaping the operational environment. Therefore, there are several options (strategies) regarding the applicability of the proposed COAs, as follows:

- COA_1 – when the aggressor can achieve the desired objectives only through strategic operations.
- $COA_1 + COA_2$ – involves the application of combat power in an offensive manner (mostly likely conventional imprinted) supported by strategic operations to shape the operational environment (shaping operations).
- $COA_1 + COA_2 + COA_3$ – largely similar to the previous version plus the need to counter the intervention of another regional or extraregional opponent.
- $COA_1 + COA_2 + COA_3 + COA_4$ – one of the most complex variants, because it relates to all the proposed COAs. It is almost similar to the previous one to which is added the need to adopt a defensive posture (most likely unconventional imprinted) as a result of the overwhelming combat power of the opponents.
- $COA_1 + COA_2 + COA_3 + COA_2$ – as complex as the previous variant, but in this situation the aggressor returns to regional operations (offensive fashion) due to the fact that he has sufficient combat power to handle with an extra adversary regionally or extraregionally.

Certainly, other strategies in the form of strategic-level COA combinations can be established, for understanding the aggressor's behaviour in the HW framework. Regardless of the selected strategy, the aggressor will contextually combine conventional and unconventional ways and means to fulfil his desired strategic objectives. Within these combined strategic-level COAs, the adversary may use a wide variety of blended tactics to fulfil designated missions and tasks. For instance, at the tactical level these blended tactics allow the adversary to operate both conventionally and unconventionally/asymmetrically. If for conventional activities the adversary normally uses regular and paramilitary forces, for unconventional ones he might use a mixture of elements including insurgents, guerrilla, terrorists, criminals, partisans, gang violence, demonstrations, riots, and so forth. On the other hand, conventional tactical activities are offensive, defensive, stability and enabling in nature, different from asymmetric tactical activities which cover a lot of tasks such as "diversionary actions; reconnaissance and early warning; money laundering, smuggling, transportation; civic actions".[15] Moreover, although each element of the hybrid force is designated to perform specific tasks, in the context of HW regular elements can also be used for asymmetric tasks, just as unconventional elements can be employed for offensive, defensive, stability or enabling tasks.

Hybrid COAs at tactical level

Understanding the previous aspects also involves the tactical design of some possible hybrid adversary's COAs which match the hybrid strategic-level COAs. These COAs will stress the type of operation, elements of combat formation, specific tasks and finally the scheme of manoeuvre (SOM). Each of the three COAs address a theme of major combat operations (MCO), and all will have specific elements of information warfare (INFOWAR). The first COA which fits into the context of strategic-level COA_2 (regional operations) has an offensive imprint and deals with a dispersed attack. From a theoretical perspective, this type of attack is an offensive action adopted when the defender is technologically superior or the aggressor does not have the capacity to provide integrated command and control (C_2) during his offensive operation. In this scenario, the hybrid adversary uses regular military forces and guerrilla elements to fulfil

[15] Department of the Army 2010: 6-7.

his designated mission. Visualising Figure 3, it can be seen that the adversary's combat formation include the following types of forces:[16]

- Fixing/disruption forces – company/battery-level units organised from reconnaissance, antitank, mechanised infantry and multiple launch rocket systems (MLRS), as well as guerrilla and INFOWAR capabilities.
- Assault forces – a detachment including 3 light infantry companies, 2 antitank batteries, 1 air defence artillery (ADA) battery and INFOWAR capabilities.
- Exploitation forces – a combined detachment comprising special purpose forces (SPF) teams, 1 ADA battery, 1 artillery battalion and guerrilla affiliated elements.

Figure 3: Hybrid dispersed attack
Source: Department of the Army 2010: A-4

[16] Department of the Army 2010.

As it can be understood by analysing Figure 3, there are specific tasks that must be conducted by each designed detachment. According to the sketch from Figure 3, these tasks generally refer to:[17]

- Fixing/disruption forces – fix the reconnaissance elements; perform deception, electronic warfare (EW) and IO; limit the use of reserves and quick reaction forces (QRF); neutralise/destroy intelligence, surveillance, reconnaissance (ISR) capabilities
- Assault forces – neutralise C2 and joint fires capabilities from the brigade level
- Exploitation forces – destroy brigade main support and sustain capabilities

Regarding the specific SOM which can be detached within this hypothetical scenario, it is characterised by the following aspects:[18]

- Using fixing forces, the attacker disrupts the defender's brigade capabilities; to do so the attacker generates IO's lethal and nonlethal effects including engaging indigenous population from the urban area of operation (AO), jamming brigade communications (EW), conducts tactical deception with all organic elements including multiple launch rocket system (MLRS) battery to deceive armoured reconnaissance battalion and the two infantry mechanised battalions with the location and time of decisive operation.
- While the deception is conducted by fixing forces, the attacker introduces the air assault detachment to neutralise the brigade C2 using INFOWAR/electronic attack and other kinetic capabilities. At the same time, he destroys the defender's joint fires capabilities.
- Once the assault forces are about to accomplish their tasks, the attacker introduces the exploitation forces to conduct the decisive operation. In this regard, using special purpose forces (SPF) and guerrilla affiliated teams, supported by heavy artillery fire, the attacker destroys the brigade's main capabilities from designated AO.

Next COA which is suitable with strategic-level COA_4 (adaptive operations) is a hybrid retrograde operation, more specifically hybrid delay from subsequent positions in which the adversary uses a mixture of regular and insurgent forces.

[17] Department of the Army 2010.
[18] Department of the Army 2010.

As can be seen in Figure 4, the adversary's combat formation is structured on four main bodies (detachments):[19]

- Disruption forces – platoon-level subunits organised from motorised infantry, insurgent elements (2 platoons for each) and SPF teams.
- Contact forces – an infantry battalion organised as a battle group (BG) structure (3 company-level BGs); as can be noticed, each interdict direction is covered by a company-level BG (infantry and armoured).
- Shielding forces – antitank, artillery and INFOWAR structures, emplaced on each probable avenue of approach.
- Reserve forces – an armoured battalion emplaced in the assembly area (AA). Armoured battalion is minus due to the fact that an organic company reinforces each company-level BG (1 armoured platoon for each infantry company).

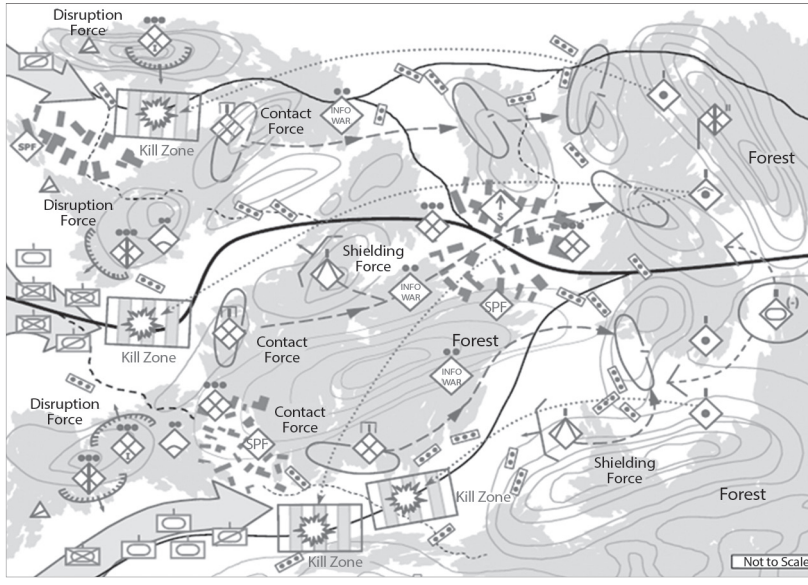

Figure 4: Hybrid delay (from subsequent positions)
Source: Department of the Army 2010

[19] Department of the Army 2010.

On the other hand, each body or detachment has specific tasks, and only their integration ensures the mission fulfilment. More specifically, the tasks may be resumed to:[20]

- Disruption forces – conduct shaping operations for modelling the AO. In this regard, specific tasks are related to fixing the reconnaissance elements that operate on each interdict direction, conducting deception, EW and IO by engaging the indigenous population and local authorities, forcing the premature use of the opponent's main forces, and destroying ISR capabilities.
- Contact forces – engage the opponent's forces during delay by defending subsequently the preplanned battle positions by forcing the opponent's main forces to slow down momentum and to deploy his forces in vulnerable positions (kill zones).
- Shielding forces – support the contact forces with support by fire and jamming communication tasks by fixing the opponent's main forces on interdict directions.
- Reserve forces – conduct the decisive operation by supporting the contact forces in maintaining the battle positions in accordance with the higher echelon's concept of operation (CONOPS).

Correlating all these tasks, the adversary's SOM that can be depicted based on the sketch from Figure 4 has the following form:[21]

- Initially the adversary uses the disruption elements to augment his combat power as follow: engage indigenous population and local authorities using SPF teams; at the same time, using INFOWAR (EW), degrades the opponent's C2 and ISR capabilities by using insurgent and motorised infantry platoons, fixes the opponent's reconnaissance elements and deceives his forces to determine their prematurely operational employment.
- Next, with contact company-level BGs and shielding batteries, defends subsequently the preplanned battle positions in accordance with the higher echelon CONOPS.
- Uses armoured battalion as a reserve to maintain the battle positions and to degrade the opponent's offensive combat power.

[20] Department of the Army 2010.
[21] Department of the Army 2010.

– Finally, using all combat detachments, channels the opponent's main forces in vulnerable positions to create favourable conditions for decisive counterattacks (CATK) conducted by higher echelon using additional combat structures.

Last COA, addressing the theme of stability operations, focuses on correlating guerrilla and SPF actions with passive measures of regular military forces. Related to the strategic picture of the hybrid adversary, this COA can be anchored in the framework of strategic-level COA_3 which deals with transition operations. Because the latter might evolve into two different directions, such as regional operations (strategic-level COA_2) or adaptive operations (strategic-level COA_4), the same could happen in the situation of the current tactical COA (hybrid stability operations). The adversary's combat formation has the following particularities:[22]

– disruption forces – organised from guerrilla elements and SPF teams
– repositioned forces – provided by mixed structures of motorised infantry, mechanised infantry and field artillery

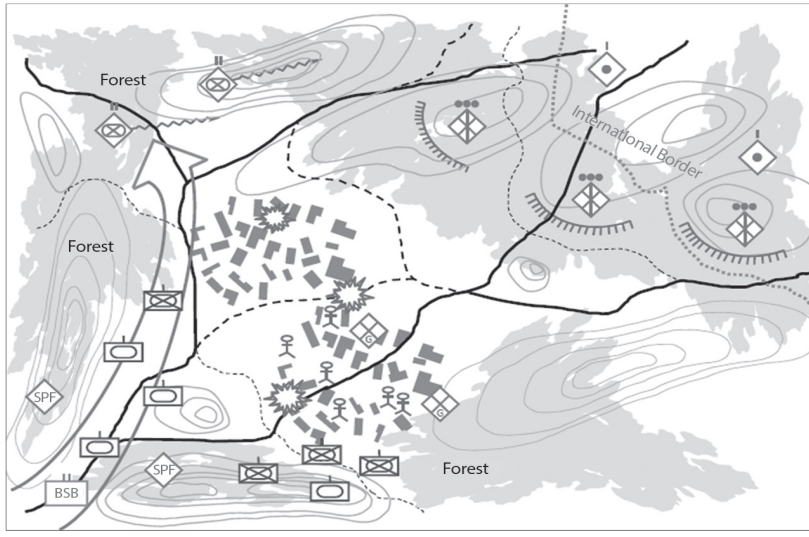

Figure 5: Hybrid stability operations
Source: Department of the Army 2010

[22] Department of the Army 2010.

As far as the specific tasks of the hybrid force's elements are concerned, they are given by:[23]

- disruption forces – fix the reconnaissance elements, deceive the opponent's main forces, conduct EW operations, shape the local population behaviour to gain its support and destabilise civil functions
- repositioned forces – deploy in the preplanned defensive positions in the vicinity of the international border, conduct presence missions in the area with the aim of deterring the opponent

Broadly speaking, the adversary's SOM for this hypothetical scenario is carried out in accordance with the following algorithm:[24]

- deploy regular military forces and occupy preplanned defensive positions
- at the same time, conduct tactical deception using affiliated guerrilla elements and SPF teams such as EW operations, disinformation, sabotage
- use the same elements (guerrilla and SPF) and with the support of indigenous population and local authorities degrades the civil critical infrastructure of the urban AO by conducting kinetic attacks
- conduct deterrence missions through the gradual prepositioning of regular military forces

Within these COAs it can be noted that the indigenous population plays an important role in the outcome of the operations. For this reason and considering the lessons learned from recent/ongoing military operations in Ukraine, Syria, Iraq and so on, the population can support the adversary either willingly or by force, for the latter option being used as a human shield. Also, in order for these tactical COAs to be logical, they must be multi-domain supported at all levels (operational, strategic and political) from a joint interagency, intergovernmental and multinational (JIIM) perspective.

Conclusion

HT and HA are the main fighting forms of HW used by an aggressor opponent. While the HT is considered a hostile intent prior to aggression, the HA represents

[23] Department of the Army 2010.
[24] Department of the Army 2010.

the actual attack using hybrid ways and means. The purpose of this chapter is to generate a comprehensive picture of the adversary's behaviour in the context of HW. Subsection *Conceptual models* highlights some of the representative conceptual models of the HT/HA. Besides the principles underlying them, this subsection analyses the constituent elements of the conceptual models such as actors, tools, domains, activities and targets, as well as the aggressor's behaviour in relation to that of the opponent. Subsection *Adversary's tools used* develops the problem of the tools used by the adversary for coagulating and directing HT/HA. The actual tools within the different domains are highlighted in terms of infrastructure, cyber, economy, space, military, information, social, etc. on the one hand, and on the other hand, the relationships that can be established between them to generate HT/HA. Subsection *Adversary's strategies, operations and tactics* is dedicated to specific strategies, operations and tactics that a hybrid adversary might use to fulfil his objectives. It analyses the main COAs at macro level such as strategic, regional, transitional and adaptive operations, the combination of which forms different strategies used by a hybrid adversary. Also, stressing some of the blended tactics based on correlating conventional and asymmetrical tactical activities is another subject of this subsection. Subsection *Hybrid COAs at tactical level* presents three variants of tactical COAs that might fit in the situation of the hybrid adversary. Within each hybrid COA, the aspects regarding the type of operation, elements of combat formation, specific tasks and SOM are highlighted.

Questions

1. What are the constituent elements of the HT/HA's conceptual models and what is the role of each one? Explain the aggressor's behaviour during HA in relation to the opponent's reaction!
2. What are the tools that the adversary could use for HT/HA?
3. How are the strategic-level COAs applicable to the adversary in the HW framework? Describe briefly each strategic-level COA!
4. Considering the strategic-level COAs, explain some of the strategies that the adversary could use in HW!
5. Explain a tactical COA that the adversary could apply within HW, highlighting the type of operation, elements of combat formation, specific tasks and SOM!

References

Balaban, Mariusz – Mielniczek, Paweł (2018): Hybrid Conflict Modeling. In Rabe, Markus – Juan, Angel A. – Mustafee, Navonil – Skoogh, Anders – Jain, Sanjay – Johansson, Björn (eds.): *Proceedings of the 2018 Winter Simulation Conference.* Gothenburg, Sweden, 3709–3720. Online: https://doi.org/10.1109/WSC.2018.8632492

Clark, Mason (2020): *Russian Hybrid Warfare.* Institute for the Study of War. Online. www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

Cullen, Patrick J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* A Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Department of the Army (2010): *Hybrid Threat. TC 7-100.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100.pdf

Department of the Army (2011): *Opposing Force Tactics. TC 7-100.2.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100x2.pdf

Department of the Army (2015): *Hybrid Threat Force Structure. Organization Guide. TC 7-100.4.* Online: https://irp.fas.org/doddir/army/tc7-100-4.pdf

Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi eds. (2021): *The Landscape of Hybrid Threats.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/44985

Monaghan, Sean – Cullen, Patrick – Wegge, Njord (2019): *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare.* A Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Csaba Krasznay – Péter Bányász – Éva Jakusné Harnos[1]

Geopolitical Context, Ideologies and Motivations

The 21st century global power shift has brought the revival if geopolitics both as a theory of international relations and a framework for analysis. Geopolitics is the study of the struggle for the control of geographical entities for political advantage. On the world stage, states are competing as strategic rivals using their territories and natural resources to a maximum in order to gain control over more. Competition for geopolitical power has material, relational and ideological dimensions. This means that, against the background of the race for material assets, relations, e.g. alliances and institutions are being restructured, and new ideologies are formulated in order to justify the objectives of the rising powers, while discourse about prevalent ideologies is amplified so as to stabilise the current international system established by the leading powers of the post-World War II era. So-called revisionist states have challenged the current status quo in international politics, first of all, China and Russia, and other ambitious rising powers can be seen in each region of the Globe. Fragmentation and re-arrangement impact nearly all components of the geopolitical framework: places, regions, territory and networks. This results in a re-interpretation of territoriality, regionality and identity, the re-conceptualisation of which is facilitated by modern technology, especially digital networks. The latter may also affect societies and disseminate ideologies unnoticed and at incredible speed. Consequently, the population of any country can be directly targeted by any system of beliefs and social or political philosophy, even hostile and subversive, which may lead to the loss of the internal and external sovereignty of a state. The power struggle for establishing a new world order has been extended to cyberspace. The importance of digital technology and the efficiency of digital networks is also proven by a case study of the Ukrainian–Russian war. Apart from the study of the effect of networks, two new factors should be considered: the geographical environment is changing due to climate impact; for instance, the Arctic has been drawn into

[1] Ludovika University of Public Service.

DOI: https://doi.org/10.36250/01236_10

the geopolitical competition; and the role and number of non-state actors is increasing, including NGOs, multinational corporations and high-tech giants.

The geopolitical perspective

Geopolitics in the traditional sense is an academic field studying the practice of states in their efforts to compete for territories and control them.[2] The theory was a justification of a country's regional or worldwide ambitions from the beginning. In the late 19th century, British scholars Alfred Thayer Mahan and Sir Halford Mackinder developed theories on the contest for land and sea power and resources. In parallel, German geopolitics was created by Friedrich Ratzel and Rudolf Kjellen, who claimed that developed states with more sophisticated culture had the right to occupy more territory. Karl Haushofer transformed the idea to extreme ideology under the rule of Hitler, which led to the disgrace of geopolitics and its disappearance from the language of politics after the Second World War for decades. In the United States, theoreticians of geopolitics took a more practice-oriented approach in the first half of the 20th century. For example, Isaiah Bowman, Nicholas Spykman and Alexander P. De Seversky discussed the global role of the U.S. and whether it should conduct an active or an isolationist foreign policy.[3] In Russia, the term and the perspective of geopolitics gained ground only in the 1990s,[4] but in the broad sense of interstate competition and less linked to geographical facts. Despite the criticism levelled at geopolitical theories, the early geopolitics scholars had relevant proposals which were accepted later. When Western strategists lay the foundations for NATO during the Cold War, they relied on Mackinder's 1924 recommendation to establish a Midland Ocean Alliance.[5] In addition, Mackinder's idea that global primacy is the question of who controls Eurasia has survived in Brzezinski's geostrategic views.[6] A comprehensive way of assessing power relations and great power competition is presented in Kissinger's World Order (1997). The major difference between early geopolitics and its contemporary trend is that

2 Flint 2006.
3 Flint 2006; Ashworth 2013.
4 Diec 2019.
5 Flint 2006.
6 Brzezinski 1997.

the former focused on the classification of territories of the Earth and their peoples into hierarchies so as to form a basis for war, alliance, or an empire, while the latter combines geographical and social knowledge so as to justify and interpret events in their overall context. Another important change has occurred in the concept of *geopolitical agent.* An agent is an entity that tries to achieve a specific objective. Nowadays states are not the only agents. Corporations, non-governmental organisations (NGOs) and various groups of people, such as a separatist movement or a group of Green activists can appear as agents. Agents may take a course of action depending on the situation and the structure in which they are embedded. Structures consist of legally enforceable rules and culturally accepted practices, that is, norms. Consequently, according to the current geopolitical perspective, not only geographical and social factors determine what agents do but also the system of international institutions and of international law. These generate expectations and decide what is acceptable. As for the role of states in the international system, agents can be *status quo states,* which want to maintain the current balance of power in the geopolitical space, or *revisionist states,* which have an interest in changing the balance even forcefully.[7] States strive for survival and they make any effort to gain as much power as possible, even aiming at hegemony. However, states cannot be certain about the intention of other states. In an effort to achieve their goals, states form alliances and establish international organisations and institutions.[8] For example, the liberal, multi-lateral institutions and the multi-level governance which we experience were established by the winner powers of the Second World War, including the United Nations Organization, NATO, the European Union, the International Monetary Fund, the World Bank. The international system is dynamic from a geopolitical perspective, that is, alliances and organisations keep transforming and re-drawing the geopolitical map. For instance, the United Kingdom exited from the European Union in 2020; Finland and Sweden have signed an accession bid to join NATO in 2022, and Iran and Argentina have applied to accede to BRICS. A coercive attempt to re-structure the geopolitical space is Russia's aggression against Ukraine and the following war, which will be discussed in a case study below. Since the realist perspective of geopolitics returned to the study of international relations, analyses have investigated the geopolitical aspirations and the underlying ideologies (see below) of revisionist

[7] Mearsheimer 2013; Mead 2014.

[8] Walt 1987.

states, especially, China, Russia and Iran.[9] Besides geopolitics, geo-economics has been used to maintain the current balance in contemporary international relations.[10] Whereas geopolitics breaks up the international system into regions, geo-economics may create macro-regions which, despite differences, may help maintain the liberal world order. Nevertheless, this idea has been challenged by China's ambitious New Silk Road Project announced in 2013, later re-named Belt and Road Initiative, which aims at establishing an extensive Eurasian sphere of influence.[11] Formerly, in this section the central role of *place,* more precisely, *space* was mentioned in addition to the key term *agent.* Researchers often distinguish between place (location), locale (local institutions which shape humans' identity) and sense of place (originating from collective identity).[12] However, space is a preferred term these days because of its multi-dimensional character. Key geographical places (features) are easy to identify on a map, for instance, continents, island, peninsulas, seas, oceans, straits, and historical experience suggests which may be fought over. But our perception of place, space and time is dynamic; that is, changes dependent on the circumstances. For instance, new geographical entities may gain significance as a result of the availability of minerals essential to IT industry. Probably, we need to adjust a map when states join or leave an international organisation, or when an ethnic group declares its independence from a state and it is recognised by the international community. Recently, due to climate change, the North Pole has become a territory of strategic importance which Western powers, Russia and China contest for. In consequence, NATO's commitment to safeguarding its security interest in the region has been declared.[13] The inclusion of space and cyberspace among the domains of military operations is also the outcome of our changing perception of *space* and of technological disruptions. The consequence of this change is stated in the strategic concepts of the alliance: Article 5 of the North Atlantic Treaty on collective defence can be invoked if a member is attacked.[14] Cyberspace has been created and maintained by human activity and its control has been crucial for nearly all fields of life, notably, for disseminating strategic narratives,

9 Mead 2014; Bolt–Cross 2018; Diec 2019.
10 Möttölä 2019.
11 Käpylä–Aaltola 2019; Leandro–Duarte 2020.
12 Starr 2013.
13 NATO 2022b.
14 NATO 2022a.

shaping international relations, influencing populations and conducting military operations, just to mention a few examples. Russia regards cyberspace a new domain for power competition referring to it as the *net empire,* which could be exploited for gaining the influence over foreign populations' minds.[15]

Ideologies, propaganda and strategic narratives

The interrelationship between political aspirations and pseudo-scientific theories developed for the justification of the objectives of state or non-state actors is illustrated by ideologies and strategic narratives, that is, types of persuasion. The present political struggle on the international world stage is interpreted as a clash of ideologies by some scholars.[16] Ideology is a set of beliefs, presented as a coherent world view that shapes norms and attitudes in society, leading to behaviour which is desirable for its propagator. It determines what is acceptable, right or wrong in a particular context.[17] Ideology always manifests in political discourse on certain focus topics and concepts, and has a regulatory impact on behaviour. Thus, the prominence of dominant political discourse in international relations is obvious: it sets the agenda, focuses or distracts attention and influences agents in their actions. This explains the importance of the media: the agents who have access to greater publicity will have more efficient strategic communication. The prevalent political discourse always seems obvious to people who are surrounded by it, and discourse which diverts because it represents different ideologies is noticed and identified as an attempt at persuasion. In the international struggle to establish a new world order all states have made propaganda strategies a component of their foreign policies.[18] Although the term "propaganda" has been discredited due to manipulation during the world wars, its definition could still be used as an umbrella term for all types of persuasion: it is "a deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behaviour to achieve a response that furthers the desired intent of the propagandist".[19] The transfer of ideology often takes the form of strategic narratives in international

[15] Diec 2019.
[16] Müllerson 2017.
[17] Jowett–O'Donnell 2015.
[18] Jowett–O'Donnell 2015.
[19] Jowett–O'Donnell 2015: 7.

relations. Narratives allocate meaning to past, present or future events and represent perceived interests. Zaffran[20] categorises strategic narratives into three types: system narratives (about international order), identity narratives (agents or actors in the international system) and policy narratives (justifying specific policies or action). In summary, the boundary between ideology and propaganda is narrow: ideology is a seemingly scientifically based system of ideas which is spread by propaganda. The most important communicator of ideas is language and its use in specific situations for political purposes is called political discourse. Propaganda comprises more than political discourse or strategic narratives because it exploits the communicative opportunities lying in language, media, sociological and psychological knowledge. Cyberspace has established new channels for disseminating rival ideologies and designing new techniques for persuasion, which may prove more effective than earlier as a result of multiple variants of disguise (see below). With the appearance of this virtual space, "cyberspace geopolitics" has evolved, with a combination of individual, institutional as well as state actors often involved in adversarial activities in order to gain superiority and occupy cyberspace, similarly to physical space. Contestation in cyberspace manifests in four layers according to Douzet: 1. physical infrastructure; 2. logistical infrastructure; 3. applications and data programmes; and 4. cognitive interactions.[21] Cyber diplomacy and efforts to set norms and legally regulate cyberspace activities have added a fifth layer to cyberspace according to Smith.[22] The layer of cognitive interactions is the location of the competing strategic narratives and influence operations of geopolitical players discussed above. The exploitation of cyberspace for malicious purposes poses a severe security threat because, due to the lack of boundaries, any disguised or covert actor can disrupt a society even in peacetime.

The sections below discuss information operations analysing a case study (cyberspace layer 4, cognitive interactions), then place the security issues of rivalry in cyberspace in geopolitical context (layers 1. physical infrastructure; 2. logistical infrastructure; and 3. applications and data programmes), also exploring the probable motivations of key players. The conclusion summarises the forecast of the UN Group of Governmental Experts on dangers arising from contestation in cyberspace and for cyberspace.

[20] Zaffran 2019.
[21] Douzet 2014: 4–5.
[22] Smith 2023:1225.

Case study: Russo–Ukrainian War

The military operation, launched by Russia on 24 February 2022, surprised the general community, despite the massive information operations that had been conducted by Ukraine and NATO, as well as by Russia, before the start of the war. The United States and its allies, including Ukraine, have regularly accused Russia of preparing to conduct a military attack against Ukraine. Meanwhile, Russia accused Ukraine with a constantly changing narrative, which was often more absurd, attempting to present itself as the victim (systematic genocide of the Russian minority, development of Covid in Ukrainian biological laboratories with U.S. support). The psychological operations that were part of the information operations increased significantly after the beginning of the war on all sides. In the early days of the war, Russia was unable to achieve its assumed goals of gaining aerial and information superiority, which resulted in a lengthened conflict – at the writing of this study, it is unclear when the armed conflict will end,[23] but the ongoing sanctions are pushing Russia towards a significant crisis.[24] The impact of sanctions also poses substantial challenges to European countries, especially regarding energy supply.[25] Among other things, the effects of the war have also drawn attention to the slowdown in the world economy and changes in global supply chains.[26] Presumably, Russia expected marginal reactions from the United States and the European Union following its aggression in 2014,[27] but from a geopolitical perspective, it chose a time for war when the different NATO and EU member state governments, given their domestic political developments, were interested in showing strict unity against Russian aggression and in supporting Ukraine significantly. Just a few examples:

- France had presidential elections during the war, and President Macron's campaign presented him as a strong leader and, in the post-Merkel period, as a visionary politician who would define the future of strong integration of the European Union.

[23] Yarchi 2022.
[24] Smith 2022.
[25] Doukas–Nikas 2022.
[26] Mariotti 2022.
[27] The fact that Finland and Sweden, breaking a decades-old taboo, indicated their desire to join NATO, which was supported by most NATO member states, is also an indication of the Russian side's misjudgement of the situation.

- There will be a mid-term election in the U.S. in the autumn of 2022, and the Biden Administration needs to show strong, competent leadership after the economic crisis caused by Covid-19 and the failed withdrawal from Afghanistan in August 2021.
- Although Poland has historically had severe misgivings about Russia, it has tried to resolve its conflict with the EU Commission on the issue of the rule of law.
- Turkey is heading into a severe recession, but President Erdogan has well recognised the reshaping of the balance of power in the Black Sea, which makes Turkey, and thus himself, an even more unavoidable stakeholder, as he will soon become a key actor in the world's grain supply and Europe's gas supply, in addition to the Syrian refugee crisis.

The length of the war surprised most experts, as there was general agreement on Russia's significant military capabilities. In addition to its conventional warfare capabilities, perhaps only Russia's cyber capabilities were – as far as we know today – significantly overestimated. Over the past decades, state-sponsored hackers linked to the Kremlin have been suspected of committing a series of paradigm-shifting cyberattacks that have shaped, guided and framed NATO's strategic thinking on cybersecurity. This includes not only the distributed denial-of-service (DDoS) attacks on Estonia's Critical Infrastructures of government, financial and media services in 2007,[28] but also the interference in the 2016 British Brexit referendum[29] and the American presidential election. Following these events, Russia was always suspected by the Western public to be behind the large-scale cyberattacks, and Russia, whether or not it was involved, used its intensive information operations to reinforce fears of Russian hackers' omnipotence.[30] The Homeland Security and FBI joint report investigating interference in the 2016 U.S. presidential election attributed Russia as the perpetrator.[31] Sophisticated cyberattacks can cause substantial damage because an attack is carried out not only in the physical dimension but also in the cognitive dimension. Following the already mentioned 2007 cyberattack against Estonia, several authors have considered the possibility of outlining scenarios for such complex cyberattacks.

[28] Lesk 2007; Arquilla 2013.
[29] Treisman 2018.
[30] Lanoszka 2019.
[31] Kovács–Krasznay 2017b.

In Hungary, for example, the authors analysed it in terms of Digital Mohács in 2010.[32] They then supplemented it with the impact of the 2016 U.S. presidential election in 2017.[33] The paradigm-shifting events of the Ukrainian–Russian conflict, which was the basis of the case study, inspired the authors to add a new addition, Digital Mohács 3.0, which is being prepared at the time of this writing. As will be seen later, cyberattacks and psychological operations in the cognitive dimension affect each other, not merely complement each other. The events of the recent war period have, in many ways, required us to rethink our perceptions of cybersecurity. Contrary to expectations, Ukraine has surprised us not only in its conventional warfare but also in its high level of cyber capabilities. In the latter, a significant contribution was made by so-called "cyber volunteers". These civilians were outraged by Russian aggression, in which the professional Ukrainian psychological operations also played a considerable part. As citizens of other countries, these hundreds of thousands of civilian volunteers were/are participating in the attack on Russian electronic information systems. Many of them are members of the IT Army, officially created by Ukraine. Volunteers have not only supported Ukraine but also a progressively growing number of pro-Russia groups, typically cybercriminal groups, in the beginning. For many years, Russia has used the Russian cybercriminals in its hybrid operations based on a silent agreement:

- Russian hackers can be active freely, but they cannot attack Russian targets, only foreign ones; and
- if the Russian state interest so requires, they should use their expertise to provide their contribution to Russia's operations in cyberspace

NATO declared at the Warsaw Summit in 2016 that cyberspace is a new field of domain in its strategic thinking.[34] The continuous strategic planning that has been going on since 2007 is necessarily able to reflect on the high-impact events that have occurred, and only on paper is it possible to plan for the capabilities and consequences of cyberspace as a field of domain. The Ukraine–Russia war, however, has rewritten the paper form and has given rise to many new types of threats whose responses we cannot assess today. In the first months of the war, Russia's electronic information systems were subjected to a tremendous amount

[32] Kovács–Krasznay 2010.
[33] Kovács–Krasznay 2017a.
[34] Kovács 2018.

of cyberattacks, with an extraordinary amount of data of various kinds being released, including personal data, financial data, and sensitive and classified data. In addition, large numbers of critical information infrastructures (transport systems, satellites, nuclear facilities, public utilities, etc.) were attacked. In addition to the cyberattacks, as mentioned above, a significant amount of psychological operations was carried out by the participating parties, with different aims. Ukraine, as the attacked party, was in a more favourable position, as it was easier to gain the support of the international public opinion. And this was vital to the war's outcome, as it meant that the European Union and NATO member states were held together, thwarting Russia's supposed expectations. This manifested not only in the acceptance of sanctions but also in substantial arms support, which at the time of writing has evened out the asymmetrical conditions between Ukraine and Russia. The psychological operations of conflict will be discussed in more detail in the chapter of the third volume of *Hybrid Warfare Reference Curriculum* entitled *Social Media: An Instrument of Public Diplomacy and a Weapon of Psychological Operations.* The successful psychological operations that Ukraine carried out led many young people from all over the world to feel the necessity to take a stand against Russian aggression, which led to the emergence of those above mentioned "cyber volunteers". Hundreds of thousands of young people have learned their offensive capabilities to penetrate protected systems without consequences. However, this involves a number of risks, of which one of the most important aspects is the "pacification" of "cyber volunteers" after the war is over. The critical question is how to ensure that they do not end up as cybercriminals, but instead use their skills ethically.[35] At the moment of writing, it is not yet clear when and in what form the war will end. What is certain is that the previous world order has been disrupted, with unforeseeable consequences. In future conflicts, cyber warfare will undoubtedly play an increasing role, with implications for the citizens of participating states and the entire world.

Cyberspace, the new domain

One of the most interesting sites of geopolitical struggle is cyberspace. While traditional physical dimensions such as the oceans, the poles and outer space have been the scene of intense competition between great powers throughout

[35] Feledy–Virág 2022.

history, digital technologies and the networks they create have only emerged lately and radically transformed our world in the last 30 years. Moreover, unlike physical space, which is mostly shaped by nature, cyberspace is a virtual space created entirely by humanity, and more specifically by the United States of America, which would not exist without the help of excellent scientists and U.S. government funding. Moreover, in cyberspace, it is not easy to identify the classical resources that could justify the special attention that this intangible space receives in the world political arena. The particular importance of cyberspace must be sought in the social and economic development of the 21st century. Computers began to proliferate in the 1980s, the Internet in the 1990s. At that time, the Internet was primarily a playground for a few million Western scientists and engineers. Today there are nearly 5 billion internet users globally. Although the importance of computers was clear from the beginning, with their use spreading steadily in both government and business, few people imagined that the digital space would one day become a dominant issue in world politics after the fall of communist regimes and the dawn of the global expansion of Pax Americana. However, U.S. government policy at the time foresaw the internet as a tool for global dominance. One of the early, but perhaps most important strategies of Bill Clinton's first presidency was *The National Information Infrastructure: Agenda for Action (NII).* It includes the following objective: "The benefits of the NII for the nation are immense. An advanced information infrastructure will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people – ameliorating the constraints of geography, disability, and economic status – giving all Americans a fair opportunity to go as far as their talents and ambitions will take them. […] Information is one of the nation's most critical economic resources, for service industries as well as manufacturing, for economic as well as national security. By one estimate, two thirds of U.S. workers are in information-related jobs, and the rest are in industries that rely heavily on information. In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance for the United States. Those technologies will help U.S. businesses remain competitive and create challenging, high paying jobs. They also will fuel economic growth which, in turn, will generate a steadily-increasing standard of living for all

Americans."[36] These ideas foreshadowed the need for the powers competing with the U.S. to be able to offer an alternative in the field of information technology and to develop their own capabilities. At the time of the Agenda's publication, Japan appeared to be the most competitive country in this area, but by the 2020s, China is clearly the country that is the main challenger to the U.S. in the technological field. For a country that was economically insignificant in the early 1990s, China's emergence as a second power, a clear competitor to the U.S., is extraordinary. Paradoxically, the global opening of the Pax Americana has helped a lot. Chinese students turned up en masse at the best universities in the U.S., while U.S. manufacturers opened manufacturing plants in China in the hope of cheap labour. Ostensibly, it was all about the U.S. economic advantage, as the brain drain strengthened the U.S. knowledge economy, while the resulting products could be made as cheaply as possible in Asia. In the 2000s, however, Chinese engineers and scientists began to return home and put their knowledge to work in Chinese universities and companies. Intellectual property that was brought to China in the course of manufacturing was treated rather loosely by the locals, who copied Western solutions to the point of industrial espionage. No wonder that by the 2010s, the intellectual capital and manufacturing capacities to create digital products and services had been created.[37] The 12th Five-Year Plan, adopted in 2012, explicitly supports the strengthening of manufacturing capabilities in emerging technologies, and the 13th Five-Year Plan in 2017 puts a strong emphasis on the diffusion of technologies such as mobile technology, cloud computing or the Internet of Things. The China 2025 strategy makes it clear that China's goal is to become the strongest "cyber power".[38] However, it is questionable whether this can be achieved. The U.S. already recognised the Chinese threat in the technological field during the Obama presidency and has tried to push back against it with tough sanctions during the Trump presidency (from the ban on 5G technologies, to the blocking of some Chinese mobile phone manufacturers from U.S. software, to the attempted acquisition of one of the most popular Chinese-owned social networks). Under President Biden, this trend is deliberately continuing, with China as the primary strategic adversary for the U.S., and he is doing everything he can to maintain U.S. global position and

[36] The White House 1993: 3.
[37] Zhang–Zhou 2015.
[38] Godement et al. 2018: 2.

break China's emergence as a (cyber)power. However, there are a number of points in the relationship between the two superpowers that will leave open the question of dominance over cyberspace in the coming decades.[39] Perhaps the most important question is how the post-World War II world politics based on multilateral relations and international organisations will be transformed. Russia's military aggression against Ukraine and the annexation of sovereign Ukrainian territories by a member of the UN Security Council clearly shakes up the international order, upsets the status quo and could reinforce China's intentions to shape an international order that is fit for the 21st century, including a national shift in global (U.S.-dominated) cyberspace, helping to create a 'splinternet' of national networks. Another important issue is China's intentions in relation to Russia and Taiwan. Russia's belligerent aggression is punished by the Western world with heavy technological sanctions, so if Russia wants to keep its economy in the 21st century, it has only China to rely on. In cyberspace, Russia has been fighting U.S. dominance for decades and exploiting the leverage of technology to achieve its own ends, but its belligerence will cut it off from these opportunities for a longer period of time, both diplomatically and technically. However, it has typically moved with China in cyber diplomacy, so it is likely that intentions will not change, but will be articulated by China in the future, primarily in its own interests. Thus, Russia will in all likelihood lose its position as a cyber power and become dependent on China. The case of Taiwan is particularly important for cyberspace because it currently produces roughly two-thirds of the world's chips and although there are serious aspirations to bring some of this manufacturing capacity back to the U.S., this is only conceivable at least in a decade. Therefore, if China interferes in Taiwan's trade, either by blockade or direct military strike, it will certainly have a longer-term impact on the digital economy in the U.S. and the world as a whole, given that the production and supply of basic cyberspace infrastructure such as computers, mobile devices and networking solutions will be at stake. Apart from these three powers, there are no other actors who have a meaningful say in the shaping of cyberspace. Some regional powers, such as the European Union, are actively trying to shape the rules of cyberspace, but there is a clear sense of an East–West confrontation, led by the U.S. on one side and China and Russia on the other.

[39] Hass–Blanchette 2022.

Conclusion

This can be clearly traced within the UN, where since the early 2000s, the so-called Group of Governmental Experts (GGE) has been working on international relations in cyberspace, with a focus on the West. But in 2019, on Russia's initiative, a parallel group, the Open Ended Working Group (OEWG), was created to deal with essentially the same issues as the GGE, but with an emphasis on the East. And while of course digital transformation due to Covid-19 and the Russian–Ukrainian war are in the process of completely rewriting the balance of power in cyberspace, it is worth reviewing what the GGE 2021 report identified as the major threats along which the power relations in cyberspace will evolve over the next decade:

- "While ICTs and an increasingly digitalized and connected world provide immense opportunities for societies across the globe, the Group reaffirms that the serious ICT threats identified in previous reports persist. Incidents involving the malicious use of ICTs by States and non-State actors have increased in scope, scale, severity and sophistication. While ICT threats manifest themselves differently across regions, their effects can also be global.
- The Group underlines the assessments of the 2015 report that a number of States are developing ICT capabilities for military purposes; and that the use of ICTs in future conflicts between States is becoming more likely.
- Malicious ICT activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals.
- In addition, States and other actors are actively using more complex and sophisticated ICT capabilities for political and other purposes. Furthermore, the Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.
- Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious. Of specific concern is malicious

ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities. The Covid-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain.

- New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. Ensuring that vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes has become a serious challenge.
- Capacities to secure information systems continue to differ worldwide, as do the capacities to develop resilience, protect critical information infrastructure, identify threats and respond to them in a timely manner. These differences in capacities and resources, as well as disparities in national law, regulation and practices related to the use of ICTs, and unequal awareness of and access to existing regional and global cooperative measures available to mitigate, investigate or recover from such incidents, increase vulnerabilities and risk for all States.
- The Group reaffirms that the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.
- The Group also reaffirms that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk."[40]

[40] United Nations General Assembly 2021: 7.

Questions

1. What is the difference between classical and modern geopolitical theories?
2. Why is our perception of time, place and space changing?
3. How are ideology and strategic narrative connected?
4. What may be the geopolitical implications of the Russia–Ukraine war?
5. Why has cyberspace become the new location for geopolitical struggle?

References

Arquilla, John (2013): Twenty Years of Cyberwar. *Journal of Military Ethics,* 12(1), 80–87. Online: https://doi.org/10.1080/15027570.2013.782632

Ashworth, Lucian M. (2013): Mapping a New World: Geography and the Interwar Study of International Relations. *International Studies Quarterly,* 57(1), 138–149. Online: https://doi.org/10.1111/isqu.12060

Bolt, Paul J. – Cross, Sharyl N. (2018): *China, Russia, and Twenty-first Century Global Geopolitics.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/oso/9780198719519.001.0001

Brzezinski, Zbigniew (1997): *The Grand Chessboard. American Primacy and its Geostrategic Imperatives.* New York: Basic Books.

Diec, Joachim (2019): Major Trends in Russian Geopolitics after 1991. *Politeja,* 5(62), 141–160. Online: https://doi.org/10.12797/Politeja.16.2019.62.08

Doukas, Haris – Nikas, Alexandros (2022): Europe's Energy Crisis – Climate Community Must Speak Up. *Nature,* 608(7923), 472–472. Online: https://doi.org/10.1038/d41586-022-02199-5

Douzet, Frédérick (2014): Understanding Cyberspace with Geopolitics. *Hérodote,* (152–153), 3–21. Online: www.cairn-int.info/article-E_HER_152_0003–understanding-cyberspace-with-geopolitic.htm

Feledy, Botond – Virág, Csaba (2022): An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas,* 3(1), 12–18. Online: https://doi.org/10.1556/112.2022.00091

Flint, Colin (2006): *Introduction to Geopolitics.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203503768

Godement, François – Stanzel, Angela – Przychodniak, Marcin – Drinhausen, Katja – Knight, Adam – Kania, Elsa B. (2018): *The China Dream Goes Digital: Technology in the Age of Xi.* European Council on Foreign Relations. Online: https://ecfr.eu/publication/the_china_dream_digital_technology_in_the_age_of_xi/

Hass, Ryan – Blanchette, Jude (2022): *Central Questions in U.S.–China Relations amid Global Turbulence.* Center for Strategic and International Studies. Online: www.csis.org/analysis/central-questions-us-china-relations-amid-global-turbulence

Jowett, Garth S. – O'Donnell, Victoria J. (2015): *Propaganda and Persuasion.* Los Angeles: SAGE.

Käpylä, Juha – Aaltola, Mika (2019): Critical Infrastructure in Geostrategic Competition: Comparing the US and Chinese Silk Road Projects. In Wigell, Mikael – Scholvin, Sören – Aaltola, Mika (eds.): *Geo-economics and Power Politics in the 21st Century. The Revival of Economic Statecraft.* London – New York: Routledge, 43–60. Online: https://doi.org/10.4324/9781351172288-4

Kissinger, Henry (2014): *World Order.* New York: Penguin Press.

Kovács, László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review,* 23(1), 16–24. Online: https://doi.org/10.2478/raft-2018-0002

Kovács, László – Krasznay, Csaba (2010): A digital Mohács, egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3(1), 44–56.

Kovács, László – Krasznay, Csaba (2017a): Digitális Mohács 2.0: Kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10(1), 3–16.

Kovács, László – Krasznay, Csaba (2017b): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 10(3), 3–15.

Lanoszka, Alexander (2019): Disinformation in International Politics. *European Journal of International Security,* 4(2), 227–248. Online: https://doi.org/10.1017/eis.2019.6

Leandro, Francisco José B. S. – Duarte, Paulo Afonso B. eds. (2020): *The Belt and Road Initiative. An Old Archetype of a New Development Model.* Singapore: Palgrave Macmillan. Online: https://doi.org/10.1007/978-981-15-2564-3

Lesk, Michael (2007): The New Front Line: Estonia under Cyberassault. *IEEE Security and Privacy Magazine,* 5(4), 76–79. Online: https://doi.org/10.1109/MSP.2007.98

Mariotti, Sergio (2022): A Warning from the Russian–Ukrainian War: Avoiding a Future that Rhymes with the Past. *Journal of Industrial and Business Economics,* 49, 761–782. Online: https://doi.org/10.1007/s40812-022-00219-z

Mead, Walter R. (2014): The Return of Geopolitics: The Revenge of the Revisionist Powers. *Foreign Affairs,* 93(3), 69–79.

Mearsheimer, John J. (2013): Structural Realism. In Dunne, Tim – Kurki, Milja – Smith, Steve (eds.): *International Relations Theories. Discipline and Diversity.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/hepl/9780198814443.003.0003

Möttölä, Kari (2019): US Grand Strategy in Flux. Geo-Economics, Geopolitics, and the Liberal International Order. In Wigell, Mikael – Scholvin, Sören – Aaltola, Mika (eds.): *Geo-economics and Power Politics in the 21st Century. The Revival of Economic Statecraft.* London – New York: Routledge, 89–98. Online: https://doi.org/10.4324/9781351172288-7

Müllerson, Rein (2017): *Dawn of a New Order. Geopolitics and the Clash of Ideologies.* London – New York: I. B. Tauris. Online: https://doi.org/10.5040/9781350986022

NATO (2022a): *NATO 2022 Strategic Concept.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2022b): *Joint press conference with NATO Secretary General Jens Stoltenberg and the Prime Minister of Canada, Justin Trudeau.* Online: www.nato.int/cps/en/natohq/opinions_206908.htm?selectedLocale=en

Smith, Elliot (2022): Russia Faces "Economic Oblivion" Despite Claims of Short-Term Resilience, Economists Say. *CNBC,* 2 August 2022. Online: www.cnbc.com/2022/08/02/russia-faces-economic-oblivion-despite-short-term-resilience.html

Smith, Hanna (2023) The Geopolitics of Cyberspace and the European Union's Changing Identity. *Journal of European Integration,* 45(8), 1219–1234. Online: https://doi.org/10.1080/07036337.2023.2277329

Starr, Harvey (2013): On Geopolitics: Spaces and Places. *International Studies Quarterly,* 57(3), 433–439. Online: https://doi.org/10.1111/isqu.12090

Stoltenberg, Jens (2022): *NATO Is Stepping Up in the High North to Keep Our People Safe.* Online: www.nato.int/cps/en/natohq/opinions_206894.htm?selectedLocale=en

The White House (1993): *The National Information Infrastructure: Agenda for Action.* Online: https://clintonwhitehouse6.archives.gov/1993/09/1993-09-15-the-national-information-infrastructure-agenda-for-action.html

Treisman, Daniel ed. (2018): *The New Autocracy. Information, Politics, and Policy in Putin's Russia.* Washington, D.C.: Brookings Institution Press.

United Nations General Assembly (2021): *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* New York: United Nations General Assembly.

Walt, Stephen M. (1987): *The Origins of Alliances.* Ithaca: Cornell University Press.

Yarchi, Moran (2022): The Image War as a Significant Fighting Arena – Evidence from the Ukrainian Battle over Perceptions during the 2022 Russian Invasion. *Studies in Conflict and Terrorism,* 1–13. Online: https://doi.org/10.1080/1057610X.2022.2066525

Zaffran, Raphaël (2019): Strategic Narrative and Security. In Taylor, Bryan C. – Bean, Hamilton (eds.): *The Handbook of Communication and Security.* New York: Routledge, 354–367. Online: https://doi.org/10.4324/9781351180962-21

Zhang, Ying Ying – Zhou, Yu (2015): *The Source of Innovation in China. Highly Innovative Systems.* Houndmills: Palgrave Macmillan. Online: https://doi.org/10.1057/9781137335067

Shay Attias[1]

Home Front Resilience, Civilian Consciousness and Information Protection in the Hybrid Digital Age

Rather than focusing on the known "hard" power, this chapter offers to examine the nonviolent face of digital hybrid warfare and focuses on the home front's growing re-emergence in the digital age. Under the new media's technological capabilities, the civilian front is under constant 24/7 digital attack against their most important "currency" of our digital-information age: their "consciousness" and the "information" they must consume. Today, the "ordinary" citizens are organised worldwide through "peer-to-peer networks" that consume, produce and spread information in a way that humankind did not know before. Therefore, the fear of harm and greater fragility than in previous eras rises in the hybrid era in which the outside is mixed with the inside, blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one dimension. The civilian front of every country is under attack, even if not during a declared "war". In contrast to older times, today's citizens know a greater power to exert pressure on the decision-makers and the military. Thus, while utilising Russia's test case, this textbook chapter sheds light on the importance of strengthening the digital consciousness of citizens in the hybrid era in which "war" is becoming increasingly constant, vague and very difficult to define. My conclusions will benefit both the bodies entrusted with strengthening "national resilience" and contribute to the military practitioners involved in the field of diplomacy and consciousness. In addition, it will allow policymakers to understand the greatness of the challenge. "The fear of harm and greater fragility than in previous eras rises in the hybrid era in which the outside is mixed with the inside, blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one."[2] Since the beginning of the 2000s, more and more voices have been heard among

[1] Bar-Ilan University.

[2] Wassermann 2018: 16.

DOI: https://doi.org/10.36250/01236_11

military practitioners and war studies scholars who refer to the current ongoing wars and conflicts as belonging to a "new" era entitled "hybrid warfare", but is it a new concept? "Hybrid warfare", in the contemporary era, became increasingly popular in policy debates following two critical developments. First, in 2005, two U.S. military officials wrote about the "rise of hybrid wars" and emphasised the combination of conventional and unconventional strategies, methods and tactics in contemporary warfare and the psychological or information-related aspects of modern conflicts.[3] Second, Russia invaded Crimea in 2014 and achieved its objectives by conflating "deniable" special forces, local armed actors, economic clout, disinformation and exploiting socio-political polarisation in Ukraine. Hybrid warfare remains a contested concept, and no universally agreed definition exists. It has been criticised for lacking conceptual clarity, being merely a catch-all phrase or a buzzword, and not bringing anything distinctly new to policy debates. Nevertheless, the concept furnishes critical insights into contemporary and future security and defence challenges.[4] However, before this chapter deals thoroughly with this critical question, we suggest a more needed evolutionary perspective. Instead of looking only at this question, we will delve deeper into the changes that have taken place in the international digital arena and the way interactions are made or become "hybrid", which requires a profound rethinking. First, the core of this chapter will not focus on changing military tactics of "command and control". However, it will emphasise the importance of the increasingly double-edged sword: the rising global and local need for information consumption and production by the "home front", and becoming a more convenient target for manipulations, disinformation, and fake news which according to Iranian agents in Israel, can lead to "Dystopia". In other words, as the dependence on information gluttony increases, so will the weakness and fragility of the "civil world" to defend itself against the defacement of its consciousness by the enemy's army. Second, this guiding textbook piece is to demonstrate and explore more about the complicated "military–society relations during the war in the digital hybrid age". This matter has become a major strategic issue discussed thoroughly in every command headquarters in modern armies. However, there have never been so many psychological and information technology available tools to re-engineer the enemy's and public's minds and hearts as today. Yes, the use of propaganda is ancient, but social media and other digital faking tools

[3] Hoffman 2007: 8.

[4] Weissman 2019; Hourcade et al. 2006.

enable unprecedented capabilities. Therefore, the civilian element, the "soft underbelly" of every country and its army is now at the forefront of the war for consciousness, which has many faces.

Soft war and home front

All ancient-historical, modern and now so-called "hybrid" war contains two essential components: one, a "hard" brutal element which is the bayonet, the sword, the rifle or the tank that fires, and another one, a "soft" one uncovered in the "nonviolent" face of war, which has been previously known as psychology warfare or more recently, consciousness re-engineering. The "soft" world of consciousness and the "nonviolent side" of wars clearly indicate a fast notice of the essential "currency" of our digital age: "information" has dramatically changed. Not for nothing, policymakers and commanders named the rush for information "the blood life", which every government and army desired to control. The mass media revolution at the beginning of the last century and, since its end, the global media revolution and the rise of global news networks known as the "CNN effect"[5] have both increased the demand for information and decreased the ability to control it. Nevertheless, since the Millennium, social media giants have broken into our lives and created abundant faces for information technology, making it a different level to explore. Since the social-digital age, the international arena has enabled far-reaching digital capabilities to be created. Above all, the simple and fast way of global interactions has made our world much more global and flatter. With these digital changes, human wars, which also include significant struggles in "soft power" areas, are affected[6] by the ability to communicate with any person at any point in the world, wholly erasing the element of space and time. Now, the "ordinary citizens" know much more about what is happening and consume information about their country and others beyond physical borders, bypassing almost every obstacle. New technological capabilities allow a two-way communication and multi-dimensional feedback to governmental or military entities. Citizens worldwide demand to know more consistently, and they use social and traditional media to generate intense international pressure that can bring the country to change its policy. This "power shift" to the citizens over

[5] Jakobsen 2000.

[6] Bjola–Holmes 2015; Adesina 2017; Attias 2012; Hallams 2010.

states is connected to an ideological revolution of "global citizenship" or "cosmopolitanism" and the "power transition" concepts.[7] Both theories lie in the thought that citizens can have a universal influence without national affiliation and promote common goals. Adding to their new social media capabilities, they were later called "digital civic networks" or "peer-to-peer networks". In other words, two trends here affect a third one: conceptual and technological, which have come together and created a kind of "mutation" of digital citizens formed as global networks that create a challenging "front" to any army that tries to defeat its opponent. These human networks can influence armies and countries before, during and after the war. They consume astronomical amounts of information and react so quickly that sometimes they are ahead of politicians or even army commanders during conflicts. Oxymoronically, the more information consumed by the citizens of our digital age world, the more vulnerable they become to misinformation. However, not only do the citizens become more sensitive but also armies and state bodies invest more and more money and effort in public diplomacy to improve "how the world sees them" and "what others think of them"; "which story they tell the world"; and how much "legitimisation" do they have for their military activities. Therefore, the social media age contains much more mental and psychological elements than before, which only amplifies the complexity of the relationship between society and the armed forces. The so-called "home front" or "civilian front" are definitions that include the totality of all actions involving civilians during wartime. World War II was a much more "total war" than its predecessors in that the defence of the home front became as important as the offensive military power or the ability to create coalitions and alliances during a world war.[8] Slowly, more and more governments began to understand the great importance of the civilian front and, since then, began to establish more units and bodies responsible for the "national resilience" of the country's citizens in times of war. With the thinking adopted to achieve "maximum civilian protection", experts and scholars began to understand that the civilian front differs from the military and includes much more psychological, communicative and cognitive elements than those in the military field. Looking through the citizen's prism, during an emergency of a war, citizens have a double challenge: on the one hand, the army of their country asks for their "national resilience" in order to support the continuation of the fighting until the goals are achieved, and on the other hand, the citizens

[7] Chan 2007; Nye 2010.
[8] Storey–Kay 2017.

are subjected to psychological and informational attacks that range from ancient psychological warfare to sophisticated digital methods that are available today: public diplomacy, fake news, fake social media accounts, interfering in elections, harming the nation's legitimacy and reputation, activation and creation of protests within the citizens of the rival country and more.[9] Special attention must be given to the fake news industry, which has vastly grown and has become more sophisticated and challenging to detect. The military is forced to act increasingly in the arena of consciousness so that the enemy does not damage national resilience and spread harmful rumours. While in the previous ages of modern war (particularly in WW2), civilians were required to nationalise their products and help provide eggs, clothes and cars to the army, in the hybrid digital era, they are asked to carry out unclear orders such as "protect the mind", and "do not believe fake news", help to strengthen the national and army's legitimacy and more recent requests that are hard to understand and measure. The already known principle that war causes severe disruption in the functioning of the "home" has been redesigned into a disruption in the consciousness that is waged 365 days a year and sometimes even several times in a minute.[10] Therefore, in the digital age in which most of the world is connected to almost any source of information, the civilian front becomes constantly threatened at any given moment. On the other hand, at any given moment, any citizen can consume false information. Another change that probably pinpointed the digital hybrid era is the final blurring boundaries between the "real" and the "virtual" and "domestic" and "external", which all coalesced into one dimension.[11] Hence, and since the last decade, it is not surprising that the concept of national security has changed and evolved into more non-typical military and nonviolent topics in recent years.

National security in the age of heredity

Before the digital age, national security was defined using mainly military concepts.[12] The relationship between the traditional national security concept and the army's operational concept was based on three legs: deterrence, warning and decision. Over the years, the concept was adapted to the security challenges that

[9] Monsees 2020; Haigh et al. 2019.
[10] Bachmann et al. 2020.
[11] Jordan 2009.
[12] Lebel 2010.

developed following the attacks on the home front using long-range weapons and suicide terrorism, and the fourth leg – defence (or defensiveness) – was explicitly defined. Over the years, defence has gradually taken an increasingly central place in security concepts because the home front has become the enemy's main front of action trying to harm the civilian population in various ways.[13] This "old–new" situation has emerged in which the readiness of the home front plays a decisive role in the decision-making process: the more heightened readiness of the home front, the greater the flexibility of the decision-making process in the activation of the military response. That is why this issue was defined as one of the defensive efforts of many armies. For example, the Israel Defense Forces announced that the intelligence assessments state that "widespread shooting against the civilian population will be a central tool in shaping the future characteristics of the next war". At the same time, the importance of preparing the home front against a missile and rocket attack to save lives remains the same. The "quality of the functioning of the civilian" becomes more critical in building natural resilience. One concept that describes this cruciality, "Casualty Panic", has recently impacted military policy, mainly "in liberal democratic states". With the growing public opinion and social media, the hesitation to enter into military engagements for fear of incurring casualties is a consequence of "moral panic" among the political and military leadership. This concept draws a solid and active connection between civil and military relationships through "Casualty Panic", which can influence military strategy and tactics.[14] But as for all the world countries, "hard power" threat is not the only one for Israelis or for other nations. One of the many examples was in 2014 when, as part of Hamas's efforts to sow panic and fear, threatening text messages[15] were sent with false information about a rocket hitting the petrochemical plant in Haifa and the death of dozens of Israelis. In what appears to be part of Hamas's psychological warfare efforts, the message reads in English: "Now: 25 Israelis have been killed by a missile strike in Haifa"; "a rocket from Gaza hit the petrochemical plant in Haifa"; "large fire, a possibility of a chemical leak, it is recommended to evacuate Haifa".[16]

[13] For example, in the "low intensity conflict" and army operations over the years, the residents of the State of Israel were subjected to a heavy and prolonged attack of rockets and missiles. According to the IDF's attribution threat, in a future conflict thousands of missiles are expected to be fired at the civilian home of the State of Israel by hostile countries and elements for several days to weeks.

[14] Lebel 2010: 183.

[15] Orpaz – Siman-Tov 2021.

[16] Bender 2014.

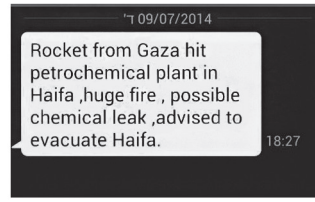

Figure 1: Fake Hamas message (originally in English) claims Haifa chemical plant hit by Gaza rocket
Source: Bender 2014

Figure 2: Fake Hamas message (originally in Hebrew):
"ישראל מתחת לאש, והכריח את כל הישראלים להיכנס למקלטים. אנחנו נמשיך בהפצצת כל מקום בישראל עד שיענו כל תנאינו הלגיטימיים בחיוב מוחלט. גדודי עיז אדין אקסאם" (השגיאות במקור)"

In English:
"The foolishness of your leaders has put all of Israel under fire, forcing all Israelis into shelters. We will continue bombing every place in Israel until all of our legitimate demands are fully met. Izz ad-Din al-Qassam Brigades" (original errors retained).
Source: Ynet 2014

That was not the first time that Hamas has sent messages to Israelis to sow fear and panic in the public. Messages of this type were sent during the "Pillar of Cloud" operation initiated by the IDF against Hamas in November 2012. The terrorist organisation then sent similar messages to Israeli citizens, with the aim of threatening the civilian population and disrupting their daily lives. Even if the Hebrew language skills of Hamas agents remain poor, it seems that the technological capabilities of the organisation have improved. The text messages sent in the "Pillar of Cloud" operation were from random cell phone numbers, their content was fragmented, they were written in unintelligible Hebrew and

were sent to the Western and Southern Negev regions. The level of sophistication of Hamas has increased and to increase their credibility and create fear among tourists, the messages were sent in English, all over Israel, using the number of the "Haaretz" newspaper. We can draw two significant conclusions from these hybrid changes: Firstly, states face challenges in controlling information and shaping narratives, thereby impacting the legitimacy of their actions. Secondly, the effectiveness of lethal force strategies in achieving strategic goals is weakened. It is important to acknowledge that the use of lethal force often carries political consequences for state armies, leading many to avoid such measures. Consequently, in addition to the aspiration to develop non-military tools of influence encompassing ideology, culture and economics, the concept of "soft power" has gained prominence in the West. It serves as the foundation for the security and foreign policies of numerous powers and countries. The concept of "soft power" refers to the ability to persuade others to act as you wish without using physical force and was based on the use of non-lethal resources and abilities, such as: economic, legal, diplomatic, cultural and ideological.[17] The components of "national power" encompass diplomacy, information, military and economic factors. While the military is typically considered a measure of last resort, particularly in Western democracies, the United States military has consistently played a crucial role in various aspects of soft power. This includes advancing democracy and strengthening partner nations through military-to-military relationships. These cooperative efforts are manifested through bilateral and trilateral exercises, which aim to support established Operation Plans, NATO, the United Nations and Theater Security Cooperation. Through active engagement in these activities, the U.S. military significantly contributes to the promotion of global stability and security. Through these efforts, among others, the U.S. military helps to carry out the diplomatic mission of the United States (military diplomacy paved the way for NATO, the European Union, and the World Trade Organization, for instance).[18] In the context of military-diplomatic matters, when military units engage in bilateral or multilateral exercises with other countries, there are multiple objectives at play. These exercises aim to enhance interoperability between the participating militaries, foster cultural exchange and understanding, and provide an opportunity to develop and test capabilities in the context of potential contingencies. The significance of military diplomacy

[17] Nye 1990.
[18] Ebitz 2019.

in foreign engagements lies in its ability to establish dialogue that can facilitate ongoing communication and, importantly, prevent misunderstandings between different cultures during times of crisis. By engaging in these activities, nations can strengthen their relationships and promote clearer communication channels, thus enhancing overall international cooperation. Moreover, in places where the U.S. military has maintained a long-term presence (e.g. Japan, South Korea, Germany), we see that military interoperability enhances regions economically – directly through commercial contracting and the resulting employment, service member contributions through commerce, and in some cases, contributions of military gear and equipment through foreign military sales or otherwise.[19] In the era of hybrid digital warfare, the dissemination of false information poses a significant threat, potentially leading to paralysis in safeguarding the civilian home front. Consequently, it becomes crucial for armies to foster strong multinational cooperation with other nations to effectively counter this threat. One essential component is the establishment of a capable Home Front Command, responsible for managing, disseminating and protecting critical information during times of combat and emergencies. The primary objective is to enhance national resilience by providing reliable information, a sought-after goal for any hybrid attack. Additionally, the Home Front Command aims to save lives by preparing the civilian population for the possibility of conflict, providing support during rescue operations and advocating for the protection of the home front. Furthermore, post-conflict, the Command assists in the swift rehabilitation of the civilian home front, contributing to its recovery and stability. During ordinary times, the Home Front Command plays a crucial role in providing guidance to the population on emergency protocols. It coordinates with local authorities, government ministries and infrastructure entities to ensure their effective response in civil defence emergencies. In times of crisis, the Home Front Command activates the rescue and recovery system, issues warnings to residents in the face of imminent threats, provides instructions on how to respond and assists local authorities and government ministries in carrying out their emergency civil defence duties. Ultimately, the responsibility for individual and family preparedness in emergencies lies with the citizens themselves. It is vital for them to access and consume reliable and accurate information. The "hybrid" nature of ambiguity and deniability, which can potentially be exploited by certain actors like Russia, poses a risk of reaching the threshold of Article 5 without actually triggering it. This situation has the potential to disrupt institutional and

[19] Gilman et al. 2014.

political mechanisms of collective defence. The 'hybrid' qualities of ambiguity and deniability – which, it is feared, would be manipulated by Russia to come close to the "Article 5" threshold but never reaching it – can paralyse the institutional and political mechanisms of collective defence.[20] Therefore, due to the lack of a universally agreed-upon definition of hybrid aggression, any discussion on this matter within the North Atlantic Council would be highly politicised, time-consuming and subjective. Even if there were a more precise and formalised specification of an automatic trigger for a collective response, such as the suggestion by former NATO SACEUR Phillip Breedlove of attributing "infiltration of foreign forces on sovereign territory" to account for instances like the presence of unidentified troops (referred to as "little green men"), it would not necessarily resolve the problem. In fact, the clearer the threshold, the easier it becomes for Russia or any other potential aggressor to tailor their actions to stay just below it. Recognising these gaps in Article 5, which could be exploited by hybrid aggressors and lack obvious solutions, NATO leaders in Warsaw assigned the primary responsibility for protection against hybrid threats to individual member states. However, the final Communique also emphasised that the Alliance and Allies will be prepared to counter hybrid warfare as part of collective defence; and "the Council could decide to invoke Article 5".[21]

National resilience

Improving resilience against the exploitation of Western societies by politically competing or potentially hostile actors is a crucial aspect that needs to be addressed. While it is evident that Russia is involved in such activities, including propaganda, funding populist parties across the political spectrum, and undermining established governing institutions and actors, the challenge lies in determining how to effectively respond. Below are some potential approaches to enhancing resilience:

1. Strengthening democratic institutions: Focus on reinforcing the transparency, accountability and integrity of democratic institutions. This includes promoting strong electoral systems, combating corruption and ensuring independent media.

[20] NATO 2023.
[21] NATO 2023.

2. Enhancing digital literacy: Invest in educating the public about critical thinking, media literacy and online security. By fostering a population equipped with the skills to discern reliable information from disinformation, societies can become more resilient to manipulative tactics.
3. Promoting social cohesion: Foster inclusive societies that value diversity and promote social cohesion. By building strong community bonds and promoting dialogue across different social and political groups, societies can mitigate divisions that can be exploited by external actors.
4. Strengthening cybersecurity: Recognise the importance of robust cybersecurity measures to protect critical infrastructure, government systems and private data. Enhancing cybersecurity capabilities and fostering cooperation among governments, the private sector and civil society is vital in countering hybrid threats.
5. International cooperation: Foster collaboration among like-minded nations to share best practices, intelligence and lessons learned in countering hybrid threats. By working together, countries can build a united front against actors seeking to exploit vulnerabilities.

Addressing the question of what should be resilient, defended, protected and strengthened in Western societies is a highly political matter that requires careful consideration. It is crucial not to leave these decisions solely in the hands of security or military experts, or to be driven by the logic of warfare.

While some argue for approaches such as strengthening national resilience around homogenous ethnic communities or resorting to economic nationalism and protectionism to address challenges posed by Russia, these strategies do not provide comprehensive security for Western societies. In fact, they often exacerbate political contestation and inadvertently play into the strengths of aspiring Great Powers like Russia. A more effective strategy lies in bolstering the resilience of liberal modes of government and societal organisation, rooted in democratic principles, fundamental rights, the rule of law and economic openness. It is important to draw from the lessons learned through successful domestication of foreign policy within the EU and its member states when seeking to protect perceived interests and confront hybrid threats. Discussions surrounding the European Global Strategy and EU foreign policy emphasise the significance of upholding a rules-based international order that supports values-based multilateral actors, moving beyond a narrow pursuit of self-interests or reverting to power politics. It is essential to navigate the changing geopolitical landscape while

maintaining the resilience of this approach, particularly in the face of hybrid threats and challenges. Moreover, media plays a vital role in building resilience. Cultivating a diverse and independent media landscape that promotes accuracy, reliability, critical thinking and media literacy is crucial. Media outlets should uphold democratic values, provide platforms for informed public discourse and actively counter disinformation campaigns. Investing in media resilience contributes significantly to the overall resilience of societies in countering hybrid threats.[22] Resilience is mainly about how states and societies resist collapse due to disastrous events. They must cope and deal with such events, adapt to them and recover from their effects in a short period. Post-facto resilience is only possible if the state and the society can anticipate the potential consequences of a series of events, be it man-made, a natural disaster, or an external challenge, like a crisis or war. Consequently, resilience is contextual; it has many forms depending upon the informational context.[23] Resilience has much to do with state capacity, governance and cohesion, and thus the support of society for its state institutions and leaders. Hence, it would be easy to conclude that so many factors contribute to resilience that it would be best to identify the concept with good governance. However, this would be a gross simplification as resilience must be developed in anticipation of scenarios that are likely to occur. This harks back to resilience in those areas from whence the challenge comes. This is not very easy to the perceptional foundations of analysis, including those problems that are of low likelihood. However, the exceptionally high risk (e.g. a nuclear attack or a significant reactor accident) cannot be ignored. No state has unlimited resources. Hence, the priority areas must be backed by resource allocation. It also may be easier said than done as there is rivalry for resources on the national agenda. Furthermore, due to various factors, some states – irrespective of their national efforts – cannot become resilient against specific concentrated, high-intensity challenges. In many cases, the public relies on a combination of formal and informal information sources, with social media often playing a role in sharing links from government websites that are deemed helpful to communities. This process not only acts as a filter for information but also amplifies the dissemination of "official" information. This chapter explores how social media, leveraging its strengths in timely information exchange and connectivity, can serve as a source of psychological first aid during the early stages of a disaster and contribute

[22] Dunay–Roloff 2017.
[23] Humprecht et al. 2020; DeWit et al. 2020.

to community resilience. A robust and healthy media landscape demonstrates resilience and adaptability to the dynamic and ever-changing social, political and economic conditions within its context. In functioning democracies, both state and non-state actors rely on strong, independent and sustainable media organisations to access reliable news and information services. These organisations also play a critical role in facilitating open debate and dialogue among various stakeholders. By upholding the principles of independence and sustainability, the media can effectively respond to the needs of the society it serves. This entails remaining responsive to the evolving media landscape and adapting to new technologies and communication channels. A resilient media landscape is one that can effectively navigate the complexities of its environment, ensuring the availability of credible information and fostering an environment conducive to open discussions and informed decision-making.[24] Recent studies keep showing more and more that social media has become a primary instrument of hybrid warfare to shape public opinion and to see its impact on different bodies of state.[25] The 21st century dawned alongside an emerging form of warfare that, in its nature and character, is remarkably diverse and whose scope extends beyond conventional elements of war. In polarised political environments, citizens are confronted with different deviating representations of reality, making it increasingly difficult to distinguish between false and correct information. Thus, *societal polarisation* is likely to decrease resilience to online disinformation. Moreover, research has shown that *populism* and partisan disinformation share a binary Manichaean worldview, comprising anti-elitism, mistrust of expert knowledge and a belief in conspiracy theories. Due to these combined influences, citizens can obtain inaccurate perceptions of reality. Thus, online users are exposed to more disinformation in environments with high levels of populist communication.[26] Previous research has consistently highlighted the crucial role of trust in news media as a determining factor for resilience against online disinformation. When there is a higher level of distrust in news media, individuals tend to be less exposed to diverse sources of political information and are less likely to critically evaluate the information they encounter. Furthermore, people's level of knowledge about public affairs plays a significant role in their ability to navigate online disinformation. Studies have shown that countries with strong public

[24] Hook–Verdeja 2022.
[25] Svetoka 2016; Ducaru 2016.
[26] Humprecht et al. 2020.

service media tend to have citizens with higher knowledge levels compared to countries where public service media is marginalised or weakened. Consequently, it can be inferred that environments with weakened public broadcasting services (PBS) are less resilient in the face of online disinformation. Trust in news media and individuals' knowledge about public affairs are closely intertwined with resilience to online disinformation. When trust is diminished, individuals are less inclined to seek out diverse information sources and critically analyse the information they come across. Moreover, the erosion of public service media environments can undermine citizens' knowledge levels and further exacerbate vulnerability to online disinformation.[27]

Increasing global synergies and awareness

As the focus is on improving awareness, it is proposed to establish dedicated mechanisms to exchange information with Member States and to coordinate the EU's capacity to deliver strategic communications. An EU Hybrid Fusion Cell within the EU Intelligence and Situation Centre[28] of the European External Action Service (EEAS) will offer a single focus for the analysis of external aspects of hybrid threats. The Fusion Cell will receive, analyse and share classified and open-source information from different stakeholders within the EEAS, the Commission and Member States specifically relating to indicators and warnings concerning hybrid threats. In liaison with relevant bodies at the EU and at national level, the Fusion Cell would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level. The Cell would enhance awareness and provide inputs to security risk assessment processes which support policymaking at national and EU levels.[29] As announced in the European Agenda on Security, the Commission facilitates common assessments of security risks in a variety of policy areas like transport security (in particular aviation), anti-money laundering and terrorism financing,

[27] Humprecht et al. 2020.
[28] Voronova–Bakowski 2022.
[29] Davies 2021.

border control, etc. One notable example of a significant initiative in countering various threats, including disinformation, is the establishment of "The Joint Framework Program".[30] Introduced on 6 April 2016, this program outlines proposals aimed at building resilience in key areas such as cybersecurity, critical infrastructure protection, combating illicit use of the financial system and addressing violent extremism and radicalisation. A crucial initial step in implementing these proposals involves the EU and its Member States adopting agreed strategies and fully implementing existing legislation. This ensures a coordinated and unified approach towards enhancing resilience against these threats. Moreover, concrete proposals have been put forward to further strengthen these efforts, indicating a commitment to continuous improvement and adaptation. While the Joint Framework Program is primarily focused on addressing the complex challenges posed by hybrid threats, it is pertinent to recognise that EU action extends beyond the mere countering of hybrid threats. The program's ambit encompasses a wider range of objectives, showcasing the EU's comprehensive approach to safeguarding its member states and societies from an extensive array of risks and challenges. By encompassing domains such as cybersecurity, critical infrastructure protection, financial system integrity and counter extremism, the Joint Framework Program exemplifies a multifaceted approach to resilience-building. This proactive stance underscores the EU's unwavering commitment to effectively confront not only disinformation but also other pressing threats that possess the capacity to undermine security, stability and societal well-being. These joint assessments at EU level provide a comprehensive analysis of the threats, consequences and vulnerabilities to support policymaking with a view to mitigate the risks. The Commission facilitates these processes with the participation of Member States' experts and other EU services. The assessments of hybrid threats, produced by the EU Hybrid Fusion Cell, will provide relevant input to feed risk assessments at the EU and national levels.[31] Critical vulnerabilities may differ from Member State to Member State, as do levels of protection ensured nationally. Nonetheless, there exist numerous sectors characterised by a significant reliance on critical services, rendering countries and societies particularly vulnerable to hybrid threats. These sectors encompass energy security and supply, space

[30] European Commission 2016.
[31] Kert-Saint Aubyn 2016.

infrastructure, maritime security, public health, transportation (including aviation, maritime and rail), cybersecurity, communications and financial systems. Hybrid threats have the capacity to exploit vulnerabilities within societies, thereby posing challenges to fundamental values and liberties or targeting marginalised groups. Adopting a comprehensive and interconnected approach to counter hybrid threats can bolster the security and resilience of each of these sectors. By adopting a "joined-up" strategy, these sectors can enhance their ability to withstand and mitigate the impacts of hybrid threats, promoting overall security and societal well-being.

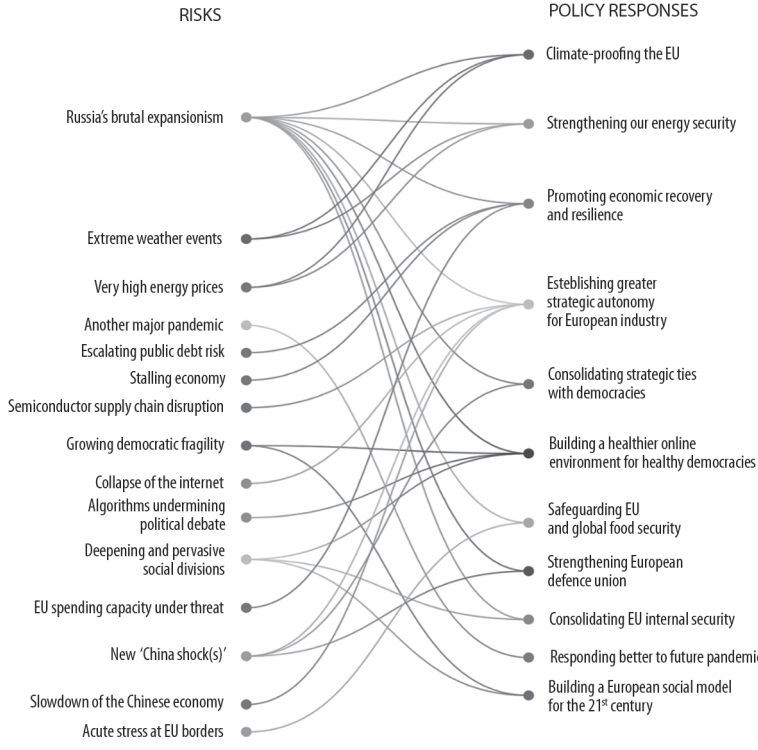

Figure 3: EU security landscape
Source: Voronova–Bakowski 2022

"In a rapidly changing and increasingly interconnected world, the EU security landscape has become very complex and unpredictable."[32]

What is the "mutual defence clause"[33] and is it relevant in this context? According to Article 42(7) of the Treaty of the European Union (TEU): "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations charter."[34] If multiple serious "hybrid threats" constitute armed aggression against an EU Member State, this mutual assistance clause could be invoked to provide an appropriate and timely response. It does not require Member States to take military action, but Member States are required to provide aid and assistance, providing that it shall not prejudice the specific character of the security and defence policy of certain Member States. However, the challenge is that many of the nonviolent hybrid threats are hard to define so can one demand to activate this article if its citizens were misinformed? Or had a special media attack by sophisticated bots?[35] One of the offered responses was "The IPCR arrangements"[36] that were adopted by the Council of the European Union on 25 June 2013 to reinforce the EU's ability to take rapid actions when facing major crises requiring a common response. The IPCR arrangements are flexible and scalable, enabling a tailored response and providing the necessary support from EU institutions and services in the context of a crisis and its evolution. They make full use of synergies between stakeholders and existing resources, structures and capabilities. They do not replace existing instruments and arrangements at sectorial level. The Commission and the EEAS contribute notably by producing regular Integrated Situational Awareness and Analysis (ISAA) reports to inform decision-making. IPCR has been activated by the Presidency of the Council for the first time in October 2015 to respond to the migration and refugee crisis. IPCR arrangements support the implementation of Article 222 of the Treaty on the Functioning the European Union.[37] Based on the IPCR, the EU will make best use of its cooperation with partner countries,

[32] Voronova–Bakowski 2022.
[33] Solidarity clause.
[34] See www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf
[35] Orabi et al. 2020.
[36] Council of the European Union 2016.
[37] Osula 2014.

including with its immediate neighbours, in countering hybrid threats. Through its external assistance, the EU will continue to strengthen its partners' national capacities in the fight against organised crime, terrorism and illegal trafficking, including in the field of border management. Further, the EU will pay specific attention to protection of critical infrastructure and develop actions to enhance cyber resilience which would ultimately contribute to countering hybrid threats in third countries. The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and "crisis prevention and response" to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation's decision-making process.[38] The actions proposed require cooperation and coordination of all relevant actors at EU and national level. Some of the proposed actions come under the responsibility of Member States, others require implementation by Member States. The EU can provide support and advice as required, including through best practices. The actions proposed in the Joint Frameworks and their implementations will be discussed in the Council of the European Union. The proposals will also be discussed by the European Parliament.[39] Private initiatives, such as specialised websites like Stopfake.org, have proven to be more effective in recognising disinformation compared to many public agencies. These initiatives relieve governments of the burden of building their own capacities. However, the number of private initiatives in this field remains limited. It is in the interest of NATO countries to systematically develop their private capacity by providing grants through the alliance and other international entities focused on security issues. Financial support should not be limited to public diplomacy but should also cover analysis. By building a network of experts, both NATO and individual allies can enhance their resilience to hybrid challenges. Hybrid warfare encompasses a range of activities and employs different instruments to destabilise societies by influencing their decision-making processes. To strengthen society against these threats, the author proposes the following actions:

1. Interference in electoral processes: Adversaries may employ various techniques, including media campaigns, social network manipulation and securing financial resources for favoured political groups, to influence election outcomes in their favour.

[38] NATO 2016.

[39] European Commission 2016.

2. Disinformation and false news: Adversaries can create and propagate a parallel reality by spreading false information, leading to social fragmentation. This disorientation makes it challenging for governments to garner public support for NATO policies or operations.
3. Cyberattacks: Adversaries can exert pressure on NATO governments by threatening with devastating cyberattacks targeted at civilian infrastructure such as hospitals, electricity grids, or water supplies. These attacks aim to discourage mutual assistance among NATO members during times of crisis.
4. Financial influence: Adversaries can exert long-term political pressure by making investments, establishing unfavourable energy supply agreements, or offering loans that render a country vulnerable to manipulation.

Addressing these challenges requires a comprehensive approach that involves countering disinformation, enhancing cybersecurity, and safeguarding financial and energy sectors. By taking proactive measures and strengthening societal resilience, NATO countries can effectively respond to hybrid threats and maintain their security and sovereignty.

Can public diplomacy help against hybrid warfare?

One available tool for any country is public diplomacy. Through transparency and open engagement, public diplomacy can counter the perception of government propaganda and bridge the trust gap. By demonstrating accountability, actively listening to public concerns and addressing them genuinely, public diplomacy can foster a sense of trust and credibility among the public. This, in turn, strengthens the effectiveness of public diplomacy in countering hybrid threats, as trust is crucial for the public to perceive and evaluate the information provided by governments. However, in the age of social media, the biggest problem of traditional public diplomacy was that, for years, it was perceived as government propaganda. Government information was treated with scepticism, as it was considered both inauthentic and unreliable. Governments would often say what they wanted people to believe, and never admitted any policy failure, thus affecting their credibility and making it hard for the public to believe them. Today, the world's citizens capture the power to administer information. People across the globe are increasingly connected. The internet is the common denominator that connects people of different cultures, languages and nations. The combination of endless

social media platforms has created the phenomenon of so-called "peer-to-peer (P2P) diplomacy", also called Peer-2-Peer diplomacy.[40] Every citizen with direct internet access can receive news instantaneously and become an entire "walking news system", analysing information, commenting upon it and distributing it to their peers. As a result, governments want to harness new social media platforms to promote their policies and diplomatic efforts. Nevertheless, governments lack both resources (financial, human and structural) and credibility. However, it seems that there is still a role for governments to play in P2P diplomacy. Governments that can harness the communication potential of their citizens will be the ones to conduct effective public diplomacy offensives. Therefore, this new model of P2P public diplomacy consists of the public – meaning the citizens – not only carrying the message but, more importantly, shaping it.[41] Generally, governments are at a disadvantage when adapting to new media and technology. New media and technology move very quickly and change how people communicate, operate and live their lives. Governments, meanwhile, move slowly. While the big fish had a distinctive advantage in the old diplomacy model, the fast, adaptable fish had a clear advantage in the new public diplomacy model. The age in which we live promotes self-expression and enables unlimited technological capabilities. Therefore, the rise of "civilian power"[42] is not limited to the public diplomacy field; it is a multi-disciplinary phenomenon and hence, there are limitations and future challenges to effective diplomacy especially in this hybrid age in which it is most needed:

- The "civilianisation" of the government's public diplomacy platform has demands: legal, financial and bureaucratic changes must occur to collaborate with civilians and diasporas.
- The government must realise that it cannot control the message these people will carry; in other words, it must cede control and accept critical voices as part of the project.
- The government must reorganise this new relationship between the state and its citizens (not as a condition). The civilian society can empower the state, which maintains the relevance of the national state through mutual collaboration.

[40] Attias 2012.
[41] Jun Ayhan 2020.
[42] Clinton 2010.

– Public diplomacy efforts by the government can only be practical if they are based on civilian determination.[43]

Conclusion

The current management and regulation of social networks often facilitate the rapid spread of disinformation. While regulation falls outside NATO's jurisdiction, the alliance can advocate for sensible legislation that enhances the resilience of social networks against abuse. This can include measures to improve the identification of false profiles and strengthen penalties for hate speech. However, the most effective weapon against disinformation lies in professional journalism. NATO and its member states should invest more in investigative journalism to provide credible alternatives to false news. Surveys indicate that approximately 70% of media references to "hybrid threats" are inaccurate.[44] NATO can contribute by supporting the development of journalists' expertise in adequately covering and monitoring this issue. Educated and informed media serve as vital partners in raising social awareness and educating citizens about coping with various forms of hybrid pressures. NATO can provide training and lead campaigns to enhance awareness of hybrid challenges, thereby bolstering local media capabilities in this domain. Election interference has long been utilised as a foreign policy tool by state actors, but it has gained greater prominence due to Russia's attempts to influence the 2016 U.S. presidential election. Existing scholarship on election interference primarily focuses on its role in promoting specific candidates or parties. However, the concept of hybrid warfare offers a powerful alternative framework for understanding election interference. Hybrid warfare theory recognises that modern conflicts are characterised by the coordinated use of diverse tactics. By adopting this perspective, NATO can gain deeper insights into the complexities of election interference and develop more effective strategies to address this hybrid threat.[45] Examining the 2016 American presidential election, the 2018 Taiwanese local elections and the 2016 Brexit referendum reveals that election interference caused an intensification of internal

[43] Clinton 2010.
[44] Treverton et al. 2020.
[45] Davies 2021.

divisions in all three countries where it occurred. In each case, external actors attempted to manipulate the electoral outcomes, exploit societal divides and fuel polarisation within the respective societies. These interference attempts deepened existing tensions, eroded trust in democratic processes and undermined social cohesion. By leveraging disinformation campaigns, targeted messaging and hacking activities, external actors exacerbated internal divisions and weakened the fabric of these nations' democratic systems. Safeguarding elections from interference, promoting transparency, countering disinformation and enhancing cybersecurity are crucial measures in mitigating the negative impact of interference and fostering a more cohesive democratic environment.[46] Election interference is conceptualised as "a tool of hybrid warfare which can be used to undermine the strength and legitimacy of a target state".[47] It is ideally suited to this role thanks to its potential deniability, inexpensive nature, and effectiveness at exploiting internal divisions within target states. Moreover, modern technologies such as social media, the internet and even artificial intelligence facilitate election interference by making it easier than ever before to create and disseminate disinformation. Deterrence of election interference is very difficult because it does not conform to traditional concepts of warfare. Not all election interference can be classified as hybrid warfare. However, intervention in a state's democratic processes can be a key component of such aggression because of its ability to undermine the foundations of a target's government, society and popular legitimacy. Given that hybrid warfare breaks down the distinction between civilian and military domains, many experts have expressed concern that hybrid attacks might profoundly affect domestic politics in eastern Europe and examined the lessons that can be learned from their experiences, since at least 2007, Russia has pursued an "all out, mainly convert, political war on the west".[48] This operation has relied on information warfare and hacking, which afford Russia a degree of plausible deniability. Russia's intervention in the 2016 U.S. presidential election can be seen as a firm clash in this continuing hybrid assault on western countries.[49]

[46] Davies 2021.
[47] Wither 2016.
[48] Orenstein 2022.
[49] Babiracki 2018.

Questions

1. What are the emerging forms of nonviolent digital hybrid warfare tactics in today's landscape?
2. What are the prominent threats posed by misinformation and fake news in the hybrid era, and what are the potential negative consequences they can bring?
3. How has the Russian–Ukraine case study contributed to our understanding of the evolving forms and definitions of hybrid warfare?
4. What is the concept of national resilience, why is it crucial in addressing hybrid threats, and can it be precisely defined?
5. In the digital hybrid age, what role does the home front play in countering hybrid warfare and protecting national security?
6. How do media actors contribute to hybrid warfare tactics, and what role do they play in influencing public opinion and perceptions?
7. What joint efforts and working groups have been established by EU countries to address hybrid threats and enhance collective security?
8. How has public diplomacy been utilised as a tool to counter hybrid threats, and what impact has it had on promoting international collaboration and cooperation?
9. What measures have been taken by governments and international entities to build private capacity in countering disinformation and hybrid warfare?
10. How has the evolution of social media and peer-to-peer communication shaped the dynamics of public diplomacy in countering hybrid threats?

References

Adesina, Olubukola S. (2017): Foreign Policy in an Era of Digital Diplomacy. *Cogent Social Sciences,* 3(1). Online: https://doi.org/10.1080/23311886.2017.1297175

Attias, Shay (2012): Israel's New Peer-to-Peer Diplomacy. *The Hague Journal of Diplomacy,* 7(4), 473–482. Online: https://doi.org/10.1163/1871191X-12341235

Babiracki, Patryk (2018): Book Review on Evgeny Dobrenko – Natalia Jonsson-Skradol (eds.): *Socialist Realism in Central and Eastern European Literatures. Institutions, Dynamics, Discourses.* New York: Anthem Press, 2018. *Slavic Review,* 78(3), 835–836. Online: https://doi.org/10.1017/slr.2019.183

Bachmann, Sascha-Dominik Dov – Lee, Doowan – Dowse, Andrew (2020): Covid Information Warfare and the Future of Great Power Competition. *The Fletcher Forum of World Affairs,* 44(2), 11–18.

Bender, Dave (2014): Fake Hamas Message Claims Haifa Chemical Plant Hit by Gaza Rocket. *The Algemeiner,* 9 July 2014. Online: www.algemeiner.com/2014/07/09/fake-hamas-message-claims-haifa-chem-plant-hit-by-gaza-rocket/

Bjola, Corneliu – Holmes, Marcus (2015): *Digital Diplomacy. Theory and Practice.* London: Routledge. Online: https://doi.org/10.4324/9781315730844

Chan, Steve (2007): *China, the U.S. and the Power-transition Theory. A Critique.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203940662

Clinton, Hillary R. (2010): Leading through Civilian Power: Redefining American Diplomacy and Development. *Foreign Affairs,* 89(6), 13–24.

Council of the European Union (2016): *The EU Integrated Political Crisis Response – IPCR – Arrangements in Brief 2016.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2860/412159

Davies, Jonathan (2021): Foreign Election Interference and Hybrid Warfare. *Senior Independent Study Theses,* (9443). Online: https://openworks.wooster.edu/independentstudy/9443

DeWit, Andrew – Djalante, Riyanti – Shaw, Rajib (2020): Building Holistic Resilience: Tokyo's 2050 Strategy. *The Asia Pacific Journal,* 18(7), 1–15.

Ducaru, Sorin D. (2016): The Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO. *Europolity – Continuity and Change in European Governance – New Series,* 10(1), 1–17.

Dunay, Pál – Roloff, Ralf (2017): *Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank.* Online: www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0

Ebitz, Amy (2019): *The Use of Military Diplomacy in Great Power Competition: Lessons Learned from the Marshall Plan.* Online: www.brookings.edu/blog/order-from-chaos/2019/02/12/the-use-of-military-diplomacy-in-great-power-competition

European Commission (2016): *FAQ: Joint Framework on Countering Hybrid Threats.* Online: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250

Gilman, Derek – Nichols, Robert – Totman, Jade C. – Minarich, Christine (2014): *Foreign Military Sales. Direct Commercial Sales.* Washington, D.C.: Defense Security Cooperation Agency – Covington & Burling LLP.

Haigh, Maria – Haigh, Thomas – Matychak, Tetiana (2019): Information Literacy vs. Fake News: The Case of Ukraine. *Open Information Science,* 3(1), 155–165. Online: https://doi.org/10.1515/opis-2019-0011

Hallams, Ellen (2010): Digital Diplomacy: The Internet, the Battle for Ideas & US Foreign Policy. *CEU Political Science Journal,* 5(4), 538–574.

Hoffman, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute of Security Studies.

Hook, Kristina – Verdeja, Ernesto (2022): *Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities.* Online: www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/

Hourcade, Jean-Charles – Jaccard, Mark – Bataille, Chris – Ghersi, Frédéric (2006): Hybrid Modeling: New Answers to Old Challenges. Introduction to the Special Issue of *The Energy Journal. The Energy Journal,* 27(Special Issue), 1–12.

Humprecht, Edda – Esser, Frank – Van Aelst, Peter (2020): Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics,* 25(3), 493–516.

Jakobsen, Peter V. (2000): Focus on the CNN Effect Misses the Point: The Real Media Impact on Conflict Management Is Invisible and Indirect. *Journal of Peace Research,* 37(2), 131–143. Online: https://doi.org/10.1177/0022343300037002001

Jordan, Brigitte (2009): Blurring Boundaries: The "Real" and the "Virtual" in Hybrid Spaces. *Human Organization,* 68(2), 181–193. Online: https://doi.org/10.17730/humo.68.2.7x4406g270801284

Jun Ayhan, Kadir (2020): A Typology of People-to-People Diplomacy. Online: https://uscpublicdiplomacy.org/blog/typology-people-people-diplomacy

Kert-Saint Aubyn, Mari (2016): *EU Policy on Fighting Hybrid Threats.* Online: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/

Lebel, Udi (2010): "Casualty Panic": Military Recruitment Models, Civil-Military Gap and Their Implications for the Legitimacy of Military Loss. *Democracy and Security,* 6(2), 183–206. Online: https://doi.org/10.1080/17419166.2010.492175

Monsees, Linda (2020): Cryptoparties: Empowerment in Internet Security? *Internet Policy Review,* 9(4), 1–19. Online: https://doi.org/10.14763/2020.4.1508

NATO (2016): *Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Online: www.nato.int/cps/en/natohq/official_texts_138829.htm

NATO (2023): *Collective Defence and Article 5.* Online: www.nato.int/cps/en/natohq/topics_110496.htm

Nye, Joseph S. Jr. (1990): Soft Power. *Foreign Affairs,* 80(Autumn), 153–171. Online: https://doi.org/10.2307/1148580

Nye, Joseph S. Jr. (2010): The Future of American Power: Dominance and Decline in Perspective. *Foreign Affairs,* 89(6), 2–12.

Orabi, Mariam – Mouheb, Djedjiga – Al Aghbari, Zaher – Kamel, Ibrahim (2020): Detection of Bots in Social Media: A Systematic Review. *Information Processing & Management,* 57(4). Online: https://doi.org/10.1016/j.ipm.2020.102250

Orenstein, Mitchell (2022): *Russia vs. the West and the New Politics of Hybrid War.* Online: https://events.ceu.edu/2022-03-10/russia-vs-west-and-new-politics-hybrid-war

Orpaz, Inbal – Siman-Tov, David (2021): The Unfinished Campaign: Social Media in Operation Guardian of the Walls. *The Institute of National Security Studies,* 12 September 2021. Online: www.inss.org.il/publication/guardian-of-the-walls-social-media/

Osula, Anna-Maria (2014): *EU Solidarity Clause and 'Cyber Disaster'.* Online: https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/

Storey, Neil R. – Kay, Fiona (2017): *The Home Front in World War Two.* Stroud: Amberley Publishing.

Svetoka, Sanda (2016): *Social Media as a Tool of Hybrid Warfare.* NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177

Treverton, Gregory F. – Thvedt, Andrew – Chen, Alicia R. – Lee, Kathy – McCue, Madeline (2020): *Addressing Hybrid Threats.* Swedish Defence University – Center for Asymmetric Threat Studies – The European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

Voronova, Sofija – Bakowski, Piotr (2022): *Future Shocks 2022: Consolidating EU Internal Security.* Online: https://epthinktank.eu/ 2022/05/22/future-shocks-2022-consolidating-eu-internal-security/

Wassermann, Felix (2018): The Blurring of Interstate Wars, Civil Wars, and Peace – "Hybrid War" as an Expression of Conceptual and Political Disorientation in the Twenty-first Century. *Sicherheit und Frieden (S+F) / Security and Peace,* 36(1), 14–20.

Weissman, Steve (2019): The Meaning of Reliability. *Natural Gas & Eletcricity,* 35(12), 1–7. Online: https://doi.org/10.1002/gas.22126

Wither, James K. (2016): Making Sense of Hybrid Warfare. *Connections,* 15(2), 73–87. Online: https://doi.org/10.11610/Connections.15.2.06

Ynet (2014): "נפציץ כל מקום בישראל" :מחמאס SMS [Hamas SMS: "We will bomb every place in Israel."] *Ynet,* 14 July 2014. Online: https://www.ynet.co.il/articles/0,7340,L-4543488,00.html

Further reading

Cullen, Patrick J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. Norfolk: Allied Command Transformation.

Huhtinen, Aki-Mauri – Rantapelkonen, Jari (2016): Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere. *Journal of Information Warfare,* 15(4), 50–67.

Mills, Claire (2015): *France and Article 42(7) of the Treaty on the European Union.* Online: https://commonslibrary.parliament.uk/research-briefings/cbp-7390/

Shay Attias[1]

Hybrid Warfare and Informational Strategies: Russia's Campaign in Ukraine (2014)

In recent years, the concept of "hybrid warfare" has transcended academic discussions and become a stark reality on the battlefield. The gradual annexation of territories by Putin's regime raised questions among experts about the emergence of a "new" era of warfare, distinct from the conventional ideas proposed by *Clausewitz* or *Mao Zedong.* The pivotal moment that triggered this shift was Russia's annexation of Crimea in March 2014, followed by its aggressive actions in the Donbas region of Ukraine. These events have had a profound impact on the perception and approach to security in Europe. Despite the growing acknowledgment of hybrid warfare, there remains a lack of consensus within NATO regarding its precise definition and the diverse forms it can assume. Nevertheless, the lessons derived from the conflict in Ukraine have prompted a critical reassessment of security strategies, leading to the development of a fresh framework for conceptualising European security. As hybrid warfare continues to evolve, it presents distinct challenges that demand a comprehensive understanding and proactive response from NATO and its member states. Establishing a shared understanding of hybrid warfare and its various manifestations is crucial to effectively counter this multifaceted and ever-evolving threat.[2] However, upon deeper analysis, the term "hybrid era" reveals its essence in the interconnectedness of two distinct components: military warfare and the civilian home front. While the involvement of civilians or the targeting of civilian infrastructure during conflicts is not a new phenomenon, the methods, capabilities and tools employed to exert civilian and public influence have undergone significant transformations. This unique convergence of military and civilian domains presents a perplexing departure from traditional military history. The evolving nature of hybrid warfare has witnessed notable changes in the ways civilian populations are impacted and utilised as part of the conflict strategy. This encompasses a wide array of tactics aimed at influencing public opinion, manipulating information and leveraging

[1] Bar-Ilan University.

[2] Bilal 2021.

DOI: https://doi.org/10.36250/01236_12

technological advancements to exploit vulnerabilities within the civilian sphere. The unprecedented scope and scale of civilian involvement and its effects distinguish the hybrid era as an unprecedented phenomenon in military affairs. As the hybrid era continues to unfold, it becomes increasingly crucial to comprehend the dynamics and implications of this interconnected relationship between military and civilian aspects. By understanding the distinct characteristics and intricacies of hybrid warfare, policymakers, military strategists and society as a whole can better navigate the complexities and devise effective responses to safeguard both military and civilian interests in this evolving landscape.[3] Accordingly, the concept of hybrid warfare had already garnered attention within the Russian General Staff by 2014, but its roots can be traced back even further within U.S. military thinking. Defense Secretary Robert Gates had recognised the significance of "hybrid warfare" in relation to counterinsurgency and proxy conflicts in the Middle East as early as 2009. Prior to that, esteemed military scholars, notably Frank Hoffman in the early 2000s, had explored the concept of hybrid warfare and related ideas. These academic contributions aimed to shed light on U.S. strategies in counterterrorism and counterinsurgency, while acknowledging the inherent hybrid nature of conflicts throughout history. The NATO alliance had also been actively engaged in strategic discussions on hybrid threats well before the Ukraine campaign. In 2010, NATO initiated its comprehensive approach through the work on "NATO's Military Contribution to Countering Hybrid Threats", which later informed the 2010 Strategic Concept. These early efforts by NATO demonstrate the recognition and understanding of the evolving nature of warfare and the need to address hybrid threats in a coordinated and comprehensive manner. By tracing the origins of the concept and its integration into military thinking, policymakers and strategists can gain valuable insights into the complexities and challenges posed by hybrid warfare. This historical context underscores the importance of continued reflection, adaptation and collaboration to effectively counter hybrid threats and ensure the security and resilience of nations and alliances.[4]

[3] Chivvis 2017; Pynnöniemi–Jokela 2020.
[4] NATO 2010.

Nonviolent civilian defence

In addition to its camouflaged nature, Russia's hybrid war has also depended on Putin's strategy of plausible deniability. This deniability shows itself in many questionable claims before February 2022: according to Moscow, there was no interstate war to which Russia is a party, merely internal ethnic conflict; Russia was not shipping weapons to parties in Ukraine; they were sold, bought, or stolen by private parties; there were no Russian troops on the ground, merely unaffiliated local militias; if there were Russians with military backgrounds engaged in combat fighting, they were off-duty army personnel, retired army veterans or armed civilian volunteers.[5] Beyond "maskirovka"[6] and plausible deniability, there was another, no less significant, component of Putin's hybrid warfare that was generally disregarded. This was the Kremlin's cynical use of collective nonviolent, civilian-led mobilisation and actions in support of its military campaigns. The popular nonviolent uprisings in Serbia (2000), Georgia (2003) and finally, the successful 2004 Orange Revolution in Ukraine all made the Kremlin worried about the possibility of a similar outburst of popular discontent in Russia and encouraged Putin to borrow from the repertoire of nonviolent organisations to strengthen his own defence.[7] To mitigate the possibility of a people's revolution, the Russian regime created a seemingly grassroots civic movement of pro-government youths known as "Nashi" ("Ours"). It was subsequently deployed whenever the Kremlin needed to organise the protest, counterdemonstrations, anti-opposition rallies, disruption of opposition events, or harassment of pro-opposition figures or diplomats. The Kremlin has used the loyal crowds of unarmed civilians to organise what became to be known as "Putingi" (a neologism combining "Putin" with "mitingi", the Russian opposition's word for protest). In 2012, the Kremlin convoked its Putingi when the opposition-held demonstrations to protest rigged parliamentary elections. It did it again during the 2014 peace marches and rallies in Moscow and elsewhere in the country. After the Euromaidan revolution in Ukraine, seemingly grassroots groups of citizens and "patriotic groups" in Russia launched an "anti-maidan".[8]

5 Gunneriusson 2019.
6 Bouwmeester 2017.
7 Bartkowski 2015.
8 Bartkowski 2015.

In 2014 the Kremlin took another critical step when it elevated nonviolent civil actions from an arguably defensive domestic asset for propping up the regime to an aggressive foreign policy and military tool. In doing so, it took lessons from the Euromaidan revolution in Ukraine. The Euromaidan was a widespread upheaval that, after 92 days of largely nonviolent mobilisation and campaigns, led to significant loyalty shifts within the regime's political, business and security pillars. These defections, combined with ongoing massive civil disobedience, sealed the fate of the pro-Russian president Victor Yanukovych who fled Kyiv on 21 February 2014.[9] The two main lessons for the Russian security services were that the Ukrainian military would rather disobey orders than shoot unarmed civilians and that at least a semblance of popular grassroots support would be necessary for the ultimate success of the subversive operations that Russia planned in Ukraine. While Russia's hybrid warfare still depends on "hard power elements", there is no doubt that many of its warfare elements is based on propaganda "maskirovka", plausible deniability and civilian-led collective nonviolent action against the enemy. During the conflict in Ukraine, the Kremlin has excelled in promulgating propaganda with effectiveness not seen since the heyday of the Soviet Union. This information warfare conducted in social and mainstream media is designed to deceive adversaries, blur the line between reality and fantasy, drive a wedge between Western allies and keep the Russian population in the dark. It became a crucial instrument in a larger strategy of the Russian Government's "maskirovka". This Russian term refers to a broadly defined "action plan" deployed as a form of "camouflage, concealment, deception, imitation, disinformation, secrecy, security, feints, diversions and simulation" against an adversary. The Russian state has deployed maskirovka on the strategic, operational and tactical levels of its military and nonmilitary campaigns to disguise its actions going back to the Napoleonic Wars. It particularly honed these skills during the Soviet period.[10] Maskirovka is indeed a concept deeply rooted in Russian military doctrine, encompassing various tactics and strategies aimed at deception, disinformation and concealment. In the context of the Ukrainian conflict, maskirovka has been utilised by Russia to hide the presence of regular Russian soldiers and military equipment on Ukrainian territory. The objective has been to prevent the publication and dissemination of reports on soldiers' deaths in Russia, thereby maintaining a façade of deniability regarding direct Russian involvement. While these efforts initially aimed to

[9] BBC News 2014.

[10] Keating 1981; Roberts 2015.

obfuscate the Russian military's role in Ukraine, they eventually became less effective as evidence of their presence became more apparent in the West. Western observers and governments increasingly recognised the involvement of Russian forces, undermining the effectiveness of maskirovka as a deception strategy. Nonetheless, it is true that the Russian strategy of maskirovka in the Ukrainian conflict was also intended to divide public opinion in the West and maintain support for the Kremlin's position on Ukraine. By sowing doubt and confusion through disinformation campaigns and other means, Russia sought to create a narrative that blurred the lines of responsibility and portrayed the conflict as more complex than a straightforward Russian invasion. Regarding public opinion in Russia, it is worth noting that Putin's approval rating did experience a significant boost in the wake of Russia's annexation of Crimea in 2014.[11] However, it is important to approach these approval ratings with caution, as they can be influenced by various factors, including the media landscape, state propaganda and limited political alternatives.[12] Russian operations in Crimea began soon after Yanukovych's departure. In an interview on 4 March 2014, a week after the arrival of Russian troops in Crimea, dressed in green uniforms without insignia whom Ukrainians sarcastically referred to as "little green men", Putin openly discussed the strategy of using nonviolent demonstrations led by local civilians to neutralise the Ukrainian military. "Listen carefully. I want you to understand me clearly: if we make that decision [to send the Russian army to Ukraine], it will only be to protect Ukrainian citizens. And let's see those [Ukrainian] troops try to shoot their own people, with us behind them – not in the front, but behind. Let them just try to shoot at women and children! I would like to see those who would give that order in Ukraine."[13] Russia used the unwillingness of Ukrainian troops to fire on fellow citizens to stage successful occupations, sit-ins and seizures of Ukrainian army garrisons in Crimea. This also created favourable conditions for desertions and defections among the members of the Ukrainian army. Instead of facing an overt armed assault that would have killed Ukrainian soldiers and raised their feelings of unit cohesion and battle spirit (as happened later in the conflict in the eastern

[11] A Gallup survey conducted from 21 to 27 April revealed that 82.8% of the Crimean population believes that the results of the referendum accurately reflect the views of the majority of Crimeans. Additionally, 73.9% of Crimeans expressed the belief that Crimea's integration into Russia would improve their own lives and the lives of their families, while a minority of 5.5% disagreed with this viewpoint.

[12] Levinson 2022.

[13] President of Russia 2014.

part of Ukraine), the troops faced unarmed civilians.[14] Moreover, the Russian side offered financial and institutional incentives to Ukrainian soldiers. For example, they were promised that they could keep their ranks and receive higher salaries if they switched sides.[15] Consequently, less than 25% of the Ukrainian troops stationed in Crimea stayed loyal to their state; 50% defected to Russia and the rest deserted.[16] Collectively, these measures allowed the armed "little green men" to take control of the Ukrainian military sites without facing much resistance. In fact, the relatively peaceful takeover of Crimea earned Russian soldiers in Putin's media and among the Russian public a nickname of "the polite people".[17]At the same time, Putin publicly acknowledged that seemingly nonviolent actions were, in fact, an adequate cover for lethal force. According to the Russian president, "you can do much more with weapons and politeness than just politeness".[18]

Russia's hybrid strategy in Crimea and Eastern Ukraine

Following the contentious Crimean referendum on 16 March 2014, Russia turned its focus to eastern Ukraine, specifically the Donbas region comprising Luhansk and Donetsk. In contrast to western Ukraine, the Donbas population exhibited limited political engagement and remained disconnected from civic activism. Even on sensitive issues like the ban on the Russian language, only a small fraction of Donbas adults expressed a willingness to participate in demonstrations against the ban.[19] The Russian Government, under Putin's leadership, employed a hybrid strategy combining armed and unarmed tactics, including coerced "legitimised voting", to annex Crimea and destabilise southeastern Ukraine. The unarmed aspect of this campaign aimed to erode loyalty to the national government among a mobilised minority, leveraging existing mistrust, fear and discontent while manipulating the genuine desire for significant political change. This strategy capitalised on the limited civic engagement, particularly in the Donbas region, where political apathy, passivity, and a lack of political awareness facilitated the influence of sophisticated Russian propaganda. Under Putin's leadership, the

[14] Luhn 2014.
[15] Reevell–Sneider 2014.
[16] Interfax Ukraine 2014.
[17] Reuters 2014.
[18] Roth 2014a.
[19] Matveeva 2016; Kudelia 2014b.

Russian Government utilised a hybrid approach that encompassed both armed and unarmed tactics to annex Crimea and sow instability in southeastern Ukraine. In addition to the use of military force, an unarmed aspect of this campaign focused on coercive and manipulated voting processes to erode loyalty to the Ukrainian Government. This strategy exploited existing mistrust, fear and discontent among a mobilised minority, while capitalising on genuine aspirations for political change. The sophisticated Russian propaganda machine took advantage of low levels of civic engagement, particularly in the Donbas region, where political apathy, passivity, and a lack of political awareness created fertile ground for their influence. During the Euromaidan revolution, the political apathy of residents in the Donbas region became apparent, as there were no actual demonstrations either in favour or against the Maidan movement. This lack of engagement allowed a minority of separatists, backed by Russia, to exploit existing fears and distrust among specific segments of the Donbas population. These separatists portrayed the new central government as a "violent fascist junta" responsible for the removal of President Yanukovych. By amplifying these sentiments, they aimed to undermine support for the central government and justify their separatist agenda.[20] In general, "unarmed civilians" played a significant role in the strategy employed by Russia and the separatists to gain control over the Donbas region.[21] This involved the initial actions of armed groups, lacking identifiable markings, who forcefully took control of local government buildings and security installations. Subsequently, unarmed civilians actively joined these groups, serving as human shields and publicly demonstrating their support for the rebels. Despite constituting a minority within the local population, these unarmed civilians added a sense of legitimacy to the rebels' cause, as portrayed in pro-Russian narratives. Similar incidents occurred in various cities across southeastern Ukraine, where civilian-led pro-Russian rallies, attempts to capture administrative buildings and calls for referenda were witnessed.[22] As expected, these events were labelled by the Russian media, officials and pro-Russian civilians as the "Russian Spring". However, a survey conducted by the Kyiv International Institute of Sociology in February 2014 indicated relatively low levels of support for joining Russia in the Donetsk region (33%) and Luhansk region (24%), as well as other southeastern regions of Ukraine.[23]

[20] Bartkowski 2015; Kühn von Burgsdorff 2015.
[21] Kudelia 2014a.
[22] Kushch 2014; Bartkowski 2015.
[23] Giuliano 2018; Katchanovski 2016.

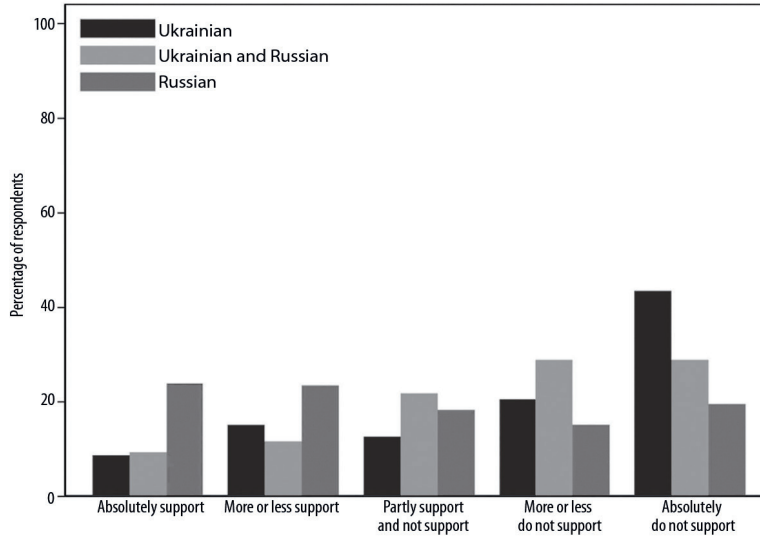

Figure 1: Support for separatism by nationality in Donbas
Source: Giuliano 2018: 166

Within this context, humanitarian convoys played a critical role in Russia's nonviolent strategy.[24] By organising and dispatching these convoys without permission, Russia aimed to present itself as a benevolent provider of aid to the occupied cities, diverting attention from its military intervention and occupation of Ukrainian territory. This approach allowed Russia to manipulate international public opinion, maintain the appearance of nonviolence and deflect criticism.[25] The Ukrainian authorities faced a dilemma in responding to the convoys, as any aggressive action would have played into Russia's propaganda and potentially escalated the conflict. Consequently, Ukraine chose to let the convoys pass, unintentionally creating unofficial "humanitarian" corridors that Russia could exploit for military purposes. Additionally, reports indicated the transport of stolen machine parts from Ukrainian industrial facilities back to Russia within these convoys.[26]

[24] Scrinic 2014: 77–88.
[25] Rácz 2014.
[26] Lister–Fylyppov 2022.

An old wine in a new bottle?

Most experts and military personnel ask whether there is any justification for calling the era of the current war "the same" or "different" and whether there is any justification for calling it a hybrid era. For this, we must examine the introduction of the term "second hybrid warfare late in the 2000s", which has been brought into the public eye by Frank G. Hoffman's research in 2007 and received great interest after Russia took over the Crimean Peninsula in 2014 and fought in eastern Ukraine for hundreds of years. However, even when we try to understand the term's origin, we run into a sharp disagreement starting with the fact that the Russians themselves do not adopt the term and there is no general agreement on the meaning of the term. However, it is generally accepted that it includes the use of actions that are "below the threshold" of war to achieve accomplishments (political or otherwise) without paying the price associated with an overt act, without the need to take direct responsibility, all the while preventing the adversary from imposing such responsibility. To a large extent, the inability to clearly define "what is hybrid warfare" makes it so. Therefore, one must be careful not to give the impression that this is a complex and sophisticated doctrine used by many and that it is precisely the simple use of well-known but skilled elements and elements that have undergone manipulations and innovations that increase the threat, which is easy to understand but not to deal with: "Russia's (2021) aggression against Ukraine has launched a process of destroying the system of European and transatlantic security."[27] Despite the challenges, there may be a bright spot that allows us to understand the development of the term, and it lies in one of the few agreements – and that is the change in the face of digital and social communication since the 2000s with the rise of the digital age. Before the advent of media and social networks, mass communication was nothing new, the use of propaganda and psychological warfare was abundant, and the number of wars and operations that were used was almost infinite. But even when we look at the most "magnificent" examples of the use of propaganda to influence the home front and the citizens, among them the First and Second World Wars, the First Palestinian Intifada, the Iran–Iraq War, Algiers and France, and more, we see that most of the capabilities promoted depended to a large extent on the means of technology which were at their disposal at the time.[28] The combat unit's technological capabilities

[27] Bratko et al. 2021: 147.

[28] Yevstafiev–Manoilo 2021; Perry–Schleifer 2006.

depended on the means of communication that Laz had at their disposal: telegrams, telegraphs, loudspeakers flying on top of helicopters, cardboard dolls in the shape of tanks, or even classic mass communication of radio and television. However, already at the end of the 1980s, during the first Iraq War, the concept of the "CNN effect" developed, which in fact marked the beginning of the global news and mega-media era that allowed the citizens of the world to join any operation or war that will break out in the world. The peak was the social media age, in which the citizens, who saw and observed the vacillation, began to form positions, opinions and feelings towards the warring parties even though the war was taking place far from their country's borders. This phase is called the information age, and it opened the first window for introducing the "ordinary" citizens to the battlefield in a way that had not been seen at the time. In this, the theories of the strong effects of the media from the first models of Laswell and McQuail were brought back, and concepts such as "global media agenda", or "public opinion", "number of viewers" and "ratings" became old currencies in the new digital consciousness age.[29] The "Information Age" is a historical period that began in the mid-20th century, characterised by a rapid epochal shift from traditional industry established by the Industrial Revolution to an economy primarily based upon information technology. Therefore, and if we assumed that the technological information is the one that gives the information age its character and capabilities, then it is easy to understand why since the 2000s when social networks burst into our lives and certainly redefined "technological communication", something happened and something fundamental changed. Today, digital communication and social media have become available, fast and accessible to almost every person in our world, something that has shrunk space and time in a way we did not know in the era of previous wars. The speed of technological communication in previous eras cannot be compared to the digital information age. This has some major consequences, firstly, digital civil networks have been created that on the one hand consume a lot of information from everywhere and at any time and in endless quantities and on the other hand, they are able to produce information in the same way. That is, the citizens of the world can organise and generate information but in the same way be exposed and need information. This concept was called "peer-to-peer networks" that have become generators and information needs in a way that bypasses the countries and are able to communicate with each other even in different cultures and

[29] Sapienza et al. 2015.

languages.[30] Second, the technological capabilities to communicate with any person or entity in our world have multiplied with the development of social networks and multiple applications together with smart phone devices that have given "ordinary citizens" or in military parlance, the civilian "home front" the ability to influence the media and global agenda. In other words, the citizens who have become more educated and informed in detail about every event that takes place in our world, are now able to repeatedly influence what is happening, react, create their own stories and try to compete for the hearts and minds of the world.[31] Thirdly, and in light of the previous two sections, the fact that citizens have become so digitised and have technological capabilities for multiple cross-border communications that encourage them to continue to be connected to what is happening, they become more and more vulnerable, they become the targets of information manipulation, mind engineering, fake news, interventions in democratic elections, the establishment of bots. The caller from a social network and implementer of technological impersonation capabilities for any person or company. Therefore, and considering all this, it is not for nothing that our age is not called the hybrid age or the digital age, but the age of "consciousness" or more correctly, the age of "consciousness re-engineering" that operates in a systematic way using the data taken from our increasing and exponential use of technological communication. For example, by means of our smartphone which has become "an organ of our body since the nineties" hidden actions are done by the developers of the applications and whose ultimate and clear purpose is to trap us inside it for their benefit. Transferring the entirety of our lives into the digital world means that every click and every form filled in is documented and analysed.[32] These digital footprints are today's gold and diamond mine. Data mining allows commercial companies to build a profile of each user, using algorithms that provide infinite psychological intelligence, and send him a flood of messages that match his personality, thereby engineering his every action, feeling and thought without the need for direct interaction with him. While most of us believe that the digital reality invites us to a lot of freedom of information and choice, the author of this paper reveals its illusory and disappointing face, and the sophisticated manipulations designed to entice the user to devote themselves to applications, to become addicted to content and social sites, and to spend more and more time and money on

[30] Yang–Chen 2008.
[31] Attias 2012.
[32] Myers 2021.

shopping sites. And in the absence of laws, regulations and brakes to protect digital users, a picture of a future reality emerges in which man is a "voluntary" prisoner in the absence of freedom of thought, will and choice.[33]

Conclusion

War has two essential components: one is complex, and the other is soft and nonviolent, which due to the changing media and digital environment has become multi-dimensional and rich in tools and tactics that are used in times of War and conflict against the "civilian front". Within the soft component, the citizen's consciousness has become a target for the bombardment of false information to damage the adversary's national strength. Unlike in previous eras, the damage is not only local. It aims to cause damage to the status of the state as well by lowering the level of legitimacy and international support and thus subtly harming the opponent.

On the civilian level:

- establishing filtering and fact-checking systems that will be available to as many citizens as possible
- initiating advocacy efforts for citizens regarding the importance of consuming reliable information
- publication of detected fake news messages

On the military level:

- establishing and improving bodies that deal with civilian information, the reliability of the information and the creation of reliable information from the battlefield
- increasing publications against fake news from the battlefield
- strengthening the relationship with civil networks to spread the message
- strengthening the relationship with journalists and opinion leaders

On the diplomatic level:

- building systems for checking information and facts regularly (not only during the war) in different languages against fake news
- establishing more cooperation and awareness to increase international synchronisation

[33] Tejomurti et al. 2018.

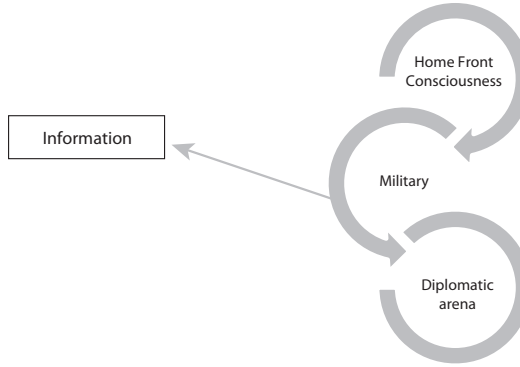

Figure 2: The 3 levels of joined information protecting model
Source: Compiled by the author

Questions

1. What is the digital face of hybrid warfare?
2. What are the new tools of deniability and civilian-led collective nonviolent action as presented in the 2021 Russian–Ukraine case study?
3. Why "legitimacy" has become so crucial in the hybrid warfare age, and what can we do about it?
4. What are the main steps we can take to strengthen our civilian front?
5. How the evolution of information age into a digital form has brought new threats to the warfare world?
6. How and why citizen's consciousness has become a target for the bombardment of false information to damage the adversary's national strength?

References

Attias, Shay (2012): Israel's New Peer-to-Peer Diplomacy. *The Hague Journal of Diplomacy,* 7(4), 473–482. Online: https://doi.org/10.1163/1871191X-12341235

Bartkowski, Maciej (2015): *Nonviolent Civilian Defense to Counter Russian Hybrid Warfare*. Washington, D.C.: Johns Hopkins University.

BBC News (2014): Ukrainian MPs Vote to Oust President Yanukovych. *BBC News,* 22 February 2014. Online: www.bbc.com/news/world-europe-26304842

Bilal, Arsalan (2021): *Hybrid Warfare – New Threats, Complexity and 'Trust' as the Antidote.* Online: www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Bouwmeester, Han (2017): Lo and Behold: Let the Truth Be Told – Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'. In Ducheine, Paul A. L. – Osinga, Frans P. B. (eds.): *Netherlands Annual Review of Military Studies 2017.* The Hague: T.M.C. Asser Press, 125–153. Online: https://doi.org/10.1007/978-94-6265-189-0_8

Bratko, Artem – Zaharchuk, Denys – Zolka, Valentyn (2021): Hybrid Warfare – A Threat to the National Security of the State. *Revista de Estudios en Seguridad Internacional,* 7(1), 147–160. Online: https://doi.org/10.18847/1.13.10

Chivvis, Christopher S. (2017): *Understanding Russian "Hybrid Warfare" and What Can Be Done about It.* Santa Monica: RAND.

Giuliano, Elise (2018): Who Supported Separatism in Donbas? Ethnicity and Popular Opinion at the Start of the Ukraine Crisis. *Post-Soviet Affairs,* 34(2–3), 158–178. Online: https://doi.org/10.1080/1060586X.2018.1447769

Gunneriusson, Håkan (2019): Hybrid Warfare and Deniability as Understood by the Military. *Polish Political Science Yearbook,* 48(2), 267–288. Online: https://doi.org/10.15804/ppsy2019205

Interfax Ukraine (2014): Kyiv Negotiating Terms for Redeploying Ukrainian Military from Crimea to Mainland. *Interfax Ukraine,* 24 March 2014. Online: http://en.interfax.com.Ua/news/general/197552.html

Katchanovski, Ivan (2016): The Separatist War in Donbas: A Violent Break-up of Ukraine? *European Politics and Society,* 17(4), 473–489. Online: https://doi.org/10.1080/23745118.2016.1154131

Keating, Kenneth C. (1981): *Maskirovka: The Soviet System of Camouflage.* Fort Belvoir: Defense Technical Information Center.

Kudelia, Serhiy (2014a): The Maidan and Beyond: The House that Yanukovych Built. *Journal of Democracy,* 25(3), 19–34.

Kudelia, Serhiy (2014b): New Policy Memo: Domestic Sources of the Donbas Insurgency. *Ponars Eurasia,* 29 September 2014. Online: www.ponarseurasia.org/memo/domestic-sources-donbas-insurgency

Kushch, Lina (2014): Pro-Russian Demonstrators Burn Books, Storm Buildings in Eastern Ukraine. *Reuters,* 16 March 2014. Online: www.reuters.com/article/world/pro-russian-demonstrators-burn-books-storm-buildings-in-eastern-ukraine-idUSBREA2F0R9/

Kühn von Burgsdorff, Elias (2015): The Euromaidan Revolution in Ukraine: Stages of the Maidan Movement and Why They Constitute a Revolution. *Inquiries Journal,* 7(2). Online: www.inquiriesjournal.com/articles/986/the-euromaidan-revolution-in-ukraine-stages-of-the-maidan-movement-and-why-they-constitute-a-revolution

Levinson, Paul (2022): *Fake News in Real Context.* Connected Editions.

Lister, Tim – Fylyppov, Sanyo (2022): Russian Ships Carrying Stolen Ukrainian Grain Turned Away from Mediterranean Ports – But not all of them. *CNN,* 12 May 2022. Online: https://edition.cnn.com/2022/05/12/europe/russia-ship-stolen-ukraine-grain-intl-cmd/index.html

Luhn, Alec (2014): Donetsk Activists Fortify Barricades after Police Clear Kharkiv Protest Site. *The Guardian,* 8 April 2014. Online: www.theguardian.com/world/2014/apr/08/donetsk-barricades-kharkiv-protest-ukraine-russia

Matveeva, Anna (2016): No Moscow Stooges: Identity Polarization and Guerrilla Movements in Donbass. *Southeast European and Black Sea Studies,* 16(1), 25–50. Online: https://doi.org/10.1080/14683857.2016.1148415

Myers, Mary E. (2021): Propaganda, Fake News, and Deepfaking. In Gayle, S. Stever – Giles, C. David – Cohen, David J. – Myers, Mary E.: *Understanding Media Psychology.* New York: Routledge. Online: https://doi.org/10.4324/9781003055648

NATO (2010): *BI SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.* Online: www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

Perry, Robert L. – Schleifer, Ron (2006): *Psychological Warfare in the Intifada. Israeli and Palestinian Media Politics and Military Strategies.* Eastbourne: Sussex Academic Press.

President of Russia (2014): *Vladimir Putin Answered Journalists' Questions on the Situation in Ukraine.* Online: www.en.kremlin.ru/events/president/news/20366

Pynnöniemi, Katri – Jokela, Minna (2020): Perceptions of Hybrid War in Russia: Means, Targets and Objectives Identified in the Russian Debate. *Cambridge Review of International Affairs,* 33(6), 828–845. Online: https://doi.org/10.1080/09557571.2020.1787949

Rácz, András (2014): Putin's Humanitarian Convoy and the Road to Ukraine: Russia May Intend to Change the Course of the Fighting. *FIIA Comment,* 10.

Reevell, Patrick – Sneider, Noah (2014): For Ukraine Military in Crimea Glum Capitulation and an Uncertain Future. *The New York Times,* 23 March 2014. Online: www.nytimes.com/2014/03/23/world/europe/for-ukraine-military-in-crimea-glum-capitulation-and-an-uncertain-future.html

Reuters (2014): Russian Lawmakers Seek Holiday to Honor Troops who Seized Crimea. *Reuters,* 17 September 2014. Online: www.reuters.com/article/2014/09/17/us-ukraine-crisis-holiday-idUSKBN0HC24720140917

Roberts, James Q. (2015): *Maskirovka 2.0. Hybrid Threat, Hybrid Response.* Tampa: Joint Special Operations University Press.

Roth, Andrew (2014a): From Russia, 'Tourists' Stir the Protests. *The New York Times,* 4 March 2014. Online: www.nytimes.com/2014/03/04/world/europe/russias-hand-can-be-seen-in-the-protests.html

Roth, Andrew (2014b): Meeting U.S. Envoy, Putin Appears to Soften His Tone. *The New York Times,* 20 November 2014. Online: www.nytimes.com/2014/11/20/world/meeting-us-envoy-putin-appears-to-soften-his-tone.html?_r=0

Sapienza, Zachary S. – Narayanan, Iyer – Veenstra, Aaron S. (2015): Reading Lasswell's Model of Communication Backward: Three Scholarly Misconceptions. *Mass Communication and Society,* 18(5), 599–622. Online: https://doi.org/10.1080/15205436.2015.1063666

Scrinic, Andrei (2014): Humanitarian Aid and Political Aims in Eastern Ukraine: Russian Involvement and European Response. *Eastern Journal of European Studies,* 5(2), 77–88.

Tejomurti, Kukuh – Hadi, Hernawan – Imanullah, Moch Najib – Indriyani, Rachma (2018): Legal Protection for Urban Online-Transportation-Users' Personal Data Disclosure in the Age of Digital Technology. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law),* 5(3), 485–505. Online: https://doi.org/10.22304/pjih.v5n3.a5

Yang, Stephen – Chen, Irene (2008): A Social Network-Based System for Supporting Interactive Collaboration in Knowledge Sharing over Peer-to-Peer Network. *International Journal of Human-Computer Studies,* 66(1), 36–50. Online: https://doi.org/10.1016/j.ijhcs.2007.08.005

Yevstafiev, Dmitriy – Manoilo, Andrei (2021): Information Wars and Psychological Operations as the Basis for New Generation Hybrid Wars. *Istoriya,* 12(6[104]). Online: https://doi.org/10.18254/S207987840016037-9

Further reading

Ackerman, Peter – Bartkowski, Maciej (2014): Challenging Annexation: In Crimea, the Referendum that Wasn't. *Open Democracy,* 22 March 2014. Online: www.opendemocracy.net/en/civilresistance/challenging-annexation-in-crimea-referendum-that-wa/

Chivers, Christpher J. – Roth, Andrew (2014): In Eastern Ukraine, the Curtain Goes Up, and the Clash Begins. *The New York Times,* 18 March 2014. Online: www.nytimes.com/2014/03/18/world/europe/eastern-ukraine.html

Melnyk, Oleksandr (2019): From the "Russian Spring" to the Armed Insurrection: Russia, Ukraine and Political Communities in the Donbas and Southern Ukraine. *The Soviet and Post-Soviet Review,* 47(1), 3–38. Online: https://doi.org/10.1163/18763324-04603009

Rachkevych, Mark (2014): Armed pro-Russian Extremists Launch Coordinated Attacks in Donetsk Oblast, Seize Regional Police Headquarters, Set up Checkpoints. *Kyiv Post,* 12 April 2014. Online: www.kyivpost.com/content/ukraine/armed-pro-russian-extremists-seize-police-stations-in-donetsks-slavyansk-shaktarysk-fail-to-take-donetsk-prosecutors-office-343195.html

Sharkov, Damien (2014): Russian 'Humanitarian Convoy' Heads for Separatist Moldovan Region. *Newsweek,* 5 December 2014. Online: www.newsweek.com/russian-humanitarian-convoy-heads-separatist-moldovan-region-289443

Shevchenko, Daryna (2014): Kharkiv City Government Building Infiltrated by pro-Russian Protesters. *Kyiv Post,* 13 April 2014. Online: www.kyivpost.com/content/ukraine/pro-russian-militants-attack-pro-ukrainian-demonstrators-in-kharkiv-including-at-least-three-severely-343292.html

Sørensen, Majken – Martin, Brian (2014): The Dilemma Action: Analysis of an Activist Technique. *Peace and Change,* 39(1), 73–100. Online: https://doi.org/10.1111/pech.12053

Yuhas, Alan – McCarthy, Tom (2014): Crisis in East Ukraine: A City-by-City Guide to the Spreading Conflict. *The Guardian,* 16 April 2014. Online: www.theguardian.com/world/2014/apr/16/crisis-east-ukraine-city-by-city-guide-map

About the Authors

Shay Attias – is a Communications and Political Science Department lecturer at Bar-Ilan University and a Senior Research Fellow at the Begin-Sadat Center for Strategic Studies. He has held several senior positions in communication and diplomacy, including Founding Head of the Department for Public Diplomacy in the Prime Minister's Office of Israel and Special Public Diplomacy Envoy of Israel's Ministry of Absorption and Foreign Affairs' Consulate in Boston. He specialises in diplomacy and U.S. foreign policy.

Péter Bányász – graduated in political science from the Faculty of Law and Political Science of the Eötvös Loránd University; then he obtained his doctorate at the Military Engineering Doctoral School of the Ludovika University of Public Service. His research interests include the human aspect of cybersecurity, network theories of psychological operations, and the relationship between privacy and surveillance. He is a lecturer at the Faculty of Public Governance and International Studies of the Ludovika University of Public Service and a researcher at the Institute for Cyber Security Research. He is also an active member of several scientific societies. He was the founding chairman of the Kápolnai Pauer István Youth Club of the Hungarian Association of Military Science, which as the head of its youth club, mentors several talented undergraduate and master students interested in military science.

Ghiță Bârsan – is the Commandant (Rector) of the "Nicolae Bălcescu" Land Forces Academy of Sibiu. He holds a PhD diploma in Engineering Sciences since 1997 and is also a habilitated doctor since 2014, coordinating PhD students in the field of Military Sciences. Research area covers Defence Modelling and Simulation, Military Sciences, E-learning, etc. He was the program director in the e-learning implementation within the Romanian Land Forces Staff and a member of the working group Partnership for Peace PfP Consortium Geneva – Advanced Distributed Learning.

Ionuț Alin Cîrdei – an Associate Professor at LFA. He has obtained a PhD title in Military Sciences in 2015, has a master's degree in Defence Diplomacy, attended several specialisation courses such as: Exercise Planning, Management of Critical Infrastructure Protection, Law of Armed Conflict, Conflict Management and Negotiation, Moniteur des techniques commando. He is also the author of valuable works related to hybrid warfare.

Andrew Dolan – is a graduate from the University of Glasgow and the Royal Military Academy, Sandhurst. On resigning his commission, he became a member of the international staff in Office of the Special Advisor to the NATO Secretary General. During this time, he worked as a U.K. National Expert and consultant to the European Commission. Following a period as a Research Fellow at the U.K. Defence Academy, he left government service to act as a consultant to the U.S. Defense Threat Reduction Agency. He is currently a senior advisor to DTRA and the U.S. DOE, as well as a recently appointed Ludovika Fellow on Artificial Intelligence and Public Policy at the Ludovika University of Public Service, Budapest, Hungary. He is the Director of the Centre for the Study of New Security Challenges.

Lucian Ispas – an infantry officer of the Romanian Land Forces with multinational experience. Currently is Associate Professor and Vice-Rector for Academics at the "Nicolae Bălcescu" Land Forces Academy of Sibiu. Since 2013, he possess a PhD title in Military Science and Intelligence and he is also an expert in various fields such as military capabilities and cross-cultural awareness in the multinational operations.

Éva Jakusné Harnos – is an applied linguist and political discourse researcher. She holds a PhD in Linguistics (Eötvös Loránd University, Budapest, 2005). Has been working in higher education since 2003. She is an Adjunct Professor, specialising on propaganda research, persuasion, deception, fake news and security studies. A curriculum developer, the author of course books on the language of politics and military terminology. A participant of the EUSecure blended and MOOC curriculum development project funded by the European Union.

Vojtech Jurčák – is a retired Colonel of the Slovak Air Force who works at the Armed Forces Academy (AFA) of General Milan Rastislav Štefánik in Liptovský Mikuláš, significantly participates in the development of the security theory, defence of the state in the context of national and international security and operations of the international crisis management organisations. He is the author and co-author of four monographs, two university textbooks and many university scripts. He is the principal investigator and co-investigator of research and development projects, one of which is within the EDA. He was a guarantor and member of the scientific boards of international scientific conferences in the Czech Republic, Poland and Ukraine. He is currently a Professor – Head of the Security and Defence Department at the AFA, and he is the guarantor of the study field Security and Defence of the State.

Csaba Krasznay – is an Associate Professor at the Ludovika University of Public Service with cybersecurity being his field of research. Currently, he is also the Head of the university's Institute of Cybersecurity. Besides his activities in higher education, he is present on the market as well. He obtained a CISA certification in 2005, CISM and CISSP in 2006, CEH in 2008, ISO 27001 Lead Auditor in 2012 and CSSLP in 2015. He is a board member of the Voluntary Cyber Defence Cooperation, member of ISACA Budapest Chapter, Magyary Zoltán E-government Association, Hungarian Association of Military Science, Scientific Association for Infocommunications and the Hungarian Association for Electronic Signature.

Ján Marek – works at the Armed Forces Academy of General Milan Rastislav Štefánik. He graduated at the Land Forces Military Academy in Vyškov. Later on, he completed postgraduate studies at the Military Academy in Liptovský Mikuláš where he was trained in combined commander specialisation. He completed Executive Program in Advanced Security Studies at the George C. Marshall European Center for Security Studies. He completed Higher Command Studies Course at the Baltic Defence College in Estonia. He completed his doctoral studies at the Armed Forces Academy of General Milan Rastislav Štefánik, specialisation National and International Security, in 2020. He specialised in the field of research of international relations, military arts and security. He is author of textbooks and has a wide portfolio of scientific and professional articles and studies in domestic and foreign journals.

Anna Molnár – is a Professor and Head of the Department of International Security Studies at the Ludovika University of Public Service, Budapest. She is the Head of the International Security and Defence Studies bachelor and master program. She received her PhD in international relations from the Corvinus University of Budapest (2003). Her published papers cover a wide range of topics focusing on security studies, EU Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP), Europeanisation of Hungary, the European Union's Mediterranean policy and on the Italian history and politics. She gives courses at Hungarian and foreign universities on EU CFSP/CSDP, European integration, international studies and Italian politics.

Dany Shoham – has PhD in medical virology, Tel Aviv University. Presently a Senior Researcher at the Begin Sadat Center for Strategic Studies, Bar-Ilan University, Israel; specifically in the field of biological and chemical warfare. Formerly a Senior Analyst in the same field at the Analysis and Production Division of the IDF Directorate of Military Intelligence (mainly covering the Arab countries and Iran).

Paul Tudorache – is a field artillery officer of the Romanian Land Forces, currently working as a Professor at the "Nicolae Bălcescu" Land Forces Academy of Sibiu. He completed doctoral and habilitation studies in Military Sciences at the "Carol I" National Defence University where he is a PhD coordinator. His expertise area covers multidomain operations, especially decision-making in full spectrum operations. He has authored valuable books and scientific papers in the field of Military Science, most of which focus on research directions and strategies for innovating and revolutionising military capabilities.

The second volume offers a selection of topics suggested for elective seminars on the subject matter, providing its readers with practical knowledge for understanding the hybrid phenomenon and its practices. This textbook highlights the different tools and approaches on hybrid warfare, and provides for case studies and methodology, as well. Russia, a par excellence user and inventor of hybrid warfare means and tools, appears in many of this book's chapters. The role of proxy wars is also introduced and analysed together with the questions of biosecurity, chemical, biological and nuclear warfare. The book introduces the establishment and functioning of the European Centre of Excellence for Countering Hybrid Threats and puts emphasis on the methodology analysing the most representative conceptual models for understanding the framework of hybrid threats, and the adversary's strategies, operations and tactics. Today, citizens are organised worldwide through virtual networks that consume, produce and spread information at an incomprehensible speed. The fragility and underlying dangers inherent in this phenomenon are also examined, pointing out the "blurring boundaries between the real and the virtual" and the possibility for mass manipulation and other forms of digital hybrid warfare. Most of the chapters provide an excellent basis for thought-provoking debates and group exercises entailing creative and innovative thinking.

9 789636 531065