Hybrid Warfare Reference Curriculum Volume I

Edited by
Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS

Hybrid Warfare Reference Curriculum
Volume I

Hybrid Warfare Reference Curriculum
Volume I
Compulsory Lectures

Edited by
Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS
Budapest, 2024

Disclaimer: This book was developed in the framework of the Hybrid Warfare project that has received funding from the European Commission's ERASMUS+ Programme under grant agreement 2021-1-HU01-KA220-HED-000032179. The information in the publications and on the website does not necessarily reflect the views of the European Commission.


Funded by
the European Union

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.

ISBN 978-963-653-031-0 (print)
ISBN 978-963-653-032-7 (ePDF)
ISBN 978-963-653-033-4 (ePub)

Contents

Introduction 7

Andrew Dolan: A New Concept for Waging War 13

Eado Hecht: Defining Hybrid Warfare 31

Boglárka Koller – Attila Marján – Péter Tálas: Global Megatrends 51

Nicola Cristadoro: Ideologies and Motivations 71

Jaroslav Kompan – Milan Turaj – Michal Vajda: Operational Environment 99

Romana Oancea – Ilie Gligorea – Aurelian Raţiu – Isabela Dragomir: Cybersecurity 129

Paul Tudorache – Ghiță Bârsan: Strategies to Counter Hybrid Threats 159

Vojtech Jurčák – Ján Mišik: Risk Analysis 181

About the Authors 197

This page intentionally left blank.

Introduction

It is a commonplace to state that the form of war is constantly evolving. In the contemporary conflict environment, hybrid actors and proxy groups often 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 underlies 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 UK 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 full-scale escalation started in 2022 in Ukraine – but missing from European universities' study programmes. The present curriculum

takes into account the diversity of actions forming part of hybrid warfare, uniting a variety of disciplines. Built upon 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, including the analysis of several known cases, 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 operations, 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

These 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 for finding 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 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 or to improve existing efforts. Moreover, we are living in a time when different generations may see the world dramatically differently. Therefore, the 20th century's experience must reach out to the 21st century's enthusiasm 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 that 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 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, first volume offers the basis for theoretic lectures on the subject matter, providing its readers with the background essential for understanding the hybrid phenomenon and its context. It explains the different concepts of a hybrid war and introduces ways to define hybrid warfare. It gives an overview about the megatrends weighing heavily on global security, such as demographic, climatic and economic challenges and the trends allowing for the incitement and involvement of the masses to be used for waging hybrid wars. Different ideologies and motivations are introduced from around the globe and operational aspects are taken stock of. The team deemed it important to put the cyber threats – and cybersecurity – in focus as an overarching element in hybrid warfare. This volume ends with different strategical approaches on how to prepare for and counter hybrid threats and ways to assess and evaluate security risks. 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

Andrew Dolan[1]

A New Concept for Waging War

Trying to define hybrid warfare has been likened by one academic, to an attempt to "capture the complexity of 21st-century warfare, which involves a multiplicity of actors, blurs the traditional distinctions between types of armed conflict, and even between war and peace".[2] Even as a shorthand description, one feels that there is much more to say and recent geopolitical events in Europe would tend to reinforce the point that precision, in terms of the definition of hybrid warfare might be a Holy Grail of war studies. Perhaps a more profitable route, as some commentators have suggested, is that instead of seeking precise definitions, one might be better served by considering the typical contours of major conflict and to ascertain where one can detect continuity or change.[3] Accounts and definitions of hybrid conflict might also benefit from asking pertinent questions as to what would hybrid – in terms of warfare – actually mean. For those familiar with only a single form of land warfare, they would see hybrid in the use of maritime power for example. Others might see the use of air power as a new dimension of warfare when it arrived but these are big picture frames of reference and one might suspect that conflict today does not reflect this significant pivot in the deployment of force.[4]

Hybrid Warfare as a concept

When Frank Hoffman deliberately or inadvertently set a descriptive benchmark for new and evolving forms of conflict in a 2007 article, he defined hybrid warfare as "different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of non-state actors".[5] Undoubtedly, this holistic description seemed to capture the

1 Centre for the Study of New Security Challenges.
2 Wither 2020: 7–9.
3 Fridman 2022; Strachan 2013.
4 Strachan 2013.
5 Hoffman 2007: 14.

essence of what was happening in the world at that time in terms of violent and sub-violent threats to peace and stability. Hoffman's explanation correctly brought to the fore some important abstract considerations and concepts such as the challenge to traditional perceptions of conflict, of the loss by the state of the monopoly of violence, of the wider attraction for aggressive parties to use proxy actors to further their aims or to disguise their intentions and the importance of coordination of effort, which relies on this variety of forms and actors. Less emphasis was placed on discussions suggesting whether most, if not all of the above, had been absent or in proximity to conflict.[6] Hoffman was not advocating that traditional forms of conflict would be abandoned – especially by states – but that the utilisation of other forms of pressure could equally deliver results and advantage in conflict. Of course Hoffman was aware and time has demonstrated that many of these new forms of conflict have been accentuated or added to by the onward march of technological development.[7] For example, cyber warfare in 2007 is not what it seems to have evolved into today. The actual deployment of Lethal Autonomous Weapon Systems (LAWS) and the potential for further associated weaponry, including advanced drone systems on the battlefield have come of age today – not in terms of concepts for use perhaps but in terms of scale, lethality and quantity. Weaponry displaying significant upgrades in speed, payload or AI-infused connectivity and control, are significantly impacting the battlefield or counterterrorist operations but certainly not to the extent that we cannot recognise the context of the traditional utility of force. Where does conflict or battlefield technology improvement end and hybrid warfare begin?[8] This is a legitimate question and one, which is given insufficient attention. Many commentators on hybrid warfare seek to build upon Hoffman's early definitional foray but actually, whether they agree or disagree with the specifics of the definition, is less important than a recognition, that complexity as a factor is critical. One is not only witnessing complexity in a technological sense but complexity as a factor in relation to decision-making. Blending these components together in order to develop a coherent policy, strategy and range of operational and

[6] Arguably this was not the intent of the author.

[7] Even a cursory glance at reputable military technology journals – for example produced by Jane's Publishers – such as Jane's Defence Weekly allows the student to keep abreast of military technology and its use.

[8] Military technologists will say that no explicit pivot is applicable to all contexts and conflicts which of course hampers the search for a complete definition of hybrid.

tactical options, does tend to reinforce the concept of hybrid.[9] Perhaps, therefore, it might be appropriate at this juncture to pursue the main lines of Hoffman's descriptions of the factors that underpin the need for new definitions of conflict, before returning to an assessment of whether hybrid is more important as a cliché for describing conflict in our times or if it does accurately reflect a significant shift in how mankind has evolved its conflict resolution, especially those based on violent action.

Key aspects of Hybrid Warfare

Essential to any definition of hybrid warfare is to undertake a tentative review of what might be the main features of this perceived novel description of contemporary conflict. It is also undeniable that any such review must regularly be audited, if nothing else, in order to keep abreast of actual developments in the field so to speak. Indeed, as Europe comes to terms with significant conflict on its own doorstep in Ukraine, it is not unreasonable to use the policies, operations and tactics unfolding daily to reflect on how we frame our definition, its efficacy and use as a descriptor for those analysing the conflict and in extremis, to assess whether it is sufficiently novel for the general public to perceive a difference in forms of conflict.[10] It is quite often overlooked that Hoffman and others never suggested that hybrid warfare would eliminate the need for conventional military operations. Some commentators have admittedly suggested that certain forms of military applications such as tank deployment for example might be nullified by certain enhancements in anti-tank technology. Perhaps they have a point. However, by any measure of analysis, conventional military operations still predominate in modern conflict but that the way that conventional operations are planned and executed might reflect more a shift in combat risk assessment, particularly in relation to the integration of new and emerging technologies as a force multiplier.[11] Yet it would be churlish to ignore the effect that new forms

[9] Wither 2016: 73–87.

[10] A typical example is the early Ukraine conflict analysis by Professor Michael Clark, Fellow of King's College London, on the UK's Sky News which early on framed elements of the conflict as hybrid but the term seems less used, perhaps the novelty factor has been lessened by more traditional images of war.

[11] Payne 2021.

of weaponry are having and might have on the conduct of future conventional operations, such as in a state to state struggle currently in Ukraine or in a state's response to asymmetrical engagements. So long as a technology can continue to drive weapon enhancements or create new forms of weapon, then it is unlikely that they would not be a feature of military planning, procurement and deployment. Of course an aspect of hybrid warfare as outlined by Hoffman and others and which impacts on this conventional underpinning is the involvement of irregular forces as a support to conventional operations. Is this a novel feature of conflict today? Not really as the integration of irregular forces and operations into more traditional forms of engagement has a well-established pedigree and by definition only supports the hybrid warfare concept because of our understanding of the abstract concept of hybrid as opposed to any novelty in utilisation.[12] For the foreseeable future, traditional norms of the utilisation of force will remain the bedrock of any concept or definition of warfare. The introduction of new forms of military hardware will undoubtedly impact on how such conventional force is used. New and emergent battlefield weapons, ranging from enhanced anti-tank weaponry or artillery counter battery assets will blend with enhanced C4 and communications-based networked situational awareness to make new weaponry faster, more accurate, have a loitering capacity or simply become more kinetic.[13] As mentioned above, many commentators emphasise the non-state actor dimension of hybrid warfare. Of course being non-state is no determinant of conflict generating capability, structure or intent. Groups such as Hezbollah in Lebanon clearly demonstrate the potential that such irregular groups have to influence local conditions on the ground during a conflict.[14] Key to understanding this integration, however, is perhaps the issue of purpose and less capability. For any state actor, having such an association can often disguise a state's true intent and offer plausible deniability when an operation is undertaken to advance one's true goals and objectives. Political deniability in the context of global relations is exceedingly important and this ability to blur the facts of responsibility and generate doubt in an opponent, especially one seeking international support, is invaluable. Such considerations of fake news or deniability of responsibility has

[12] The Russian Wagner Group has been operating in support of Russian operations for many years in places such as the Middle East and Africa.

[13] Frantzman 2021.

[14] Hoffman 2007.

been reinforced by technology and especially social media but it nevertheless complicates the issue of attribution.[15] Does this new form of activity justify or contribute to the definition of Hybrid Warfare? History would suggest otherwise. Propaganda has often been used to disseminate false information, whether to weaken an opponent's resolve, or influence their policies, strategies and operations and of course, to generate deceit and surprise.[16] Commentators of hybrid warfare and serious students of conflict studies would all agree, however, on the increasing relevance and importance of cyber operations as a fast-moving and potentially very destructive form of conflict and they would be right. Right up to a point. As we can see for ourselves in relation to Ukraine, cyber operations might not have as decisive an influence in conflict as first supposed. Would that be a fair assessment however? One of the attractive attributes of cyber capability is an ability to act anonymously and with deniability. Cyber capabilities can enhance surveillance of an opponent's secure data, damaging the networked operations of an opponent's vital national critical network infrastructure or collapse daily societal support functions within a designated area of operations.[17] Yet having the potential capability – sophisticated cyber powers in the global order are increasing – is not quite the same as using it successfully. Having a cyber capability can infer hostile intent but equally it can reflect a form of deterrence. Much more has to be considered also as to the effect of a coordinated cyber and real world operational posture, which is far more than a short-term, one-off strike. Where one might argue that it is novel is strangely enough the question of the legal and regulatory framework regarding cyber conflict. What cyber action would constitute an act of war? What cyber actions might trigger an asymmetrical response and where does the law lie there? Where sits Jus ad bellum or Jus in bello?[18] Answers to such questions are far from satisfactory but does hint at traditional definitions, rightly or wrongly, being under threat from revisionist concepts.

[15] Already, the conflict in Ukraine is raising numerous incidences of fake news and deepfake videos as part of the conflict narrative and propaganda war.

[16] Galeotti 2022.

[17] UK National Cyber Strategy 2022.

[18] Such questions have been a staple diet of international symposia and debate for well over a decade.

Associated activities

A defining feature of the debate surrounding the definition of hybrid warfare is the extent to which commentators seize on a range of activities which can influence conflict and as such, seen as tools of warfare. This list of actions seems to fluctuate depending on one's particular perspectives on conflict and its conduct. This regular shift in emphasis of what might constitute supporting conflict – related measures, require some thoughtful consideration. Sir Henry Wotten, a seventeenth century English diplomat once defined an ambassador as more or less "an honest man sent to lie abroad for the good of his country".[19] Was it ever thus? Modern diplomacy has many functions within the confines of supporting state policy and one must assume that elements of it can be aimed at furthering national aims and objectives in a period of tension or conflict. What else could be expected of one's diplomats abroad? Of course it is to be hoped that the quality of your diplomacy might persuade others of the righteousness of your policies and convert others to see the world as you do. More synthetic and duplicitous perhaps could be the use of diplomacy to eschew truth and generate falsehood. The repetition of a narrative at variance with your opponent's perspective or stated position on an issue fosters dubiety at best and deception at worst. The question remains, however, does the use of diplomacy actually signify hybrid warfare or is this simply the best use of whatever means you have at achieving some form of influence over the behaviour of others, particularly influential neutral parties.[20] One of course might speculate as to other forms of behaviour, certainly not diplomacy per se but rather the utilisation of diplomatic staff and facilities and indeed international diplomatic legal norms to support other forms of engagement. Embassies have often been abused as protected sites for the placement of non-diplomatic officials, the creation of false documentation and even the smuggling of weapons. There are numerous ways that state actors with malicious intent can abuse diplomatic protocol just as much as diplomats can abuse the truth in the service of government policy.[21] Before leaving this 'associated measure', one should not overlook the nexus between diplomacy and intelligence collection. It is hardly possible to imagine a situation whereby

[19] Brind 1999.

[20] Richardson 1994.

[21] An interesting example might be found in the series of recent UN Security Council debates on aspects of the conflict in Ukraine.

diplomacy does not reflect the need to learn more of the intentions and capabilities of friends and foe alike. Can this spill over into a more aggressive measure to acquire knowledge or to influence or suborn others? Most definitely yes! In essence, diplomacy and statecraft is frequently a handmaiden of a state's military actions. That this should be so seems historically and functionally obvious.[22] One could legitimately argue over the definition of terrorism as much as hybrid warfare. Throw irregular warfare into the mix and an overarching definition becomes ever more elusive. Some experts have argued cogently that terrorism or aspects of it can quite easily be integrated into a wide spectrum form of warfare. Terrorism in particular has the capability of engaging and tying down significant numbers of opposing combatants, either Army or Police, thus deflecting them from more traditional or essential purposes. Terrorism can be target-specific or target-indiscriminate depending on the objectives. Terrorism can deny space or mobility within a specific boundary.[23] Integrating such potential, however, is not so straightforward – assuming a perfect identification and harmonisation of interests cannot be taken for granted and it is not inconceivable that operational cohesion might be jeopardised through conflicting priorities. Certainly there is much to ponder regarding how a state can best exploit terrorist actions or a campaign of irregular warfare in a particular target state of interest, especially if it is a neighbouring state and one has an ability to influence the level and direction of terrorism or irregular warfare. The potential for disguised or deniable action would be considerably heightened.[24] The coordination of terrorist or irregular warfare activities with more traditional forms of conventional warfare is not new. The important feature to observe, however, is less the activity and more the coordination. It is the level of coordination that might push opportunism into actual policy. Interfering in another country's affairs through policies of disinformation and the manipulation of electoral practices has become a frequent talking point of late. That it exists seems hardly in doubt, especially if one examines the formal government reports regarding interference in the elections in the last USA elections or even the Brexit referendum in the UK. Such subversion reminds one of the general atmosphere during the Cold War, where both blocs regularly attempted to influence or interfere in

[22] Omand–Phythian 2018.

[23] Jasper–Moreland 2014.

[24] This is particularly so regarding North Korean and Iranian use of military assets as commercial entities in relation to WMD proliferation activities.

the affairs of the other, mostly without great success. So-called 'Active Measures' is hardly new.[25] Today, it is exceptionally difficult to appreciate how effective such interference could be. Those commentators who regularly point to the internet and social media platforms as tools for online manipulation do so from a point of view that sees the message as the main problem. Others see technology as the primary concern, in so far as it facilitates manipulation and structured messaging in a way that precludes viable alternative messaging. Part of this concern is well understood by those whose area of expertise is psychological warfare and who regularly exploit the vulnerabilities of internet governance or media freedoms in general.[26] Yet to better appreciate the nature of the activity under consideration, one must acknowledge that there are wider factors at play and that have more to do with changes and movement in the individual's perspective on issues such as data harvesting, information management, online commerce and privacy than simply being discerning about the likes and dislikes of a particular message.[27] That interference in the internal affairs of another state goes on is not in question. That it happens through the exploitation of new communications technology can be a concern but perhaps a greater concern is the fear of such behaviour leading to more sophisticated monitoring and surveillance and ultimately control of the internet in your opponent's state. The war in Ukraine has highlighted once more the use of economic sanctions, as a suitable tool for seeking to inflict damage or pain on an adversary or as a way to modify behaviour. It can be an attractive policy option, as it certainly does not envisage the use of traditional kinetic force.[28] That said, economic warfare generally or targeted sanctions specifically are not morally or ethically neutral. They are, as a tool of coercion, designed to inflict pain and suffering on the intended target – it is the level of pain and suffering that is often associated with economic warfare that generates dispute. As to their efficacy, the jury is possibly 'out' on that. Targeted or 'smart sanctions' against the likes of Iran or North Korea under the auspices of the United Nations in order to modify their behaviour as regards nuclear weapons development has failed to meet expectations. The EU and the G7 sanctions on Russia as a result of the action in Ukraine have also

[25] Rid 2021.

[26] Hearing before the Select Committee on Intelligence of the U.S. Senate on Policy Response to the Russian Interference in the 2016 U.S. Elections.

[27] Ibid.

[28] It also introduces an element of deniability.

clearly failed in their intention of modifying Russian behaviour.[29] Of course modifying vital interests of an adversary is one thing. Denying routine access to general or specific economic or financial markets is another and it is difficult to conceive that such sanctions do not raise the threshold of disruption to strategic supplies or essential commodities. More often or not, economic sanctions can result in the suffering of too many innocent parties in the targeted state and even within the state of the instigator of the sanctions – the so called 'blowback effect' can hit one's own people and economic interests.[30] Such results inevitably lead to speculation as to whether so-called 'smart sanctions', the spearhead of economic warfare, are really as sharp as people anticipated or that the terminology simply disguises a blunt weapon. Additionally, is the judicious use of economic actions, alongside other forms of military or paramilitary action, really a new form of warfare? Few commentators today are likely to agree.[31]

Definition or distraction

Away from the contentious issue of seeking to define what is a hybrid war lies a rich field of study on why seek to define it in the first place. Furthermore, as even this brief review above hopefully demonstrates, even those activities, which arguably represent the constitutive parts of hybrid warfare, are themselves subject to dubiety. Why should this be the case? Part of the problem of defining hybrid warfare lies in part with society's penchant for simplifying complex concepts as if this process can and does make the issue more transparent or manageable in terms of understanding. In terms of hybrid warfare, this is certainly not the case. In part, slick definitions have also been a feature of military studies discourse. Not that long ago we had concepts such as Network Centric Warfare, Deep Strike, Deep Battle and Asymmetrical Warfare as semaphores for a certain discourse on the utility and utilisation of force. Such concepts engendered significant and contentious debate as military strategists posited their opinions on the significance of these military policy applications, often supported by

[29] At the last count, the EU has initiated 9 sets of sanctions – incremental actions but also reflects that influencing Russia's behaviour through economic sanction is not easy.

[30] The EU debates on energy supplies and the cost of energy is typical of the blowback in this arena.

[31] Mulder 2022.

operational analysis based on real applications of force or larger scale conflict. The lessons learnt culture is alive and well in military circles and each and every global conflict of any import is studied and analysed to identify potential force multipliers.[32] However, as European militaries in particular shifted focus from the Cold War to small scale regional conflicts, much of it in support of state building or peace-keeping policies, it was understandable that traditional forms of warfare would adapt or in some cases, go out of business, even if only temporarily. Yet the need for definition remained; under the rubric of expeditionary warfare, it was becoming apparent that less traditional forms of operation were required, if not as the primary form but at least an important element of it. However, as the complexity of a globalised world took root, the requirements of military application did not wither on the vine but rather became a stop-gap sticking plaster against which it sought to maintain peace and security against a raft of diverse and often novel threats, risks and challenges.[33] Under such conditions, it was inevitable that the study of modern forms of conflict would generate new but non-specific concepts that were difficult to pin down and describe. The term hybrid warfare was merely one effort at packaging the complexity in a form that might have supported concentrated analysis and crucially, thinking on dealing with some of the new abstract issues within the hybrid definition.

Hybrid conflict concepts

A primary consideration regarding Hybrid Warfare is the issue of complexity. How does one go about planning and controlling a strategic engagement with the component parts equally complex and requiring a no small amount of finesse in terms of direction and leadership? Obviously decentralisation is essential but the trend today is to encourage political leadership to have intimate control of military or military-political applications. Whether we like it or not, it is not unusual to have civilian commanders-in-chief both observe and in effect make decisions on tactical actions that have strategic impact, whether this is regarding the killing of a high value terrorist target or the decision to use force against an

[32] This is the whole point in establishing and maintaining military educational institutions.

[33] These conflicts ranged from Iraq and Afghanistan to Sierra Leone and Mali.

adversary state target on foreign soil.[34] There is every reason to believe that such blurring of command and control function is likely to become a permanent feature of how modern democratic states wage war. The devolution of control and responsibility for military action in a hostile environment – a traditional feature of the chain of command system most of us are familiar with – might be modified in the future to better integrate or embed civilian authority, including legal authorities, with the option to overrule military authority when they see fit.[35] Further emphasis in this aspect of conflict does seem to suggest that in a way, a form of hybrid command and control will evolve in such a way as to give some meaning and additional substance to those arguments, which clearly recognise the hybrid nature of warfare.[36] At the other end of the spectrum of warfare evolution is the notion of ceding various forms of authority – in other words, command and control – to machines or at least machine intelligence. It is nigh on impossible to ignore the military application of artificial intelligence (AI). Such applications include not only more versatile and faster missile technology such as hypersonic platforms, surveillance systems, maritime domain robotic controlled vessels or stealth torpedoes and of course the phenomenally successful drones. Enthusiasts of military AI salivate over the potential regarding some nanotechnologies and smart materials as a vital component of the combat soldier of the future.[37] Impressive as these examples are, however, the main concern seems to lie in ceding authority to certain types of Lethal Autonomous Weapon Systems, especially those, which adopting loitering functions, can determine what target to engage and when, absent the human in the decision-making loop. Technical experts will argue that this independence is not complete but as the debates at the UN on banning such weapons has revealed, the ability to cede a kill authority is a technical application away, a mere 'weapon of math destruction' as one writer described a range of capabilities generated by algorithms.[38] Inherent in this direction of military development is a more realistic component or contribution to hybrid warfare. The time is coming when the battlefield might be populated by a novel form of man and

[34] President Obama and Hilary Clinton observed U.S. forces undertake the attack on Bin Laden in his Pakistani compound.

[35] The embedding of legal officers at unit level in the Israeli Army is a case in point.

[36] There are interesting parallels to the Soviet military's use of political officers.

[37] Weissmann et al. 2021.

[38] O'Neil 2016.

machine cooperation, the augmentation of the man and aided by ever-sophisticated applications of AI-inspired weaponry.[39] Another complexity and abstract consideration governing the early thinking on the 'why' of hybrid warfare was the subject of the exploitation of information or data as we might prefer to describe it today. This was an abstract consideration as the traditional forms of information warfare were being impacted by exciting and imaginative technical applications, not only in terms of communications and the forms of communication but also more interestingly on the exploitative potential related to data as a concept. The problem for military strategists was not that information warfare was divorced from strategic planning but rather what was this more indeterminate product – data – and how might it be exploited? Like many a new technology, the early military association with the internet would be superseded by cutting-edge technology start-up companies that easily surpassed the military in its application and exploitation of data, albeit for commercial advantage.[40] Today, this situation concerning data exploitation is hard-wired throughout society and the number of self-empowered actors has proliferated. So too has their products and capabilities to such an extent that states often rely on their technical applications to augment their own capabilities. Additionally, in response to the profit motive, these data empowered entities have both offered and are implementing levels of networked data applications throughout our societies, certainly generating significant energy saving application for the individual and society but inadvertently creating levels of networked vulnerabilities that can, if targeted in a conflict, leave flourishing societies defenceless and exposed to malicious influence from destruction to blackmail.[41] Incorporating critical network infrastructure into national defence is not new. We have already spoken of cyber vulnerabilities. What is novel is the level of integration and connectivity encouraged by system network functionality and the fact that it was never constructed with security in mind. We actively undertake the protection of nuclear sites for example but do we invest similar amounts on protecting the 'Cloud' and its associated power supplies?[42] A sad but worrying feature of conflict since Frank Hoffman coined his hybrid warfare phrase has been the

[39] Frantzman 2021.

[40] Interestingly, U.S. DARPA still continues to fund commercial companies in this sector.

[41] This explains much of the activism of groups such as those opposed to the deployment of lethal Autonomous Weapons Systems.

[42] Kissinger et al. 2021.

willingness on the part of state and non-state actors to develop weapons of mass destruction, primarily chemical. However, there is a growing suspicion that several states might be exploiting developments in life sciences, particularly through the enhancements afforded by artificial intelligence. As the recent global pandemic has highlighted, our societies are exceedingly vulnerable to the ravages of certain viruses and bio-security has become a matter of some urgency and concern in security circles. The protection of hazardous materials and the processes and research that goes with them is a challenge and for the time being, there is an inadequate global structure to manage such concerns.[43] It would be inconceivable that states would not be taking note of such developments in the bio-security domain and equally inconceivable that non-state actors would fail to see the potential applications, certainly as a possible method for mass destruction but equally to acquire leverage in any form of ransom action. Here then is a form of activity that could augment traditional forms of military action, particularly if the agent is manageable and containable. Some will argue and at times successfully that biological warfare is an unstable application of force and as such, difficult to adequately control and direct. However, life scientists will counter this and point to the phenomenal power of AI-inspired techniques that can empower the developer and make precision strikes possible and even desirable in some contexts.[44] Hoffman and his successors were alive to such possibilities but again the devil is in the detail. Under what circumstances would a biological warfare component of a wider strategic military application fit in to such a concept? Perhaps the answer might lie in the timing of such an action. Using a managed biological warfare action well in advance of a more traditional use of force – especially when the target society has been weakened or seriously depleted by their bio-response or simply because they lack resilience – might tip the balance in the eventual application of conventional arms. Under such a scenario, the term hybrid might have some merit.[45] Finally, attention can be drawn to a few other aspects of deliberate state behaviour, which might constitute an asymmetrical tactic in support of wider military or coercive behaviour against individual adversaries or groups of adversaries. Here, one might consider

[43] Kissinger et al. 2021.

[44] Advocates of AI-enabled weapons frequently cite the fact that AI weapons are devoid of emotions and not subject to the stresses and strains of conflict and how this might negatively influence a soldier on the battlefield.

[45] Hoffman 2007.

the use of the displacement and movement of large numbers of refugees or migrants, the deliberate withholding or controlling of water sources and denying food supplies to stimulate serious hunger and perhaps famine. Europe has recently been subjected to state-sponsored manipulation of refugees by Belarus in order to modify the policies of the EU. Such behaviour, including the deliberate deception of migrants and refugees with a promise of safe entry to the EU, deliberately flouts international norms of behaviour and puts the refugees and migrants at terrible risk. The Belarusian authorities used such a coordinated move to deliberately seek to punish its neighbours for imposing EU-inspired sanctions against Belarus and the fact that it failed and resulted in a climb down by Minsk has not lessened the lessons to be drawn from such policies.[46] Similar examples abound with regard to clashes over water rights – which generally occurs in parts of the world where sufficient supplies of natural water, is at a premium. It is worth pointing out however that such manipulation can be either short-term or, if part of a longer strategy of attrition, a long-lasting affair and likely to have a significant environmental impact for many years after. The current Russian blockade on Ukrainian grain supplies is very similar to the above and must be measured as a short-term measure. The move is seen as an attempt to both ensure the short-term lifting of international economic sanctions against Moscow and equally to damage Ukrainian economic standing in the wider international community and influence the international perspective of the conflict. Indeed, should there be sufficient economic and social dislocation as a result of the denial of access to food supplies, some countries might witness the beginnings of new migration flows away from impoverished and hungry states to the richer northern and predominantly EU states.[47] The above actions can easily be seen as useful components of hybrid warfare but it is worth noting that it is not the type of action that would generate immediate strategic gain. It is difficult to predict let alone control such phenomena once unleashed and such a degree of unpredictability – unless that be the ultimate objective – is fraught with potential complications that might not work to the advantage of those who would initiate such actions.

[46] Rudnik 2021.

[47] An often overlooked fact in this dispute is that Russia is keen to have its fertiliser transferred without sanctions.

Conclusion

Clausewitz once noted that "every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions".[48] It is difficult to disagree with such an assessment. Commentators differ as to what hybrid warfare actually is, although there is a degree of consensus on the fact that numerous forms of military and supporting activity can have a bearing on the conduct of modern warfare. These activities, however, tend to reinforce the application of new concepts based on the potential inherent in new technologies for example or new forms of strategic thinking regarding the exploitation of the globalised networking of societies, in essence a recognition of the 'dual-use' function of much of society's basic systems and infrastructure and methods of interacting. A simple recent blockage of ships transiting the Suez Canal and the delays and shortages of both consumer and essential goods it generated, can be replicated in wartime as the Russians have demonstrated in the Black Sea. Hybrid warfare has never been – indeed it would have been difficult to justify – a totally novel form of warfare but is rather a reflection of how one might engage in conflict between interconnected parties in a more connected and technically globalised environment. That parties to a hybrid conflict might choose to use both dedicated and dual-use assets in an imaginative way can easily be placed alongside the realities of asymmetrical engagement, including kinetic, and the interest of non-state parties, who are not invested in the full panoply of state interest. Yet it would be futile to deny that something seems to have changed regarding warfare. For many communities, it represents a backward step in international politics, an environment, which such subscribers to this view, suggest is becoming less violent. That might be so but the facts on the ground deny wishful thinking and point to modes of conflict, which, through emerging technologies, are affording opportunities to use force and other forms of pressure, in creating an interconnectivity of a full spectrum of forms of violent persuasion and action. It is worth speculating, however, as to where a truly hybrid warfare concept might arise if what we are managing is not it? The total militarisation and integration of space operations could very well justify such a label. Total war in the cyber realm could be another. Perhaps a future robot war or a machine–human integration could change the face of battle. Think the unexpected. Perhaps the only thing that is certain is that conflict stimulates analysis and emulation and time will lend itself to the evolution of even

[48] Clausewitz 1993: 727.

newer forms of conducting war. For the purist and traditionalist, such evolution might be unwelcome but at the end of the day, Clausewitz will still recognise the principles of war at work.

Questions

1. Explain the reasons why you think that Frank Hoffman coined the phrase hybrid warfare in his 2007 article and state if you agree or disagree with his thinking.
2. What features of modern conflict do you think best contribute to an understanding of hybrid warfare and indicate how this is evidenced in the current Russia–Ukraine war?
3. Hybrid warfare: continuity or change? Discuss.
4. Which future developments in modern conflict might reinforce the notion that war is truly hybrid and how might this impact European security?
5. How should military training establishments in the EU recalibrate their thinking and methods in the light of the current war in Ukraine, as a typical example of modern hybrid conflict?

References

Brind, Harry (1999): *Lying Abroad: Diplomatic Memoirs.* London: Lying Abroad: Diplomatic Memoirs.

Clausewitz, Carl von (1993): *On War.* New York: Everyman's Library.

Frantzman, Seth (2021): *Drone Wars. Pioneers, Killing Machines, Artificial Intelligence, and the Battle for the Future.* New York: Bombardier Books.

Fridman, Ofer (2022): *Russian 'Hybrid Warfare'. Resurgence and Politicisation.* London: Hurst and Co.

Galeotti, Mark (2022): *The Weaponisation of Everything. A Filed Guide to the New Way of War.* New Haven: Yale University Press.

Hoffman, Frank (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies.

Jasper, Scott – Moreland, Scott (2014): The Islamic State Is a Hybrid Threat: Why Does This Matter? *Small Wars Journal,* 12 February 2014. Online: https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter

Kissinger, Henry A. – Schmidt, Eric – Huttenlocher, Daniel (2021): *The Age of AI. And Our Human Future.* New York: Little, Brown and Company.

Mulder, Nicholas (2022): *The Economic Weapon. The Rise of Sanctions as a Tool of Modern War.* New Haven: Yale University Press. Online: https://doi.org/10.2307/j.ctv240df1m

Omand, David – Phythian, Mark (2018): *Principled Spying. The Ethics of Secret Intelligence.* Washington, D.C.: Georgetown University Press. Online: https://doi.org/10.2307/j.ctvvngtm

O'Neil, Cathy (2016): *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy.* New York: Crown.

Payne, Kenneth (2021): *I, Warbot. The Dawn of Artificially Intelligent Conflict.* London: Hurst and Co.

Richardson, Bill (1994): Crisis Management & Management Strategy: Time to "Loop the Loop"? *Disaster Prevention & Management,* 3, 59–80.

Rid, Thomas (2021): *The Secret History of Disinformation and Political Warfare.* London: Profile Books.

Rudnik, Alesia (2021): *The Belarusian Diaspora and Its Role in Solving the Political Crisis.* Online: https://frivarld.se/wp-content/uploads/2021/11/Belarus-Diaspora-Rapport.pdf.

Strachan, Hew (2013): *The Direction of War.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9781107256514

Weissmann, Mikael – Nilsson, Niklas – Palmertz, Björn – Thunholm, Per eds. (2021): *Hybrid Warfare. Security and Asymmetric Conflict in International Relations.* London: I.B. Tauris.

Wither, James K. (2016): Making Sense of Hybrid Warfare. *Connections,* 15(2), 73–87.

Wither, James K. (2020): Defining Hybrid Warfare. *per Concordiam,* 10(1), 7–9. Online: https://perconcordiam.com/defining-hybrid-warfare

Further reading

Caliskan, Murat – Cramers, Paul Alexander (2018): What Do You Mean by "Hybrid Warfare"? A Content Analysis on the Media Coverage of Hybrid Warfare Concept. *Horizon Insights,* 1(4), 1–14.

Deshpande, Vikrant (2018): *Hybrid Warfare. The Changing Character of Conflict.* New Delhi: Pentagon Press.

Kaihko, Ilmari (2021): The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession. *Parameters,* 51(3), 115–127.

McFarland, David (2021): *Understanding Hybrid Warfare. Navigating the Smoke and Mirrors of International Security.* Independently published.

Mumford, Andrew (2020): Understanding Hybrid Warfare. *Cambridge Review of International Affairs,* 33(6), 824–827. Online: https://doi.org/10.1080/09557571.2020.1837737

Murray, Williamson – Mansoor, Peter R. eds. (2021): *Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present.* Cambridge: Cambridge University Press.

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

Van der Venne, Timothy (2021): Old Wine, New Bottles: A Theoretical Analysis of Hybrid Warfare. *E-International Relations,* 30 November 2021.

Vračar, Milinko S. – Ćurčić, Milica T. (2018): The evolution of European Perception of the Term 'Hybrid Warfare'. *Vojno Delo,* 70(1), 5–21. Online: https://doi.org/10.5937/vojdelo1801005V

Eado Hecht[1]

Defining Hybrid Warfare

Definitions and terminology are important. They help us explain and understand phenomena and convey ideas relevant to those phenomena. Conversely, once they have been determined, they tend to restrict the way we interpret reality as it occurs around us. A wrong, inaccurate or imprecise definition or term may prevent us from understanding events and steer us to choose the wrong action or reaction. Therefore, though the choice of definitions and terminology is important in all fields of human endeavour, because of the extremely high price of mistakes in the conduct of war, the choice of definitions and terminology relevant to war is especially important. The term hybrid warfare was chosen to describe a conceptual military problem facing the U.S. and NATO in understanding a particular aspect in the conduct of war. Therefore, before defining hybrid warfare, it is necessary to understand its context. The term warfare is generally defined as the act of waging war against an enemy, or, in a narrower sense, as a specific manner of conducting war. This requires the addition of a term describing that unique manner as distinct from other different manners of warfare, thus for example, hybrid warfare.

Defining war

So what is war? According to the Prussian General and military theorist Carl von Clausewitz: "War is nothing more than large-scale duel […] an act of violence to force our will upon our opponent […] the objective of the war is not part of the war itself […]. War is the continuation of the political intercourse with the addition of other means."[2] Chinese Communist leader Mao Dze Dong provided a variation such as "politics is war without bloodshed, while war is politics with bloodshed".[3] Whereas most people assume that Clausewitz was referring only to states or at least nations, and Mao was referring to the socio-economic strata within a state or nation, British historian John Keegan argued that any group of

[1] Bar-Ilan University and Begin-Sadat Center for Strategic Studies.
[2] Clausewitz 1832: 8.
[3] Dong 1938: paragraph 64.

people can and do conduct Wars; "war antedates the state, diplomacy and strategy by many millennia. Warfare is almost as old as man himself".[4] As history shows, individuals sometimes employ violence as a tool to achieve various goals. Groups of individuals, not just states, do the same – the difference being that they do so in concert and to gain an accepted common goal that benefits the group as a whole, though not necessarily every individual in that group. The process of agreeing on the common goal, the process of working to achieve it are an act of politics and the relationship with other groups are the political intercourse referred to by Clausewitz.[5] However, one-sided violence motivated by a political purpose is not yet war – to become war the violence must be mutual. The reciprocity of violence is a point stressed repeatedly by Clausewitz as an inherent part of the essence of war – if one side attacks and the other side is passive, neither defends nor attacks, it is not war. So war is violence employed as a tool to achieve a political goal against a rival reciprocating with violence to deny that achievement while achieving his own political goals.[6] Thus the definition of war reads as follows. War is purposeful reciprocal violence between groups of people. When groups of people are in conflict they each have a number of tools they can employ to compel, induce, entice or convince their rivals to give in to their opposing demands: direct or indirect negotiations, economic pressure or inducements, overt or covert psychological and information influence operations, third-party arbitrators and violence. The conduct of war does not necessarily preclude or even reduce the continuation of efforts to simultaneously achieve the group's goal also by the other available tools. War might be chosen as the main effort, supported by the other tools, or only as a supporting effort to the other tools.[7] Hybrid warfare is therefore a specific method of conducting violence by a group in order to compel a rival group to agree to its political demands. However, as in many other aspects of military theory, there is no one generally accepted definition for what violent actions or modes of action are included in the specific phenomenon termed hybrid warfare. Furthermore, as will be described below, even the terminology used for defining this phenomenon varies.

4 Keegan 1994: 3.
5 Clausewitz 1832.
6 Clausewitz 1832.
7 Clausewitz 1832.

Evolution of the term Hybrid Warfare

In 1993, Captain Eric F. McMillin, published an MA thesis on the First Lebanon War (1982). In that war Israeli military forces fought both the military forces of the Palestine Liberation Organization and those of Syria. McMillin focused his study on the confrontation between the Israelis and the Palestinians and found a problem defining the type of warfare conducted in that confrontation: "A new 'middle way' of warfare emerged, though through no design of the antagonists. It was not guerrilla warfare with an elusive foe refusing decisive engagement with a superior conventional foe. Neither was it a contest between the armies of two states on the open battlefield as, ironically, both the PLO and the Israelis would have preferred. Rather a low technology, relatively untrained and unseasoned, largely militia force was able to preclude a powerful state army, stripped of its technological edge and limited in the freedom to use its overwhelming firepower, from achieving its war aims."[8] Not having a term to define this form of warfare he declared it to be a "new 'middle way' of warfare". However, he was mistaken – it was not new. Three years later, in 1996, Dr. Thomas Huber of the U.S. Army Combat Studies Institute, published a study on Napoleon's attempt to conquer Spain (1808–1814) and highlighted the combined use of regular and irregular forces in regular and irregular modes of operation by Napoleon's enemies. He termed this combination compound warfare.[9] This study became the basis for an anthology of case studies published in 2002 analysing a variety of compound warfare campaigns (including two earlier than Napoleon's war in Spain) but neither the article nor the anthology generated enough interest to create a general debate on the concept.[10] One of the first, if not the first, use of the term hybrid warfare was in a book published by historian Thomas R. Mockaitis on British counterinsurgency wars from the 1960s till the mid-1990s. He dubbed the war between Indonesia and Malaysia, the latter assisted by Britain, a "hybrid war, combining low-intensity conventional engagements with insurgency".[11] The hybridity was not only in the purely military issues. Indonesian strategy was "a combination of subversion, diplomatic pressure and military incursions […]. While [Indonesia] could never hope to defeat the British militarily, [it] might

8 McMillin 1993: iii.
9 Huber 1996.
10 Huber 2002.
11 Mockaitis 1995: 14–15.

use their presence to portray Malaya as a puppet state and Rahman [Prime Minister of Malaya] as a 'colonial stooge'. He might also provoke the British into a retaliatory attack across the border that would create a favourable international incident".[12] Indonesian military actions combined the use of irregular forces and regular forces to conduct irregular warfare operations and actions – small to medium – sized harassment raids, with regular warfare operations in which they attempted by those same forces to grab and hold small pieces of Malayan territory. The British responded in kind as they too employed regular and irregular forces, adapted strategies, operations and tactics developed during the 19th century and first half of the 20th century to defeat insurgencies inside the British Empire and tribal plunder raids entering British Empire territory from beyond its borders to what was in fact an inter-state conflict (Malaysia–Indonesia) combined with an insurgency (communist and ethnic inside Malaysia), generally conducted at low intensity with occasional brief escalations, but never crossing the threshold to all-out high-intensity warfare. In 1998, in an MA thesis written at the U.S. Naval Postgraduate School, a United States Marine Corps officer, Robert G. Walker, described the U.S. Marine Corps as "a hybrid force, capable of conducting operations within both the conventional and unconventional realms of warfare".[13] He defined hybrid warfare as "that which lies in the interstices between special and conventional warfare. This type of warfare possesses characteristics of both the special and conventional realms, and requires an extreme amount of flexibility in order to transition operationally and tactically between the special and conventional arenas".[14] Walker conflated Unconventional Warfare and Special Operations, even though the latter are only one type of the former.[15] In 2002, the same year that the anthology on compound warfare was published, another U.S. Marine, William J. Nemeth, wrote an MA thesis entitled *Future War and Chechnya: A Case for Hybrid Warfare.* Nemeth's discussion focused on the societal changes that were occurring in a variety of non-Western states in which the modern state was devolving into something different, a hybrid society that still included the trappings of the modern state organisation, but in which older, tribal organisations were returning to the fore of political organisation and conduct. These societal and political transformations, were, argued Nemeth,

[12] Mockaitis 1995: 16.
[13] Walker 1998: v.
[14] Walker 1998: 4–5.
[15] Walker 1998; *Department of Defense Dictionary of Military and Associated Terms* 1989.

creating a new paradigm of war, one which was different and incomprehensible to Western cultures.[16] So, whereas Walker used the term Hybrid Warfare to describe a variation in tactics and operations amalgamating different methods emanating from a purely military decision, Nemeth's approach was political. Changes in social organisation created changes in the manner societies organised and employed war "hybrid societies are a mixture of the modern and the traditional. Hybrid societies in turn have organized hybrid military forces, and it is these forces that will challenge military and diplomatic planners in the future […]. The intention of this thesis is to establish the links between hybrid societies, hybrid warfare and pre-state societies and warfare".[17] As a modern case study Nemeth chose the Russo–Chechen conflict of 1994–2002. The Chechen forces combined an indigenous martial culture of irregular warfare with Soviet military training in regular warfare and experience in Soviet army ranks in the Soviet–Afghan War (1979–1989) as well as various conflicts in the Caucasus as the Soviet Union collapsed. This, argued Nemeth, enabled them to merge the advantages of each in order to defeat the Russians in 1995–1996. The thesis was written before the end of the second round of war between Russia and Chechnya which was won by Russia and therefore does not describe why Russia ultimately succeeded in re-conquering Chechnya. Three years later, in a 2005 professional lecture and article by U.S. Marines General James A. Mattis and Frank G. Hoffman, they adopted fellow Marine Walker's purely military term hybrid warfare with a slightly expanded definition.[18] The expansion encompassed the entirety of what the American military regarded as unconventional warfare, and is more commonly known as irregular warfare or guerrilla warfare. Hoffman continued to develop the term over the following years in a series of studies and articles, however, the best known of his papers, the paper that made this term popular among military theorists and practitioners, was *Conflict in the 21st Century: The Rise of Hybrid Wars,* which, in addition to describing his understanding of the occurring transformations in the conduct of war included a case study of the recent 2006 war between Israel and Hezbollah. That war that had seen the highly touted Israel Defense Forces apparently fail to defeat what was considered to be a weak guerrilla-style military force. The sensation caused by that war lead to a deluge of writing trying to explain the unexpected results,

16 Nemeth 2002.
17 Nemeth 2002: 3–4.
18 Mattis–Hoffman 2005: 18–19.

and Hoffman's monograph rode that wave of interest in providing a theoretical framework for understanding it and publicising the concept of hybrid warfare. Ostensibly, Hezbollah's success was achieved by merging regular and irregular modes of combat – a combination the Israeli military failed to cope with, i.e. hybrid warfare.[19]

Blurring of war forms

The goal of the discussion on compound or hybrid warfare was not to develop a general military theory. It was focused on the context of threats potentially facing the U.S. The heart of the argument was that whereas in the past the U.S. had faced different types of enemies separately, whether states employing "conventional capabilities" or non-states employing "asymmetric or irregular tactics", in the future "these may no longer be separate threats or modes of war". Instead there would be "an increased merging or blurring of conflict and war forms" and therefore, "future contingencies will more likely present unique combinational or *hybrid* threats that are specifically designed to target U.S. vulnerabilities […]. There are a broadening number of challenges facing the United States […]. These include traditional, irregular, terrorist and disruptive threats or challengers. [Planners must choose] between preparing for states instead of separate challengers with fundamentally different approaches (conventional, irregular or terrorist) we can expect to face competitors who employ *all* forms of war and tactics, perhaps simultaneously. Criminal activity may also be considered part of this problem as well, as it either further destabilizes local government or abets the insurgent or irregular warrior by providing resources, or by undermining the host state and its legitimacy".[20] None of these forms of action was new in itself – the novelty was in the amalgamation as "at the strategic level, many wars have regular and irregular components. However, in most conflicts, these components occurred in different theaters or in distinctly different formations.[21] In Hybrid Wars, these forces become blurred into the same force

[19] Hoffman 2007.

[20] Hoffman 2007: 7.

[21] Hoffman adopted Huber's term, 'Compound Warfare' for these strategically coordinated but geographically and organisationally separate operations, arguing that all the examples studied in the anthology were not hybrid – i.e. combined units conducting combined operations in the same

in the same battlespace. While they are operationally integrated and tactically fused, the irregular component of the force attempts to become operationally decisive rather than just protract the conflict, provoke overreactions or extend the costs of security for the defender".[22] Though Hoffman stated that "Hybrid Wars can be waged by states or political groups, and incorporate a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".[23] The focus of his discussion and choice of the Second Lebanon War case study was on the hybrid threat posed by non-state actors, because, following the dissolution of the Soviet Union, they were deemed to be the more likely enemy of the U.S. and were the challenge cited repeatedly as examples for hybrid forms of action. And, in fact, the U.S. and its allies were at that time fighting non-state rivals in Asia and Africa (various Moslem Jihadi organisations). State on State War seemed to be a thing of the past.[24] However, at the same time, the political and strategic situation in Europe was changing with the resurgence of an active Russia. Russia was actively engaging in a variety of activities perceived by NATO members to be confrontational but problematic to define. Though Hoffman and most U.S. theorists discussing the subject till 2014 mentioned that part of the essence of hybridity was also the blurring of the boundary between war and peace, they focused on the operational and tactical hybridity within a war.[25] Writers focusing on the evolving political situation in Europe, especially following Russian actions in Ukraine, were more concerned with political and strategic hybridity – the merging of hostile activities, some non-violent and yet disruptive politically, such as the use of covert operations,

space and time. This article also addressed the problem of having more than one definition of Hybrid Warfare (see Hoffman 2009).

[22] Hoffman 2007: 8.

[23] Hoffman 2007: 58.

[24] This opinion was promoted first by a variety of academic researchers whose ideas were adopted by some military commanders. Typical examples are Creveld 1991: 33–62; Kaldor 1999: 15–31, 71–93; Kaldor 2005: 2–3; Kaldor 2013; Smith 2005: 3–30; Gat 2012: 149–157; Hecht–Shamir 2016: 124–127. Smith's book was translated by the Israel Defense Forces (IDF) to Hebrew in 2013 and declared required reading for all IDF officers.

[25] Note that all the writers quoted above, including those in the anthology published by Huber, discussed only the operational and tactical aspects of hybrid warfare. This is true also of all the articles in the anthology edited by Murray–Mansoor 2012. Nemeth ascribed the source of the Chechens' ability to conduct warfare to be cultural and societal, but he too focused on the operational and tactical levels (see Nemeth 2002).

psychological and information operations, disruptive economic actions and cyber operations to destabilise states, with a sprinkling of semi-covert violent acts of extremely low intensity such as assassinations or destruction of property and occasionally a more powerful but still very limited overt military action, sometimes using proxies and sometimes not, all this without officially declaring war.[26] Given the West European cultural preference to clearly delineate a separation between war and not-war, participants and non-participants, this fuzzy area which merged the two situations was the main dilemma facing European governments and military establishments – for them hybrid warfare was the deliberate conduct of hostile operations of this nature. Thus in an official NATO website the hybrid threat is defined as: "Hybrid threats combine 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. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies. The speed, scale and intensity of hybrid threats have increased in recent years. Being prepared to prevent, counter and respond to hybrid attacks, whether by state or non-state actors, is a top priority for NATO."[27] The European Centre of Excellence for Countering Hybrid Warfare defines hybrid warfare as: "An action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution. Hybrid action is characterized by ambiguity as hybrid actors blur the usual borders of international politics and operate in the interfaces between external and internal, legal and illegal, and peace and war. The ambiguity is created by combining conventional and unconventional means – disinformation and

[26] Note the official definitions by NATO and the European Centre of Excellence for Countering Hybrid Warfare below and see a long list of essays on the threat posed by Russia. Typical examples are Bērziņš 2014; Hoffman 2014; NATO 2015; Kofman 2016; Hughes 2016; Murphy 2016; Fedyk 2017; Fox 2017; Pronk 2018a; Fridman 2018; Jonsson 2019; Rumer 2019; Bērziņš 2020: 355–380; Bowen 2020; Käihkö 2021: 115–127.

[27] NATO 2021; NATO 2015; Pronk 2018b.

interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare."[28] This definition adds a nuance absent from previous definitions. Only covert actions, those below the threshold of detection and attribution, are included. However, this requirement in the first paragraph contradicts the use also of "conventional" means and warfare mentioned in the second paragraph. A similar, previous and separate development occurred in the U.S. Army under the heading Full Spectrum Operations. This concept, which was not adopted outside the U.S. Army, was first described in that army's *Field Manual 3-0: Operations* in 2001 and further developed in the later 2008 update of that manual: "This edition of FM 3-0 reflects Army thinking in a complex period of prolonged conflicts and opportunities. The doctrine recognizes that current conflicts defy solution by military means alone and that landpower, while critical, is only part of each campaign. Success in future conflicts will require the protracted application of all the instruments of national power—diplomatic, informational, military, and economic. Because of this, Army doctrine now equally weights tasks dealing with the population—stability or civil support—with those related to offensive and defensive operations. This parity is critical; it recognizes that 21st century conflict involves more than combat between armed opponents. While defeating the enemy with offensive and defensive operations, Army forces simultaneously shape the broader situation through nonlethal actions to restore security and normalcy to the local populace."[29] However, later versions of the manual, though mentioning the need to maintain the capability to operate in all the above-mentioned fields, dropped the term Full Spectrum Operations. The U.S. Army has not officially adopted the term hybrid warfare in its doctrine.

Changing the culture of war

What is clear is that the issue that most distresses NATO members is the blurring of the boundary between war and not-war. This is a cultural issue. A school of thought that developed gradually in Western culture and became prevalent in the second half of the 20th century, sought to create a distinct boundary

[28] Hybrid CoE s. a.
[29] The Pentagon 2008: vii.

between the two situations. A clear distinction between what behaviour is war and what is not; who may conduct war and who may not; what actions are acceptable or not-acceptable in war, what actions are acceptable or not-acceptable in conflicts that are not-war. These distinctions were codified as the Laws of War, thus converting the discussion from a focus on best practice to a focus on legality of practice. This created two world views – NATO members and others accepting this strict delineation as opposed to other entities that do not. It also created a problem for those accepting the boundaries and laws to understand the behaviour of those who do not – how can an action be not-war yet look and behave as war? Existing terminology and concepts, sharply separating the two, prevented the ability to discuss what was happening. The term hybrid warfare was adopted to solve this problem. War and not-war are separate political and military phenomena, hybrid warfare is a conceptual patch covering the gap between the two and slightly overlapping each. In 2013, Russian Chief of the General Staff Valery Gerasimov, lectured on the topic of hybrid warfare as a political and military phenomenon.[30] Though often described as the Gerasimov doctrine, this lecture actually described Gerasimov's interpretation of Western doctrine of modern warfare and the need for Russia to learn to cope with it.[31] He too focused first on the "tendency toward blurring the lines between the states of war and peace". But after stating that "wars are no longer declared", he added, "and having begun, [they] proceed according to an unfamiliar template".[32] This new template includes "the broad use of political, economic, informational, humanitarian and other non-military measures – applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict […]. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The defeat of the enemy's objects is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. The application

30 Gerasimov 2013.
31 Adamsky 2015; Galeotti 2018; Galeotti 2020.
32 Gerasimov 2013.

of high-precision weaponry is taking on a mass character. Weapons based on new physical principals and automatized systems are being actively incorporated into military activity […]. Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected".[33] However, though these new forms of action were more and more prominent, and the focus of that particular lecture, they did not completely erase the use of older forms of action – the employment of massed mechanised formations, as was made clear in the graphs that accompanied the lecture and in later lectures, various articles published in Russian professional journals and Russian military exercises, and in the invasions of Ukraine in 2014 and 2022.[34] Analysts studying the Russian debate attempted to separate the Russian concepts from the Western concepts, or from the Russian understanding of Western concepts as they were described in the Russian professional journals, by using the Russian term New Generation Warfare for the Russian concept and Hybrid Warfare for the Western concept. However, though there are differences in the details, in principle these two concepts are indeed similar as far as the separation of War and Not-War are concerned and the general internal composition of the military operational and tactical methods, including the exploitation of new technologies by those methods, are concerned.[35] To summarise it, the term hybrid warfare came to refer to two separate phenomena – first, a style of purely military operational and tactical actions and second, a style of aggressive political behaviour combining military and non-military actions. Unfortunately, as the term hybrid warfare gained popularity it lost clarity. The various concepts, definitions and terms represent a professional debate on the topic. Some of the debaters merely sought to improve previous ideas and definitions as they understood them, some sought to adapt them to the specific contexts they were facing, others tried to delineate the boundaries of the concept back to a form of

[33] Gerasimov 2013.

[34] Gerasimov 2013; Sutyagin 2015; Bartles 2016: 30–38; Kofman 2016; McDermott 2019: 345–378; Bērziņš 2020: 355–380; Clark 2020; Polyakova–Boulègue 2021; Zarembo–Solodkyy 2021.

[35] Jonsson–Seely 2015: 1–22; Thomas 2016: 554–575; Schnaufer 2017: 17–31; Bērziņš 2019: 157–184; Suchkov 2021: 415–440; Baqués 2021.

behaviour in war rather than between war and not-war and others argued that the concepts and terminology were wrong and harmful.[36] Evolving with each new paper written about it, the term became a slogan covering a plethora of hostile behaviours, activities and organisations in a wide variety of military and non-military contexts, some of which had existed before under different names, while others, lacking violence, were not truly war. When a term comes to mean many different things, it becomes useless as a tool for communication. Another problem is that while defining Hybrid Warfare the various authors were not and still are not precise in their use of terminology, thus, for example, conventional, traditional and regular warfare are used interchangeably though there are subtle differences in meaning as are unconventional, guerrilla, asymmetric and irregular warfare. Terrorism, itself lacking an agreed definition,[37] is now a separate category of actions. For state armies there are War, Military Operations Other than War and Operations Below the Threshold of War. The terms war and warfare themselves lost coherence – one experienced General even wrote that war no longer exists – though the various violent activities that make-up a war such as confrontation, conflict and combat still do,[38] whereas an academic specialising in political science claimed that war existed but had changed drastically into something new. New War was characterised by what she claimed to be new political goals and new forms of violence.[39] Furthermore, a plethora of new terms were invented, some preceded the term hybrid warfare, others were alternatives suggested by various authors such as Fourth Generation Warfare, Fourth Epoch Warfare, New Warfare, Post Modern Warfare, Degenerate Warfare and Compound Warfare, which preceded the term hybrid warfare while others sought to focus on a particular aspect for example the Grey Zone emphasising the use of violence without officially declaring war, or Political Warfare that focus on all hostile actions that do not include violence.[40] Some of the discussions

[36] Stoker–Whiteside 2020; Schadlow 2015.

[37] NATO Counter-Terrorism Reference Curriculum 2020.

[38] Smith 2005.

[39] Kaldor 1999. New, slightly revised editions, responding to various criticisms were published later but the essential argument remained the same. The criticisms focused on the historical inaccuracy of her claims that the political goals and forms of violence were new.

[40] The term 'Political Warfare' (defined as "the employment of all the means at a nation's command, short of war, to achieve its national objectives") was originally invented by U.S. State Department Policy Planning Director George Kennan in a Top Secret memorandum entitled *The Inauguration of Organized Political Warfare,* written on 30 April 1948. Kennan explained the necessity for the

approached the topic from a purely military aspect – tactics, operations and strategy and their effect on the conduct of wars, whereas others approached the topic from the opposite direction, the cultural and political developments that preceded, initiated and directed wars and the forces established to conduct them to achieve the ideological and political objectives set by the societies and their leaders. Many of the terms used actually define more the cultural or strategic tunnel through which the user was observing the world than the general reality of war as a practical phenomenon. Many of the criticisms published against each author's work were against that tunnel vision misleading him/her. Proponents of theories claiming a break from past experience to a new reality were often criticised for exhibiting insufficient knowledge of the history of warfare.[41]

Conclusion

None of the arguments are completely wrong and none are completely right. War is one of the most complex of human activities. It exists and is fought on all the physical, the emotional, the spiritual and the mental planes of human existence, it invokes both rational and irrational behaviour. It is therefore difficult to define it and the phenomena that compose it with mathematical precision. Many phenomena that in theory are distinct do not have precise borders with adjacent phenomena in practice, the transition from one to the other is often gradual with a considerable overlap – there are many shades of grey, but where each shade specifically ends and another specifically begins is usually very difficult to discern. Given that the very essence of hybrid warfare is the merging of phenomena, it is especially difficult to define, to characterise and to create a distinct theory as to how to conduct it successfully. However, if we are to conduct a meaningful discussion and come away with the common understanding necessary for coordinated actions, it is necessary to provide definitions useful to practitioners while accepting the blurry edges of each phenomenon. As noted

term because: "We have been handicapped however by a popular attachment to the concept of a basic difference between peace and war, by a tendency to view war as a sort of sporting contest outside of all political context." It was suggested as a more intuitively more understandable replacement for the term Hybrid Warfare when discussing hostile non-violent actions. However, the term elicited a negative response (Robinson et al. 2018: xix–xx).

41 Berdal 2003: 477–502; Berdal 2011: 109–133; Cohen 2007; Mello 2010: 297–309; Newman 2004: 173–189; Roberts 2005.

above, the term hybrid warfare as it is most commonly used today refers to two separate phenomena:

- On the political-strategic continuum the concept termed hybrid warfare refers to the combined use of all the tools available to the belligerents to force their rival to accept their political demands – all forms of aggressive diplomacy, economic actions, psychological and information actions and violent actions. All these may include a mix of overt and covert actions. As regards the acts of violence, these may be official (declared war) or unofficial (undeclared war).
- Within the internal continuum of conducting war (methods of conducting violent operations) hybrid warfare refers to the combined use of the different manners of military action, both regular warfare and irregular warfare.

Therefore, when using the term hybrid warfare, the user must make clear to which of the two phenomena he/she is referring to. Both phenomena of hybrid warfare affect the chosen military strategy for a particular war and its implementation; however, each does so differently. They are not conditional to each other, they can co-exist or one may be chosen and implemented while the other is not.

Questions

1. What conflicting definitions of Hybrid Warfare do you know?
2. What other terms are used as equivalents to the term Hybrid Warfare?
3. What are the main obstacles to the adoption of a single universally accepted term and definition for Hybrid Warfare?
4. What are the similarities and differences in the definition of Hybrid Warfare?
5. What common elements exist within the various definitions of Hybrid Warfare?
6. Is having a precise single definition of Hybrid Warfare necessary for conducting Hybrid Warfare operations?
7. How could differences in definitions affect the implementation of the Hybrid Warfare concept?
8. How should the use of the same term for two separate phenomena be resolved?

References

Adamsky, Dmitry (2015): *Cross-Domain Coercion: The Current Russian Art of Strategy.* IFRI Security Studies Center. Online: www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

Baqués, Josep (2021): La versión rusa de la guerra híbrida [The Russian Version of Hybrid Warfare]. *Ejercitos,* 08 November 2021. Online: www.revistaejercitos.com/en/2021/11/08/the-russian-version-of-hybrid-warfare/

Bartles, Charles K. (2016): Getting Gerasimov Right. *Military Review,* January–February 2016, 30–38.

Berdal, Mats (2003): How 'New' Are 'New Wars? Global Economic Change and the Study of Civil War. *Global Governance,* 9(4), 477–502.

Berdal, Mats (2011): The 'New Wars' Thesis Revisited. In Strachan, Hew – Scheipers, Sybelle (eds.): *The Changing Character of War.* Oxford: Oxford University Press. 109–133. Online: https://doi.org/10.1093/acprof:osobl/9780199596737.003.0007

Bērziņš, Jānis (2014): *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.* Center for Security and Strategic Research, National Defence Academy of Latvia. Online: www.sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Bērziņš, Jānis (2019): Not 'Hybrid' but New Generation Warfare. In Howard, Glen E. – Czekaj, Matthew (eds.): *Russia's Military Strategy and Doctrine.* Washington, D.C.: The Jamestown Foundation. 157–184.

Bērziņš, Jānis (2020): The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies,* 33(3), 355–380. Online: https://doi.org/10.1080/13518046.2020.1824109

Bowen, Andrew S. (2020): *Russian Armed Forces: Military Doctrine and Strategy.* Congressional Research Service. Online: https://crsreports.congress.gov/product/pdf/IF/IF11625

Clark, Mason (2020): *Russian Hybrid Warfare, Institute for the Study of War.* Military Learning and the Future of War Series. 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

Cohen, Eliot A. (2007): The End of War as We Know It. Review of the Utility of Force by Rupert Smith. *Washington Post,* 18 January 2007. Online: www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801981.html

Creveld, Martin Van (1991): *The Transformation of War.* Los Angeles: The Free Press.

Department of Defense Dictionary of Military and Associated Terms (1989).

Dong, Mao Dze (1938): *On Protracted War.* Online: www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm#p1

Fedyk, Nicholas (2017): Russian "New Generation" Warfare: Theory, Practice, and Lessons for U.S. Strategists. *Small Wars Journal,* 05 April 2017. Online: https://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists-0

Fox, Amos (2017): *Hybrid Warfare: The 21st Century Russian Way of Warfare.* Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College.

Fridman, Ofer (2018): *Russian 'Hybrid Warfare'. Resurgence and Politicisation.* London: Hurst and Co.

Galeotti, Mark (2018): I'm Sorry for Creating the 'Gerasimov Doctrine'. *Foreign Policy,* 05 March 2018. Online: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Galeotti, Mark (2020): The Gerasimov Doctrine. *Berlin Policy Journal.* Online: https://berlinpolicyjournal.com/the-gerasimov-doctrine/

Gat, Azar (2012): Is War Declining – Why? *Journal of Peace Research,* 50(2), 149–157. Online: https://doi.org/10.1177/0022343312461023

Gerasimov, Valery (2013): Ценность науки в предвидении [The Value of Science in Prediction]. *военно-промышленный курьер* [Military-Industrial Courier]. Online: https://vpk-news.ru/articles/14632

Hecht, Eado – Shamir, Eitan (2016): The Case for Israeli Ground Forces. *Survival,* 58(5), 123–148. Online: https://doi.org/10.1080/00396338.2016.1231535

Hoffman, Frank G. (2009): Hybrid vs. Compound Wars. *Armed Forces Journal,* 01 October 2009. Online: http://armedforcesjournal.com/hybrid-vs-compound-war/

Hoffman, Frank G. (2014): On Not-So-New Warfare: Political Warfare vs Hybrid Threats. *War on the Rocks,* 28 July 2014. Online: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hoffman, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington : Potomac Institute for Policy Studies.

Huber, Thomas M. (1996): *Napoleon in Spain.* Fort Leavenworth: U.S. Army Command and General Staff College.

Huber, Thomas M. ed. (2002): *Compound Warfare. That Fatal Knot.* Fort Leavenworth: U.S. Army Command and General Staff College.

Hughes, Geraint (2016): Little Green Men and Red Armies: Why Russian 'Hybrid War' is Not New. *Defence-in-Depth,* 14 March 2016. Defence Studies Department, Online: https://defenceindepth.co/2016/03/14/little-green-men -and-red-armies -why-russian-hybrid-war-is-not-new/

Hybrid CoE (s. a.): *Hybrid Threats as a Concept.* Online: www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Jonsson, Oscar – Seely, Robert (2015): Russian Full-Spectrum Conflict: An Appraisal After Ukraine. *Journal of Slavic Military Studies,* 28(1), 1–22. Online: https://doi.org/10.1080/13518046.2015.998118

Jonsson, Oscar (2019): *The Russian Understanding of War. Blurring the Lines Between War and Peace.* Washington, D.C.: Georgetown University Press.

Käihkö, Ilmari (2021): The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession. *Parameters,* 51(3), 115–127. Online: https://doi.org/10.55540/0031-1723.3084

Kaldor, Mary (1999): *New and Old Wars. Organized Violence in a Global Era.* Redwood City: Stanford University Press (second revised edition 2007, third revised edition 2013).

Kaldor, Mary (2005): *Old Wars, Cold Wars, New Wars, and the War on Terror.* Lecture given by Professor Mary Kaldor to the Cold War Studies Centre, London School of Economics. Online: www.academia.edu/3444310/Old_Wars_Cold_Wars_New_Wars_and_the_War_on_Terror

Kaldor, Mary (2013): In Defence of New Wars. *Stability Journal,* 2(1). Online: https://doi.org/10.5334/sta.at

Karber, Phillip A. (2015): *Russia's 'New Generation Warfare'.* National Geospatial-Intelligence Agency. Online: www.nga.mil/news/ Russias_New_Generation_Warfare.html

Keegan, John (1994): *A History of Warfare.* New York: Vintage Books.

Kofman, Michael (2016): Russian Hybrid Warfare and Other Dark Arts. *War on the Rocks,* 11 March 2016. Online: https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

Mattis, James N. – Hoffman, Frank (2005): Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine,* 132(11), 18–19. Online: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf

McDermott, Roger N. (2019): Deciphering the Lessons Learned by the Russian Armed Forces in Ukraine, 2014–2017. In Howard, Glen E. – Czekaj, Matthew (eds.): *Russia's Military Strategy and Doctrine.* Washington, D.C.: The Jamestown Foundation. 345–378.

McMillin, Eric F. (1993): *The IDF, the PLO and Urban Warfare: Lebanon 1982*. MA Thesis, The University of Chicago, Center for Middle Eastern Studies. Online: https://ia600106.us.archive.org/11/items/DTIC_ ADA266491/DTIC_ADA266491.pdf

Mello, Patrick A. (2010): Review Article: In Search of New Wars: The Debate about the Transformation of War. *European Journal of International Relations,* 16(2), 297–309. Online: https://doi.org/10.1177/1354066109350053

Mockaitis, Thomas R (1995): *British Counterinsurgency in the Post-Imperial Era.* Manchester: Manchester University Press.

Murphy, Martin (2016): Understanding Russia's Concept for Total War in Europe. *The Heritage Foundation,* 12 September 2016. Online: www.heritage.org/defense/report/understanding-russias-concept-total-war-europe

Murray, Williamson – Mansoor, Peter R. (2012): *Hybrid Warfare. Fighting Complex Operations from the Ancient World to the Present.* Cambridge: Cambridge University Press.

NATO (2015): *Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar.* 25 March 2015. Online: www.nato.int/cps/en/natohq/opinions_118435.htm

NATO (2021): *NATO's Response to Hybrid Threats.* Online: www.nato.int/cps/en/ natohq/topics_156338.htm

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Monterrey: Naval Post Graduate School.

Newman, Edward (2004): The 'New Wars' Debate: A Historical Perspective Is Needed. *Security Dialogue,* 35(2), 173–189.

Polyakova, Alina – Boulègue, Mathieu (2021): *The Evolution of Russian Hybrid Warfare: Executive Summary.* Washington, D.C.: Center for European Policy Analysis (CEPA). Online: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary/

Pronk, Danny (2018a): *(Russian) Political Warfare: Methodology.* The Hague: Clingendael Netherlands Institute of International Relations.

Pronk, Danny (2018b): *The Return of Political Warfare.* Online: www.clingendael.org/pub/2018/strategic-monitor-2018-2019/the-return-of-political-warfare/

Roberts, Adam (2005): The Utility of Force, by Rupert Smith. *The Independent,* 11 November 2005. Online: www.independent.co.uk/arts-entertainment/books/reviews/the-utility-of-force-by-rupert-smith-326177.html

Robinson, Linda – Helmus, Todd C. – Cohen, Raphael S. – Nader, Alireza – Radin, Andrew – Magnuson, Madeline – Migacheva, Katya (2018): *Modern Political Warfare. Current Practices and Possible Responses.* Santa Monica: RAND.

Online: www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf

Rumer, Eugene (2019): *The Primakov (Not Gerasimov) Doctrine in Action.* Carnegie Endowment for International Peace. Online: https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254

Schadlow, Nadia (2015): The Problem with Hybrid Warfare. *War on the Rocks,* 02 April 2015. Online: https://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/

Schnaufer, Tad A. II (2017): Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security,* 10(1), 17–31. Online: https://doi.org/10.5038/1944-0472.10.1.1538

Smith, Rupert (2005): *The Utility of Force. The Art of War in the Modern World.* London: Allen Lane.

Stoker, Donald – Whiteside, Craig (2020): Blurred Lines: Gray Zone Conflict and Hybrid War: Two Failures of American Strategic Thinking. *Naval War College Review,* 73(1). Online: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4

Suchkov, Maxim A. (2021): Whose Hybrid Warfare? How 'The Hybrid Warfare' Concept Shapes Russian Discourse, Military, and Political Practice. *Small Wars & Insurgencies,* 32(3), 415–440. Online: https://doi.org/10.1080/09592318.2021.1887434

Sutyagin, Igor (2015): *Russian Forces in Ukraine.* Briefing Paper – Royal United Services Institute. Online: www.rusi.org/explore-our-research/publications/briefing-papers/russian-forces-ukraine

The Pentagon (2008): *FM 3-0: Operations.* Headquarters, Department of the Army.

Thomas, Timothy (2016): The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. *Journal of Slavic Military Studies,* 29(4), 554–575. Online: https://doi.org/10.1080/13518046.2016.1232541

Walker, Robert G. (1998): *SPEC FI: The U.S. Marine Corps and Special Operations.* Monterey: Naval Post Graduate School.

Zarembo, Katerina – Solodkyy, Sergiy (2021): *The Evolution of Russian Hybrid Warfare: Ukraine.* Washington, D.C.: Center for European Policy Analysis (CEPA). Online: https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-ukraine/

This page intentionally left blank.

Boglárka Koller – Attila Marján – Péter Tálas[1]

Global Megatrends

Numerous definitions have been created for describing the overarching and complex processes of the world. What they have in common is that they all define these as ones that can determine the way the world operates over a longer period of time and thus provide a possible basis for imagining future occurrences. The futurist, John Naisbitt' bestseller book, published in 1982 has been instrumental in bringing megatrends to the attention of the researchers of various fields (economists, demographers, sociologists, political scientists etc.).[2] Another futurist, David Houle argues that we live in a 'shift age', in an era of transformation determined by new evolutionary factors, thus it is crucial how humanity deals with the coming twenty or thirty years of challenges. Another scholar, Haven Allahar highlights the importance of understanding major global megatrends when deciding upon launching new policies.[3] As consequence of this increased interest in the topic, *Future Studies,* also known as *Futurology* or *Futurism,* has emerged as a unique field that focuses on the grand societal, technological and economic changes with the aim to forecast the possible scenarios of the forthcoming decades and centuries. Richard Slaughter critically reflects on the value and applicability of the megatrend concept and asks to what extent these megatrends can be used to draw conclusions for the future. In his later analysis, he provides a new methodological approach by combining the 'breadth' and 'depth' in enquiries on the future. Slaughter also contributed significantly to understand what is, and what is not a megatrend. Due to our embeddedness in our present perceptions, sometimes it is hard to differentiate them from 'game changing events', 'black swan' occurrences or even 'critical uncertainties'.[4] As an example a political one can be mentioned: The worldwide polarisation of the electorates can be considered a megatrend, nevertheless, the democratic deficit of the European Union (EU) cannot. International organisations and the

[1] Ludovika University of Public Service.

[2] Naisbitt 1982.

[3] Houle 2011; Allahar 2014.

[4] Slaughter 1993: 827–849; Slaughter 2002: 493–507; Slaughter 2013: 354–359.

European Union have also included megatrends in their vocabulary. In one of its science and innovation outlook, the Organisation for Economic Co-operation and Development (OECD) defines megatrends as "large-scale social, economic, political, environmental or technological changes that are slow to form but which, once they have taken root, exercise a profound and lasting influence on many if not most human activities, processes and perceptions".[5] The United Nation's (UN) 2020 report lists five megatrends such as 1. climate change; 2. demographic shifts and ageing; 3. urbanisation; 4. the emergence of digital technologies in the fourth industrial revolution; and 5. inequalities. "Each of these megatrends has evolved continuously over decades, developing its own dynamics, and influencing economic, social and environmental dimensions of sustainable development."[6] The EU has just recently realised that the Union has to be aware of the megatrends. Exploring the current developments and anticipating the future scenarios have to be embedded in the policy-making processes. One of the vice-presidents of the Commission was assigned to chair the task of forecasting. The first Strategic Foresight Report was launched in 2020. Since then, one has been published every year with the aim to "explore, anticipate and shape the future" and be able to provide a platform for reaching policy goals that can be only done by applying a wider perspective and being aware of the megatrends and their interlinkages.[7] Just as there are different definitions of megatrends by scholars and institutions, there are also different lists of megatrends. While acknowledging the unique approach of the various scholars, in this chapter we will use the definition formulated by the Megatrends Hub of the European Commission that defines them in the broadest possible sense: "Megatrends are long-term driving forces that are observable now and will most likely have significant influence on the future."[8] While being aware that other lists of megatrends can be composed, we will now attempt to briefly discuss the following ones in our chapter: 1. demographic changes and challenges; 2. economic power and development; 3. backsliding democracies; 4. geopolitics, security concern and securitisation; 5. climate change and the environment; 6. connectedness, information, technology and AI; 7. vulnerable individuals – identities and identity politics.

5 OECD 2016: 1.
6 UN Report 2020: 22.
7 European Commission 2020, 2021a, 2022a.
8 European Commission 2022b.

We have selected these because we think that in order to better apprehend the new generation of hybrid means used in local, regional and global conflicts, it is essential to understand the dynamics and interlinkages of these seven megatrends. Megatrends as key drivers of socio-economic and geopolitical developments are therefore key to understand the general framework of the dynamic of global power shifts and international conflicts.

Demographic changes and challenges

In late 2022, global population surpassed the 8 billion mark. The UN's principal population projection (the medium variant) suggests that the world population will grow to nearly ten billion by the middle of this century, and will level off at around 10.4 billion by the 2080s. However, if fertility declines by less than projected, the world population could exceed twelve billion by the end of the century. Urbanisation is also an important megatrend which accelerates global migration. The first year in which more people lived in urban than rural environment was 2007. By 2050 almost 70% of the world population will be living in cities.[9] The global population has been exploding in the last hundred years but according to projections it will stabilise later in the 21st century. Between 1950 and 2018, average annual population growth was 1.6%. Recently it is 1% and will decline gradually. The population of the earth is projected to stabilise at around 11 billion. Even if the global population stabilises around that figure, unsustainability both economically and environmentally seems a real issue. Moreover, many of the world's least developed countries have populations projected to double between 2022 and 2050, while the populations of more than 60 countries are expected to decrease in the coming 25 years due to declining fertility, especially in high income countries, such as the member states of the EU.[10] The global population is ageing on average: the share of the population over age 65 will rise from 5% in 1950 to 15% in 2050 and further up to 25% by 2100. 2018 was a global demographic turning point: the planet had more people aged 65 years and over than children under five for the first time in history. Having said this there is considerable diversity across regions: Europe, Japan

[9] United Nations 2022.
[10] United Nations 2022.

and the United States are ageing most rapidly, thereby losing their labour-force base at a quick pace. These trends point to a sustained and long-term migration pressure on European countries. Europe is particularly vulnerable regarding demographics, unless a radically different policy approach to the old-age pension systems is established. Otherwise, the European pension systems and in a broader sense, the European social model will most probably prove to be unsustainable. The recent experience of complex difficulties with the integration of third country nationals into the European labour market and the new waves of immigration imposes additional burdens on states and the EU. The general trend of overpopulation, and radically different age-composition of EU and African countries, coupled with climate unsustainability and the possible emergence of regional conflicts around its border puts a massive and complex security pressure on Europe both EU and nation state level. The radical increase (doubling in hardly more than a generation) of the dependency ratio (ratio of retirees over the active population) in every EU member state is one of the most powerful and highly underrated trends that impacts not only the labour market, but the general budgetary stability and in the medium-term the sustainability of the European social model and also the political system of the European Union. The inherent instability of the European demographic situation (persistently low fertility rate – way under the minimal 2.1 – standing around 1.5), the unprecedented demographic ageing of the society, coupled with ever more evident policy failures related to labour force import by immigration is also a game changing phenomenon in the long run. Unless tackled efficiently, the negative demographic trends in the EU will result in further erosion of societal peace and security.[11] Migration from insecure and poor regions of the neighbourhood is a long-term reality for Europe. The stark difference of the age tree and the level of security and wealth between Europe and most of its immediate neighbouring areas will guarantee that the migratory pressure on Europe will be sustained for several generations. Migration and the potential mismanagement of it remains a direct and indirect security challenge for the EU and most of its member states, moreover migration has already been and will most probably be weaponised by adversaries of the EU and its adversaries.

[11] Marján 2010.

Economic trends

There is a major realignment taking place in the global economic power equilibrium, while still the West accounts for the majority of global economic production. Moreover, countries with shrinking labour forces (typically highly developed western countries) contribute to 90% of today's global economic growth. At the same time the main centres of continued population growth are in the Indian subcontinent and Sub-Saharan Africa, and this latter will account for over a quarter of total population growth for the rest of the 21st century. The portion of the world living in high income countries will fall from 32% in 1950 to 10% by 2050.[12] The most remarkable element of this global realignment is the rapid increase of China's global economic clout which, by 2022 clearly has geo-political consequences and the realisation thereof in Western political thinking. The U.S. was first to react to China's ever more assertive economic expansion both in terms of exponentially growing production and international trade and foreign direct investment activities and major bilateral and multilateral deals worldwide (mainly Africa and Asia). Projections now are inconclusive whether and if so when the Chinese economy overtakes the U.S. as number one in the world as China seems to have to cope with multiple challenges recently. The U.S., especially since the Trump Administration, later further intensified by the Biden Administration ramped up its counter-China economic actions, clearly connecting economy with geopolitical and security considerations. Compared to the traditional toolbox of trade barriers mostly in the form of customs duty rise and imposing trade barriers, the drastic measures of 2022 related to the trade ban on high-end microchips (involving coordination with other major international players, such as Taiwan and South Korea) represent a wholly new level of economic war. Europe was slower to engage in a more stringent stance towards China in the economic warfare, but it is clearly on a similar path, rendering for instance incoming Chinese investments more difficult. Economic tensions between the EU and the U.S. were also on the rise (although this was overtaken by the historically close cooperation between the two powers in relation to the war in Ukraine). The controversial U.S. legislation, the Inflation Reduction Act of 2022 that provides 350 billion subsidy to

[12] Quillin 2019.

high-end companies, including those active in clean energy made strong waves in EU capitals that are afraid of losing key industrial bases by investments and companies relocating to the U.S. This posed a major policy challenge in Europe, whether or not keep up its traditional libertarian economic model, or follow the American example to allow massive state intervention in sectors of key importance. In general, due to several factors, such as the Covid lockdowns, the global economic slowdown, the heightened level of geopolitical competition between the U.S. and China, multiple ruptures in the global supply chains, the Russian aggression in Ukraine dealt a series of blows to globalisation. A fundamentally trade and investment based global order seems to be over. Geopolitical and security considerations are getting ever more important in the global economic policy decisions and practice. This would probably have negative impact on the global output and wealth and ironically the major loser of a fractured global economy will be China. Russia will probably slide further back globally as an economic, geopolitical and military power, probably isolated for a long time from the West, notwithstanding the end result of its war against Ukraine. Similarly to the future global security framework that will see a fractured system, in which two blocks, West–East will compete ever more intensively, the global economic landscape will also be based on a two-block opposition including the separation of key business areas such high-end chip production, robotisation, artificial intelligence development, further eroding globalisation. The rising level of tensions in economic competition, especially in high-end technological sectors, like semiconductor production points beyond economy and stems from national security concerns, therefore upping the possibility of escalation to measures beyond traditional trade disputes.

Backsliding democracies

"The world has been in a mild but protracted democratic recession since about 2006."[13] But as Carothers and Press argues, although democratic backsliding is a global trend in politics, there is not an agreement on its drivers.[14] The rise

[13] Diamond 2015: 145–155.
[14] Carothers–Press 2022.

of autocratic leaders, often supported by undemocratic regimes like China and Russia, the digital transformations and changes in media consumption as well as the rise of various forms of surveillance, economic inequalities, rise of populism and intensified political polarisation can all be blamed for leading to democratic backsliding.[15] There are several democracy measurements and indexes available with different data sources and methodology. One of the most referred and acknowledged one is the V-Dem Institute's yearly published democracy report that includes separate indexes on electoral, liberal, participatory, deliberative and egalitarian traits of democracies based on more than 470 indicators and a unique methodology. As the V-Dem Institute's latest democracy report argues: "The level of democracy enjoyed by the average global citizen in 2021 is down to 1989 levels. The last 30 years of democratic advances are now eradicated."[16] As the report argues, democratic decline is apparent in Asia-Pacific, Eastern Europe and Central Asia, Latin America and the Caribbean.[17] While in 2012 42 states could be characterised as liberal democracies, in 2021 this number is only 34, which is the lowest level in 25 years, while autocracies and dictatorships are on the rise worldwide. Further, as the V-Dem experts argue, the world has significantly changed in ten years' time in terms of democracies. Toxic political polarisation, threatened freedom of expression lead to a sharp increase of the number of people who live in autocracies worldwide.[18] Another widely cited index was developed by the Economist Intelligence Unit. The biennially published index analyses the state of democracy in 167 countries along five aspects: electoral process and pluralism, functioning of government, political participation, political culture and civil liberties. On the basis of experts' opinion, countries are given scores and put into four main categories of regimes: full democracies, flawed democracies, hybrid regimes and authoritarian regimes.[19]

15 Carothers–Press 2022.
16 V-Dem Institute 2022: 6.
17 V-Dem Institute 2022: 12.
18 V-Dem Institute 2022.
19 EIU 2022.

Table 1: EIU Democracy index by regime types (2022)

	No. of countries	% of countries	% of world population
Full democracies	24	14.4	8.0
Flawed democracies	48	28.7	37.3
Hybrid regimes	36	21.6	17.9
Authoritarian regimes	59	35.3	36.9

Note: "World" population refers to the total population of the 167 countries and territories covered by the Index. Since this excludes only micro states, this is nearly equal to the entire estimated world population.
Source: EIU

In 2022, 45.3% of the world population lives in full and flawed democracies but only 8% in full democracies, while 17.9% in hybrid and 36.9% in authoritarian regimes. While in 2006 51.3% of the world population lived under some sort of democracy (full or flawed) and 13% in full democracies. (United States of America also fall out of the category of a full democracy in 2016.) In other words, the number of people living in democracies has been steadily decreasing. However, the number of people who live in hybrid or authoritarian regimes has been increasing. It was 48.4% in 2006, and it is 54.8% now. Nevertheless, in the aggregate ratio, the number of people living in hybrid regimes has increased significantly, while the number of people living in authoritarian regimes decreased slightly since 2006.[20] Although the democracy indices can be criticised for their data collection and datasets as well as their applied methods, they do support the assumption that democracies are in decline worldwide and the number of people living in democracies has been steadily decreasing.

Geopolitics, security concerns and securitisation

From a geopolitical point of view, the most likely scenario for the coming years is that the international system will continue to move towards a post-hegemonic world order.[21] In particular, through a process wherein the hegemonic power of the former hegemon – the U.S. – is challenged in the various areas (political,

[20] EIU Democracy Index by regime types, 2006, 2022.
[21] Callahan 2008: 749–761; Vezirgiannidou 2013: 637–651.

economic and military power, also diplomatic influence and model value), as well as its former hegemonic role at the global and/or regional level. Consequently, the hegemon and its allies are unable or unwilling to maintain the previous international power structure.[22] They do not want to uphold it as it already serves their opponents better and the 'cost' of maintaining it remains mainly on their shoulders, or they cannot maintain it, because their challengers are simply stronger advocates. The main actors in this process will be the powers and states defending or challenging the status quo. Challenging the status quo can take place in different dimensions – e.g. territoriality, system of rules, ideological theorems, functioning and the mere existence of institutions, etc. – and by different means – e.g. economics, diplomacy, war and proxy war, hybrid means, etc.[23] The most important conflicts of the near future will take place between these actors, and since the dependency on globalisation in the event of such conflicts carries serious risks (see Europe's position in the Russia–Ukraine war and its dependency on Russian energy), the de-globalisation and the elimination of the resulting dependency will be one of the main concerns of the major powers involved in the conflicts. Although the pace of change and the conflicting nature of the post-hegemonic world order will depend on many factors, in particular on the extent to which its actors revert to spheres of interest politics and post-hegemonic wars waged by major powers (e.g. Russia–Ukraine), it seems certain that in order to avoid direct war between major powers, the opposing parties will resort to hybrid threats more often than in the past.[24] The latter is understood as a set of military and non-military means and methods, whose coordinated use makes it possible to impose the will of the aggressor on the target state. The non-military toolbox of hybrid threats may include political, diplomatic, administrative, economic, financial, energy, information, cyber, intelligence, terrorist and criminal pressure, pressure on critical infrastructure, the use of radical social groups, political forces and movements, mobilisation of national and ethnic minorities, artificially triggering a migration wave, etc. It is important to note, that non-military hybrid instruments can also be asymmetric instruments, and are therefore present in the toolbox of non-state actors and weaker state actors (Iran, North Korea) as well, not limiting hybrid conflicts to major powers. Hybrid threats also include the use and threat of use of irregular

[22] Ikenberry 2018: 15–29; Juutinen–Käkönen 2016.
[23] Cooley–Nexon 2020; Kailong 2022.
[24] Sinkkonen 2022: 121–131; Bargués et al. 2022.

armed groups, private military companies and regular armed forces. In other words, in the post-hegemonic era, global or regional geopolitical actors may more often use hybrid threat instruments such as:

- the use of information and communication technologies to achieve geopolitical objectives
- the use of externally financed and controlled radical social groups, political forces and movements to artificially induce migration flows in order to destabilise the socio-political situation in a country
- the use of covert humanitarian activities
- the increased involvement of irregular armed groups, private military companies and civilians
- increased activities of foreign secret services
- the use of fabricated propaganda, deniable forces, intelligence, mobilisation of minorities in enemy territory
- terrorism

In parallel with the growth of hybrid threats, the role of resilience in national and international security policy is increasing.[25] In other words, the set of capabilities of the state, society and individuals that enable them to face and respond effectively to hybrid threats, and to resist effectively and restore rapidly the working order in the event of an open armed attack, natural disaster, or damage to vital system elements. A key element of strengthening resilience will be whole-of-government and whole-of-society preparedness, including strengthening military capabilities.

Climate change and the environment

Negative trends in climate change and environmental degradation will continue in the coming years, even if the steps and processes that had been initiated to curb them continued at an optimal pace, which, based on our experience so far, is unlikely. In practice, this means that even in the most optimistic scenario, the only success will be in reducing the scale and pace of climate change and environmental degradation, mitigating their effects, and adapting effectively to the changes they bring about. In other words, we must continue to expect

[25] Jacobs et al. 2022: 3–19.

rising temperatures, melting ice sheets at the North and South Poles, rising sea levels and flooding of coastal regions. As a result of climate change, extreme weather events such as storms, floods, heat waves, droughts and forest fires will continue to occur more frequently and more intensely in the coming years. Meanwhile, we can also expect that climate change and environmental degradation, and the mitigation of their effects, will be increasingly seen by societies as a security issue and thus as a political priority. This is illustrated by the fact that while in 2011 only 3–5% of the EU population had considered climate change to be the most important European problem,[26] by 2021 this figure rose to 25–26%.[27] Indeed, a survey published in June 2021 showed that European citizens considered climate change to be the most serious problem facing the world. More than nine out of ten people surveyed considered climate change to be a serious problem (93%), while almost eight out of ten (78%) considered it to be very serious.[28] When asked to choose the single most serious problem facing the world, more than a quarter (29%) chose a problem related to climate change and environmental degradation: climate change (18%), the degradation of nature (7%) or health problems caused by pollution (4%).[29] A particular issue is that climate change and environmental degradation are also key issues when it comes to examining the so-called interlinking effects and addressing the threats and tensions that arise from such effects. It is a long-standing phenomenon that climate change and environmental degradation not only have the potential to cause cataclysmic events, but that they can, when combined with other – demographic, ethno-political, economic – trends, also amplify and feed tensions already existing in other dimensions of security. They could, for example, have a decisive impact on our health and food security, exacerbate and escalate the struggle for resources into armed conflict, or trigger mass migration.[30] And they can do so with far-reaching effects, regardless of how and to what extent a particular region is affected by the direct consequences of climate change and environmental degradation. It is important to emphasise that developing countries are in an increasingly vulnerable position in the midst of growing competition for resources and raw materials, because major powers are able to exploit them

[26] European Commission 2011: 35.
[27] European Commission 2022c: 23.
[28] European Commission 2021b: 7.
[29] European Commission 2021b: 9.
[30] Liu 2016; Marsai 2021.

by confronting local elites and certain (ethnic) groups with the broader society, while the environmental burden is borne by local communities.[31] We must also see that the costs of technological development and energy transition can be borne much more easily by developed, modern (industrialised) societies than by underdeveloped, poor ones. In other words, fragile states, especially in Africa, are in a particularly difficult position in this respect. For all these reasons, climate change and environmental degradation may be a particularly attractive area for those seeking to use hybrid threats. For them, the effects of climate change and environmental degradation provide a broad spectrum of vulnerabilities that promise complex and far-reaching consequences, if exploited. The tools and methods of hybrid threats can also be very broad. From the denial of climate change and amplification of climate sceptic voices, to attempts to weaken trust in the state and state institutions, and thus undermining social resilience, or in extreme weather events and in emergencies caused by environmental degradation, to the deliberate deepening of threats and tensions caused by interconnection effects. To make matters easier for those who pose hybrid threats, both climate change and hybrid threats are controversial phenomena, and are very often viewed with scepticism by local populist politicians and political movements. On the other hand, the other major obstacle to tackling the hybrid threat is that social resilience to climate change and environmental degradation should be developed and strengthened while avoiding oversecuritisation, which could lead to mass climate distress, climate depression and climate panic,[32] which could also help those who want to pose a given hybrid threat.

Connectedness

The rapid growth in global trade and globalisation in general has changed many aspects of the global economy, international business, and also rearranged the global distribution of economic output. Globalisation in its heydays was supported by a relatively stable geopolitical order. In the last 10 or so years, this order seems to show ruptures, the sophisticated, therefore vulnerable global economic web, supported by complex global value chains cannot take long-term geopolitical stability as a given factor. Another game changer is the rapid

[31] Piketty 2015.

[32] Warner–Boas 2017: 203–224.

emergence of Artificial Intelligence (AI); as a clear game changer, AI systems are disrupting markets, legal rules and principles that could be used so far.[33] AI will have major impacts on the global and local labour markets as well. The Council of Europe defines AI as a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. The development of common sense, reasoning and problem-solving skills in machines is a very difficult task, which is why AI combines research in a wide variety of fields. John R. Searle (1980) introduced the definitions weak AI (Artificial Narrow Intelligence, Weak AI) and strong AI (Strong Artificial Intelligence). In the case of weak AI, intelligence is only a "semblance", but we do not know whether it has a mind or not. A strong AI is a system that really thinks, has an independent consciousness. By 2050, we should expect human-like AI robots to 'live' with people in many areas. It will be in the interest of mankind to live in harmony and work with it. In the legal regulation of artificial intelligence technologies, in addition to a wide range of rules on legal responsibility, a number of open issues remain: the benefits and risks of its use, what ethical issues arise in the case of a malfunctioning AI, who is responsible, whether the protection of privacy can be ensured, whether the full spectrum of risks and damages can be covered by legal mechanisms, whether AI can be considered a legal entity from a moral and practical point of view, etc. The recognition and wording of application problems puts lawyers under "coercion of legal development".[34] More than twenty-five states announced their AI strategy or published plans for future strategies, including the United States, Russia, China and India. Many plans focus on maintaining a competitive advantage in the emerging AI market, although many also take into account the ethical and security aspects of promoting AI.[35] The rapid development of information technologies, based on globally connected infrastructures, hardware networks elevated to a whole new level by AI may radically change several aspects of the economy, the society, the world of labour, some aspects of human behaviour and even political dynamics. The heightened global interconnectedness and as a consequence extremely long and complex value chains may render international trade vulnerable and even minor disruptions by adversarial actions may induce serious repercussions.

[33] Bostrom 2014.
[34] Keserű 2020: 199–220.
[35] Nash 2019.

More vulnerable individuals – identities and identity politics

It may seem that megatrends are such large-scale processes that individuals, the smallest actors in political systems, do not perceive much of them. But this is not the case. What political party or social movement we feel close to, how we vote at elections, what we think about a war or a crisis, which policy reforms we prefer, what print or online media we consume, what products we buy, are all determined by our identity.[36] Fukuyama in his 2018 book argued that "the inner self of dignity seeks recognition".[37] Individuals demand public recognition of their world. Identity politics has become of crucial importance in our time. "Identity politics encompasses a large part of the political struggles of contemporary world, from democratic revolutions to new social movements, from nationalism and Islamism to the politics of contemporary American university campuses."[38] All forms of social actions are built around collective identities. The distribution of public goods and the mobilisation of different social groups require a distinction between the categories of 'us' and 'them'. There has been an increasingly strong articulation of identities in the manifestos of political parties, in the speeches of political leaders and in the decisions of voters. Further, the persuasiveness of policy arguments based on rational calculations, of measures based on economic considerations and rigorous calculations, is being overshadowed by emotional and less rational influences. The individual votes for a party and supports a movement that he or she perceives as similar to his or her own group. The collective identity of the individual thus determines his/her actions. Some authors also suggest that there is a close link between the rise of different patterns of populism and identity politics, due to the fact that identity messages are also embedded in the anti-elitist attitudes of social groups.[39] The strengthening of identity politics is, however, not only evident in the actions of populist leaders and parties – though certainly in theirs – but can be seen as a general phenomenon in the increasingly polarised societies of the 21st century, where individuals are looking for firm references for their identifications.[40] One of the most powerful tools of identity politics is storytelling,

[36] Koller 2022: 365–376.
[37] Fukuyama 2018: 10.
[38] Fukuyama 2018: 10.
[39] Velasco 2021: 1–8.
[40] Koller 2022: 365–376.

collective action wrapped in narratives. Frederick W. Mayer argues that it is precisely the shaping of individuals' identities that makes narratives effective.[41] Based on a constructivist perspective, for political parties, leaders, media actors, narratives are in fact also facilitators of the creation of symbols and myths.[42] A well-conceived, constructed narrative precisely frames the group boundaries of 'us' and 'them', guides individuals in judging 'right' and 'wrong', by answering the basic questions of existence, and thus creating continuity. However, narrative is itself a product, which the opinion leader, who plays a key role in identity construction, can also misuse. It is a product that has power and/or economic value. The narrative is used by the politician to maximise votes and forge political capital, by the journalist and the editor to enhance reputation and viewership, by the economic actor to promote consumer choices. However, narrative can also be a dangerous tool, since it is by framing, constructing and demarcating group boundaries that it is ideally suited to fear and hate mongering, to fostering a sense of insecurity, to labelling enemies or allies, and to packaging disinformation that can lead to persistent antagonism and group conflict between social groups within and outside the states. In a world shaped by megatrends it is necessary to look beyond one's own communities in order to enable collective action, it is particularly important to understand how and what forges or breaks up communities. To do this, we need to understand the process of identity formation and the tools of identity politics used and misused in our time.

Conclusion

Megatrends are evidently shaping our future, thus understanding their nature is essential to draft suitable policy plans. Demographic trends and ageing populations lead to both economically and environmentally unsustainable situations that significantly affect societies and require new policy answers from the states. Migration from insecure and poor regions to more wealthy territories, such as the European Union or the USA will be a long-term reality. There is a major realignment taking place in the global economic power equilibrium too, and geopolitical and security considerations are getting ever more important in the global economic policy decisions and practice. The world is in a democratic

[41] Mayer 2014.
[42] Anderson 1991.

recession and democratic decline is apparent in Asia-Pacific, Eastern Europe and Central Asia, Latin America and the Caribbean. Fewer people leave in full democracies than before. At the same time, the international system moves towards a post-hegemonic world order, where the hegemonic power of the former hegemon – the United States – is challenged in politics, economics, diplomacy and military. The negative trends in climate change and environmental degradation will continue in the coming years, despite efforts by states and other international actors to control them. The emergence of Artificial Intelligence (AI) disrupts markets, legal rules and affects politics and the ways of life of the people in the widest sense. Individuals become more vulnerable and are exposed to manipulations and misuse of identity politics.

Questions

1. How will the world population change in this century?
2. What challenges do ageing societies pose for countries?
3. Who are the most powerful players of world economics? Where are the division lines?
4. What does the trend of democratic backsliding mean?
5. Why are climate change and environmental degradation attractive areas for those seeking to use hybrid threats?
6. What are the characteristics of a post-hegemonic world order?
7. What are the consequences of the massive technological change and the emergence of AI?
8. What can be the threats of misusing the tools of identity politics?

References

Allahar, Haven (2014): Major Global Megatrends: Implications for Advanced and Emerging Countries. *Journal of Management,* 2(8), 1–18.

Anderson, Benedict (1991): *Imagined Communities. Reflections on the Origin and Spread of Nationalism.* Revised Edition, London – New York: Verso.

Bargués, Pol – Bourekba, Moussa – Colomina, Carme eds. (2022): *Hybrid Threats, Vulnerable Order.* CIDOB Report. Online: www.cidob.org/en/publications/publication_series/cidob_report/cidob_report/hybrid_threats_vulnerable_order

Bostrom, Nick (2014): *Superintelligence. Paths, Dangers, Strategies.* Oxford: Oxford University Press.

Callahan, William A. (2008): Chinese Visions of World Order: Post-hegemonic or a New Hegemony? *International Studies Review,* 10(4), 749–761. Online: https://doi.org/10.1111/j.1468-2486.2008.00830.x

Carothers, Thomas – Press, Benjamin (2022): *Understanding and Responding to Global Democratic Backsliding.* Carnegie Endowment. Online: https://carnegieendowment.org/files/Carothers_Press_Democratic_ Backsliding_v3_1.pdf

Carothers, Thomas – O'Donohue, Andrew (2019): *Democracies Divided : The Global Challenge of Political Polarization.* Washington, D.C.: Brookings Institution Press.

Cooley, Alexander – Nexon, Daniel H. – Ward, Steven (2019): Revising Order or Challenging the Balance of Military Power? An Alternative Typology of Revisionist and Status-Quo States. *Review of International Studies,* 45(4), 689–708. Online: https://doi.org/10.1017/S0260210519000019

Cooley, Alexander – Nexon, Daniel H. (2020): *Exit from Hegemony. The Unraveling of the American Global Order.* Oxford: Oxford University Press.

Diamond, Larry (2015): Facing Up to the Democratic Recession. *Journal of Democracy,* 26(1), 141–155.

EIU (2006): *EIU Democracy Index 2006.* Online: www.economist.com/media/pdf/democracy_index_2007_v3.pdf

EIU (2022): *EIU Democracy Index 2022. Frontline Democracy and the Battle for Ukraine.* Online: www.eiu.com/n/campaigns/democracy-index-2022/

European Commission (2011): *Standard Eurobarometer 76. December 2011.* Online: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=46434

European Commission (2020): *Strategic Foresight Report 2020.* Online: https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2020-strategic-foresight-report_en

European Commission (2021a): *Strategic Foresight Report 2021.* Online: https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2021-strategic-foresight-report_en

European Commission (2021b): *Special Eurobarometer 513. Climate Change.* Online: https://climate.ec.europa.eu/system/files/2021-07/report_2021_en.pdf

European Commission (2022a): *Strategic Foresight Report 2022.* Online: https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2022-strategic-foresight-report_en

European Commission (2022b): *Megatrends Hub 2022.* Online: https://knowledge4policy.ec.europa.eu/foresight/tool/megatrends-hub_en

European Commission (2022c): *Standard Eurobarometer 96. Winter 2021–2022.* Online: www.ffms.pt/sites/default/files/2022-08/Standard_Eurobarometer_96_Winter_2021-2022_Infographic.pdf

Fukuyama, Francis (2018): *Identity. Contemporary Identity Politics and the Struggle for Recognition.* London: Profile Books.

Halliday, Fred (2009): International Relations in a Post-Hegemonic Age. *International Affairs,* 85(1), 37–51. Online: https://doi.org/10.1111/j.1468-2346.2009.00779.x

Houle, David (2011): *The Shift Age.* Naperville: Sourcebooks.

Ikenberry, John G. (2018): Why the Liberal World Order Will Survive. *Ethics and International Affairs,* 32(1), 15–29. Online: https://doi.org/10.1017/S0892679418000072

Inflation Reduction Act of 2022 to provide for reconciliation pursuant to title II of S. Con. Res. 14. Eff. 16 August 2022.

Jacobs, Thomas – Gheyle, Niels – De Ville, Ferdi – Orbie, Jan (2022): The Hegemonic Politics of 'Strategic Autonomy' and 'Resilience': Covid-19 and the Dislocation of EU Trade Policy. *Journal of Common Market Studies,* 61(1), 3–19. Online: https://doi.org/10.1111/jcms.13348

Juutinen, Marko – Käkönen, Jyrki (2016): *Battle for Globalisations? BRICS and US Mega-Regional Trade Agreements in a Changing World Order.* New Delhi: Observer Research Foundation.

Kailong, Yu (2022): *To What Extent Can We Speak of a Post-US Hegemonic Order? Will the Global Liberal Order Outlast US Hegemony?* Online: http://dx.doi.org/10.2139/ssrn.4069548

Keserű, Barna Arnold (2020): A mesterséges intelligencia magánjogi mibenlétéről. In Lévayné, Fazekas Judit – Kecskés, Gábor (eds.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr: Universitas-Győr Nonprofit Kft. 199–220.

Koller, Boglárka (2022): „Vágyódás az elismerésre" – Az identitás mint a 21. század társadalomtudományi elemzéseinek kulcsfogalma. In Koltay, András – Gellér, Balázs (eds.): *Jó kormányzás és büntetőjog. Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára.* Budapest: Ludovika University Press. 365–376.

Liu, Qinqin (2016): Interlinking Climate Change with Water-Energy-Food Nexus and Related Ecosystem Processes in California Case Studies. *Ecological Process,* 5(14). Online: https://doi.org/10.1186/s13717-016-0058-0

Marján, Attila (2010): *Europe's Destiny. The Old Lady and the Bull.* Translated by Péter Szücs. Baltimore: Johns Hopkins University Press.

Marsai, Viktor (2021): *Az afrikai klímaváltozás okozta kihívások és azok hatása Európára.* Green Policy Center. Online: www.greenpolicycenter.com/wp-content/uploads/2021/02/green-policy-center_tanulm%C3%A1ny5_END-1.pdf

Mayer, Frederick W. (2014). *Narrative Politics. Stories and Collective Action.* Oxford: Oxford University Press.

Naisbitt, John (1982): *Megatrends. Ten New Directions Transforming Our Lives.* New York: Warner Books.

Nash, Margaret ed. (2019): *Understanding Machine Learning.* New York: Clanrye International.

OECD (2016): *OECD Science, Technology and Innovation Outlook 2016.* Online: https://doi.org/10.1787/sti_in_outlook-2016-en

Piketty, Thomas (2015): *A tőke a 21. században.* Budapest: Kossuth Kiadó.

Quillin, Bryce (2019): *Changing Global Demographics: The Certain Future.* Online: www.bbvaopenmind.com/en/economy/global-economy/changing-global-demographics-the-certain-future/

Sinkkonen, Ville (2022): A Fleeting Glimpse of Hegemony? The War in Ukraine and the Future of the International Leadership of the United States. *TPQ,* 21(1), 121–131.

Slaughter, Richard A. (1993): Looking for the Real 'Megatrends'. *Futures,* 25(8), 827–849. Online: https://doi.org/10.1016/0016-3287(93)90033-P

Slaughter, Richard A. (2002): Beyond the Mundane: Reconciling Breadth and Depth in Futures Enquiry. *Futures,* 34(6), 493–507. Online: https://doi.org/10.1016/S0016-3287(01)00076-3

Slaughter, Richard A. (2013): Time to Get Real: A Critique of Global Trends 2030–Alternative Worlds. *World Futures Review,* 5(4), 354–359. Online: https://doi.org/10.1177/1946756713510280

United Nations (2022): *World Population. Prospects 2022: Summary of Results.* UN DESA/POP/2022/TR/NO. 3. Department of Economic and Social Affairs, Population Division.

V-Dem Institute (2022): *Democracy Report 2022. Autocratization Changing Nature?* Online: https://v-dem.net/media/publications/dr_2022.pdf

Velasco, Andrés (2020): Populism and Identity Politics. *LSE Public Policy Review,* 1(1), 1–8.

Vezirgiannidou, Sevasti-Eleni (2013): The United States and Rising Powers in a Post-hegemonic Global Order. *International Affairs,* 89(3), 637–651. Online: https://doi.org/10.2307/23473847

Warner, Jeroen – Boas, Ingrid (2017): Securitisation of Climate Change: The Risk of Exaggeration. *Ambiente & Sociedade,* 20(3), 203–224. Online: https://doi.org/10.1590/1809-4422asocex0003v2022017

This page intentionally left blank.

Nicola Cristadoro[1]

Ideologies and Motivations

Nowadays, does it still make sense to speak of armies in the traditional sense, intended as military forces of large numerical entity for land use in large-scale war operations? Considering the 'special military operation' carried out by Russia with the full-scale invasion of Ukraine on 24 February 2022, the answer would appear to be affirmative. However, if we consider most conflicts that have erupted or protracted over the past decade, this conception appears at least anachronistic. Observing the use of the land forces of the nations fighting in the various contemporary operational theatres, we do not see divisions, brigades or regiments that manoeuvre facing each other for the conquest and occupation of a territory or for its defence. If the Kurdish Peshmerga still wear uniforms and fight in regular units that, despite internal divisions, make them comparable to an army, the same cannot be said of their direct enemies, the Islamic State of Iraq and Syria (ISIS) fighters. These, in fact, despite being largely veterans of the Iraqi army after its disbandment, incorporate foreign fighters from different areas of the world and fight with a mixture of weapon systems and multiform technical-tactical procedures, according to the canons of 'asymmetric warfare'.

Examples worldwide

The concept of 'asymmetric warfare' itself, at present, appears outdated. If the Warsaw Pact and NATO doctrines for conventional warfare belong to prehistory, 'asymmetric warfare' can now be considered history. Asymmetrical were the conflicts of decolonisation in Africa, the Viet Cong campaigns in Indochina, the actions of Palestinian terrorist organisations against the Israeli security forces, the attacks of the Taliban and Al Qaeda-affiliated against the coalition deployed in Afghanistan. To refer to contemporary conflicts, it seems more appropriate to speak of 'ambiguous', 'non-linear' and 'hybrid' warfare, i.e. wars fought at different levels and prevailing over the ways in which the opposing forces clash on the ground. The term 'hybrid warfare' currently refers with

[1] University of Turin.

immediacy to Russia. This term was coined in 2002 by William J. Nemeth (for more details see the chapter authored by Eado Hecht in this book) to describe the Chechen insurgency, which saw the fusion, hence the adjective 'hybrid', of guerrilla techniques with modern military tactics, resorting extensively to the support of civilian technology from mobile phones to the Internet. The social paradigm presented by Nemeth, which sees the degeneration of an evolved society into a 'hybrid society' as a premise for the development of 'hybrid' conflicts, is interesting. "There is increasingly a body of work that is challenging the accepted norm of peaceful pre-state societies that turned violent only as higher and more centralized forms of societal organization became prevalent […]. Devolving societies are societies that are returning to more traditional forms of organization, but are doing so unevenly. That is, these societies are bringing with them an eclectic mix of modern technology as well as political and religious theory and institutions as they devolve […]. These societies, many of which retain the trappings of the state system, are either a multitude of warring clans contained within the previous state boundaries, or a mostly homogenous socio-political unit that is fighting against a perceived oppressor. In either case these hybrid societies are a mixture of the modern and the traditional. Hybrid societies in turn have organized hybrid military forces, and it is these forces that will challenge military and diplomatic planners in the future. Currently a large body of work exists regarding hybrid military forces under the rubric of Fourth Generation Warfare, New Warfare, or more conventional terms such as Low Intensity Conflict and Terrorism. Fourth Generation Warfare coined by Bill Lind and others in the late 1980's saw warfare in non-states as developing along a divergent path when compared to that being developed by Western nations. The developed world is increasingly moving toward "Advanced Technology" warfare, which will embed the increasing reliance on high technology seen Western society in Western military forces. Countering this in non-western states, and especially hybrid societies, is an increasing shift toward an idea driven concept of war. This idea driven concept of war […] envisions a mix of terrorism and Low Intensity Conflict that is non-national or transnational in nature and bypasses the western military to directly attack western cultural."[2] The illegal annexation of Crimea to Russian territory and the contribution to instability in the eastern provinces of Ukraine, notably the Donbas, by the Russian Federation and its armed forces have provided a significant example of 'hybrid warfare',

[2] Nemeth 2002: 2–3.

both at the tactical and strategic-operational levels, even ahead of the full-scale invasion in February 2022. Russian actions in Ukraine and Crimea appear clearly in line with this conception, although many scholars of military history and doctrine have pointed out that such an operational choice is nothing new for Russia. An example, albeit a prototypical one, of the adoption of this tactical conception is represented by *Operation Storm 333* conducted in Afghanistan on 27 December 1979 for the capture of President Hafizullah Amin's residence and his elimination by KGB special forces, in conjunction with Army and GRU units. In order to deceive the enemy and take them by surprise, the Soviet soldiers engaged in this operation did not wear the uniforms and insignia of their own units, but Afghan uniforms, except for a white armband tied to one arm, to recognise each other. What we can otherwise call 'ambiguous warfare' involves elements with a very high training and disciplinary profile who, without wearing a uniform and bearing distinctive symbols, are placed in combat zones in a very short time and, in collaboration with local supporters, on the sidelines of traditional operations resort to psychological operations, intimidation and bribery to undermine the adversary's resistance. By 'ambiguous warfare' one can also indicate a certain *modus operandi* in conducting warfare, which was in use in U.S. governmental circles between the 1960s and 1980s and is still widely practised today in both the Iraqi and Syrian scenarios. The *Phoenix Program* implemented between 1967 and 1975 in Vietnam under CIA supervision is indicative of such procedures. Through infiltration, capture, terrorism, torture and assassination, the aim was to identify and 'neutralise' the structure of the National Liberation Front of South Vietnam, the paramilitary organisation better known as the Viet Cong. Even more significant is the support given to the paramilitary units of the Contras in Nicaragua in the late 1970s, which today serve as a model for similar organisations such as the Death Squads active in Iraq or the Free Syrian Army (FSA) operating in Syria. In general, the definition prefigures situations in which a belligerent state or non-state entity deploys military and paramilitary units in a confusing and deceptive manner to achieve military and political objectives, disguising the direct participation of its armed forces in operations. Complicating the model is the attempt to describe modes of operation that fall below the threshold of conventional military conflict. There are in fact, especially in Russian military philosophy, two sub-categories that need to be explored in depth. The 'grey zone warfare' on the one hand and 'hybrid warfare' on the other. In particular, the latter "is more limited to the battlefield, whereas Grey Zone Warfare also considers the political sphere and the

international framework, with all the possibilities for action that these allow […]. It involves even less military action than hybrid warfare […]. Its three main characteristics are ambiguity, a low degree of distinctiveness and the possibility of denying everything".[3] Hence, the topicality of the thought of General Valeriy Gerasimov, the Russian Chief of Defence Staff, who goes beyond the 'asymmetrical' model by elaborating a doctrine that envisages attacking the adversary economically, cognitively and physically by making extensive use of unconventional procedures. In particular, in the perspective of deploying forces capable of operating on a post-modern battlefield, it is preferable to replace traditional manoeuvre and logistic support units with small units that are flexible in terms of deployment, extremely mobile, fast in action and, perhaps, without insignia and badges that can be traced back to their affiliation and nationality. We speak, of course, of Special Forces. The reference to the figures of the American and Soviet 'military advisers' active in Latin America, Asia and Africa between the 1960s and 1980s is immediate. If this aspect already constitutes a peculiar element of the 'ambiguous warfare', such a definition becomes more comprehensible if one considers the other actors that make up the military structure in today's theatres of war, such as Libya, Syria, Iraq, Afghanistan and, extremely representative, Ukraine, with the events in Crimea and the Donbas region. In fact, alongside Special Forces from countries other than the areas of operation and interested in controlling the policies and resources of these areas, there are local paramilitary groups, mercenaries, groups of civilians loyal to one or the other party on an ethnic basis and, last but not least, criminal organisations interested in profiting from the trafficking linked to the conflict. In this already sufficiently confused picture, one must not overlook the increasingly cogent role of hackers, the 'lords of cyberwar' who, with their skills and increasingly sophisticated tools at their disposal, represent the vanguard of the 'infowar'. To them belongs the domination of 'white', 'grey' or 'black' propaganda, and theirs is the ability to strike devastatingly at the nerve centres of a state's economy, society and politics, by compromising or neutralising computer networks. It will be increasingly difficult to determine 'who is who', and this premise portends a further evolution of future war into a form of uncontrollable conflict that we would call the "total chaos warfare". It is difficult for a culture such as that of the West, which, at least in theory, is based on principles of transparency and democracy, or which, *a priori,* repudiates war of aggression in its constitutional dictates, to conceive

[3] Ottaviani 2022: 33.

of such an approach to warfare. Above all, it is difficult to win against adversaries who base their tactics on such doctrinal principles. To understand, therefore, who engages in this type of operation and for what purpose, we are helped by the concept of 'sharp power', which we can metaphorically refer to as a sharp knife that pierces, penetrates or perforates the media and political environment in the targeted countries. "Today's authoritarian states – notably including China and Russia – are using "sharp power" to project their influence internationally, with the objectives of limiting free expression, spreading confusion, and distorting the political environment within democracies. Sharp power is an approach to international affairs that typically involves efforts at censorship or the use of manipulation to sap the integrity of independent institutions. This approach takes advantage of the asymmetry between free and unfree systems, allowing authoritarian regimes both to limit free expression and to distort political environments in democracies while simultaneously shielding their own domestic public spaces from democratic appeals coming from abroad."[4] However, as we shall see, Russia and China are not the only states that are extremely proactive in the conduct of undeclared or even denied wars. We opened with one question and two others emerge as a premise for the development of this discussion. What are the motivations that lead a state to choose to engage in a hybrid conflict and what forms of government best favour the planning, organisation and conduct of an undeclared war? In the following we will examine several state and non-state realities that seem to us to represent suitable models for answering the questions formulated.

Russian establishment

Following the collapse of the Soviet Union in 1991, Russia struggled to find and reclaim its place in the world order. Reactionary elements within the government, intelligence services and armed forces found common cause with the new economic elites and elements of the Russian Orthodox Church in their desire to reclaim the loss of empire. Thus, even before the *de jure* dissolution of the Union of Soviet Socialist Republics (USSR), Moscow began to reassert its control over the members of the Commonwealth of Independent States (CIS). Russian methods of intervention evolved from conflict to conflict as leaders sought the most

[4] Walker 2018: 9–23.

efficient ways to bring weaker powers to their knees while avoiding the stigma of imperialism, invasion and war with the West.[5] The events that led to Lithuania's independence in 1991 were the first lesson learned about exercising power abroad in the post-Cold War era. Large-scale conventional operations against sovereign states would expose the Kremlin to unwanted scrutiny by the International Community (IC), international pressure and protests within Russia itself. To maintain control over the 'near-abroad' states, Moscow would have had to exercise power in a more clandestine and concealable manner. The most effective tactics implemented by Russia to act in the so-called 'grey zone' are (dis)information operations and cyber operations, followed by political coercion and space operations. The Russian info-ops of the Internet Research Agency – whose owner Yevgeny Prigozhin is also the financier of the Private Military Company 'Wagner' – continue to be generously funded, relentless and prolific. The coercive activity directed at the socio-political structures in Europe has become increasingly aggressive over time, following Putin's attempts to block NATO's eastward expansion. In this context, Moscow's deeper ties with Serbia, with the Bosnian Serb component and the failed covert operation to block the Prespa Agreement,[6] must be read with growing concern. Even in space, Russia has demonstrated its capacity and unscrupulousness in targeting states from which it feels threatened, with actions to jam GPS signals during NATO military exercises, with attacks against U.S. commercial and allied military satellites, and even by damaging the sensors of a Japanese satellite with lasers.[7] The prerogative offered by hybrid warfare, especially acting in what we have called the 'grey zone', is precisely that of dereliction of responsibility for its own actions, and during the campaigns in Ukraine, wherever possible, Moscow strenuously denied its involvement, exploiting elements of proximity and resorting to deception to evade the IC's condemnations associated with a conventional armed invasion.[8] The Federal Security Service (FSB) and the Ministry of Internal Affairs (MVD), in fact, assumed the role of directing forces acting by proxy, an organisational technique that began at the end of the last century and would

5 Herd–Akerman 2002: 357–372.

6 The "Prespa Agreement" is an agreement reached in 2018 between Greece and the Republic of Macedonia, under the auspices of the United Nations, resolving a long-standing dispute between the two. Apart from resolving the terminological differences, the agreement also covers areas of cooperation between the two countries to establish a strategic partnership between them.

7 Harrison et al. 2019.

8 The United States Army Special Operations Command 2015.

continue in subsequent Kremlin-led war operations. Let us recall that from 1999 to 2009, Moscow directed a campaign that effectively suppressed the Islamic insurgency in Chechnya and reasserted Russian control of the region. As long as wars could technically be considered internal affairs, Russia was able to avoid accusations of aggression. However, global outrage in the wake of civilian deaths and the growing refugee problem led Putin's military and intelligence components to transfer control of counterinsurgency operations to reliable proxies such as local militias and paramilitary forces to be deployed in place of regular Russian troops. In developing their operations, therefore, the Russians alternately denied involvement or downplayed the size and activities of their forces. In particular, they introduced the use of information warfare on an unprecedented scale. In the 2008 Russian–Georgian conflict, for instance, Russian agents extensively used cyberwar and intense propaganda to neutralise the Georgians' combat options and smear them in the press as aggressors, even accusing them of genocide. The Russian military brought journalists to the area of operations to reinforce Russia's message of protecting the population from Georgian aggression. Moscow carefully managed television broadcasts both at home and in the region, highlighting the atrocities the Georgians allegedly inflicted on the people of South Ossetia. These procedures have been named 'spetzpropaganda' and are taught at the Department of Military Information and Foreign Languages of the Ministry of Defence Military University. As an academic discipline, it is aimed at military personnel, intelligence officers, journalists and diplomats. The doctrine specifies that an information campaign is multidisciplinary and includes politics, economics, social dynamics, military, intelligence, diplomacy, psychological operations, communications, education and cyber warfare. In general, Russian information warfare aims to influence the consciousness of the masses, both at home and abroad, to condition it with a view to a clash of civilisations between Russian and Western Eurasian culture. Through the coordinated manipulation of the entire information domain including newspapers, television, internet websites, blogs and other media, Russian operatives attempt to create a virtual reality in the conflict zone that influences perceptions or replaces the truth with versions that fit the Russian narrative.[9] In Crimea and the subsequent operations in the Donbas, Russian 'spetzpropaganda' developed the theme that pro-Russian intervention was necessary to save the Ukrainian people from submission to the Kiev regime imposed "by the Banderovtsy and the Maidan

[9] Darczewska 2014.

fascists".[10] This is the background to the strategic thinking of General Valery Gerasimov,[11] Chief of the Defence Staff of the Russian Federation. General Gerasimov's main thesis is that modern conflict differs significantly from the paradigm of World War Two and even from the Cold War conflict. Instead of declared wars, strict definition of military and non-military efforts, and large conventional forces to be deployed in battle, the modern conflict features undeclared wars, hybrid operations combining military and non-military activities, and the employment of smaller forces with specific training: *spetsnaz,* paramilitaries, mercenaries. Gerasimov explained that the 'coloured revolutions' and the 'Arab Spring' have shown that the line between war and peace is blurred. Although liberal democratic uprisings may not look like war, they often result in foreign intervention (both overt and clandestine), chaos, humanitarian disasters and civil war. These activities can become the typical war of the modern era and Russian military practices must evolve to adapt to the new methods. Modern warfare, said Gerasimov, focuses on intelligence and the domination of the information space. Information technologies have reduced the spatial, temporal and information gap between army and government. Targets are achieved in remote contactless warfare; the strategic, operational and tactical levels, as well as offensive and defensive actions, have become less distinguishable. Asymmetric actions against enemy forces are more common. The military dimension, therefore, must include information warfare. Armed, but not in uniform, Russian forces in Crimea have provided Moscow with the possibility of deniability, albeit implausible. The pro-Western press called the intruders 'little green men', while Russian cultural supremacist theorist Aleksandr Dugin called them 'nice men', referring to their kindness and diplomatic retreat once an area was secured. The goal is the very essence of Sun Tzu's expressed ideal of "winning without fighting". In Crimea, it worked. In eastern Ukraine, it did not and led to an escalation of the conflict. To catalyse domestic consensus, the Putin Administration went so far as to popularise the idea of a NATO plan to invade Russia and even foreshadowed that the West, led by the U.S., intended to annex Crimea. Sevastopol would then become a NATO naval base. Linked to these themes, it then played on the idea that the Russian people, with its history of religious, cultural and military greatness, had been artificially divided after the collapse of the Soviet Union. Once again, the West was presented as

[10] The United States Army Special Operations Command 2015.

[11] Cristadoro 2022.

the architect of the conspiracy to prevent Russia from enjoying unity, peace, security and its rightful place in the world order. From the Russian point of view, since the West is persecuting Russia, everything becomes permissible in the pursuit of a true justice that reaffirms Moscow's deprived role. Let us come to the events of 24 February 2022. The invasion implemented with the massive recourse to conventional forces lends itself to a twofold interpretation: on the one hand, it may represent the failure of the Russian infowar in Eastern Ukraine, hinting at an extreme attempt by Putin to make up for the failures of the policy of deploying 'asymmetrical' forces in the Donbas; on the other hand, in perfect adherence to the 'Gerasimov Doctrine', it represents the logical continuation of the Russian info campaign, which is partly designed to establish the conditions for invasion, should it be necessary.

Dragon on the attack

China aggressively and effectively employs many hybrid 'grey zone' tactics. The main ones are provocation using forces under state control, economic coercion, cyber operations and space operations. The motivations behind Beijing's warfare through 'grey zone' tools, and the tools themselves, are summarised in NATO's Strategic Concept 2022. "The People's Republic of China's (PRC) stated ambitions and coercive policies challenge our interests, security and values. The PRC employs a broad range of political, economic and military tools to increase its global footprint and project power, while remaining opaque about its strategy, intentions and military build-up. The PRC's malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm Alliance security. The PRC seeks to control key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains. It uses its economic leverage to create strategic dependencies and enhance its influence. It strives to subvert the rules-based international order, including in the space, cyber and maritime domains. The deepening strategic partnership between the People's Republic of China and the Russian Federation and their mutually reinforcing attempts to undercut the rules-based international order run counter to our values and interests."[12] A peculiar element of Beijing's operations in the 'grey zone' is the construction of artificial islands. Indeed, since 2013, China has

[12] *NATO 2022 Strategic Concept:* 5.

engaged in dredging and building islets in the Spratly Islands archipelago and constructing outposts throughout the Paracel Islands. To enforce these activities, the Chinese rely on both the coast guard and the People's Armed Forces Maritime Militia (PAFMM).[13] Interestingly, members of this militia operate in the South China Sea without identification marks and are therefore referred to as 'little blue men'. The reference to their counterparts who participated in the 2014 invasion of Crimea is obvious. At least as far as the Spratly Islands are concerned, China has turned some islands into military bases, "complete with radar domes, shelters for surface-to-air missiles and a runway long enough for fighter jets."[14] According to Admiral Philip S. Davidson, this militarisation of the area indicates that "China is now capable of controlling the South China Sea in all scenarios short of war with the United States".[15] Let us now look at economic coercion; this includes the Belt and Road Initiative (BRI) economic and foreign policy project. Although the BRI improves Chinese trade links and reduces China's domestic industrial production surplus, Beijing uses its economic leverage to influence the interests of other states[16] and for the purpose to "deter confrontation or criticism of China's approach to or stance on sensitive issues".[17] It must also be considered that the BRI's 'debt-trap diplomacy' creates opportunities for China to introduce military forces in states where local development interventions are carried out, as in the case of Djibouti, where the naval base established by Beijing is of strategic importance both militarily and economically for controlling trade routes. Nevertheless, alongside the development of the BRI there has been the Digital Silk Road (DSR) initiative to bring technological advances and digital infrastructure to developing economies. Like the BRI, the DSR can create economic benefits for China, but there are well-founded concerns that the initiative has unstated security purposes.[18] For example, through the installation of fibre-optic cables, Chinese state-owned or state-affiliated enterprises can acquire large amounts of data that the Chinese Government could eventually use to exert pressure in areas outside of the economy.[19] In the race for 5G, it is feared that once a company like Huawei has installed its network, it will be used for espionage

13 Thomas 2020.
14 Beech 2018.
15 Beech 2018.
16 Cristadoro 2021.
17 Department of Defense 2018: 12.
18 Department of Defense 2018.
19 Harding 2019.

activities,[20] aimed at acquiring sensitive data useful for industrial purposes, but also for potential coercive influence. Economic coercion aimed at acquiring intellectual property or conducting industrial espionage is carried out through cyber espionage or by Chinese companies under the control of Guoanbu, the foreign intelligence agency. Such activity includes the acquisition of "companies and technology based on their government's interests – not on commercial objectives".[21] For example, from 2013 to 2016, Chinese companies sought to acquire several businesses in the semiconductor industry. China's potential dominance of that industry could play a crucial role in altering the future global military balance, as semiconductors are essential in the components of advanced military systems.[22] China, therefore, relies on cyber operations in the 'grey zone' that go beyond purely economic purposes. Cyberwar is a favoured route to conduct espionage and intelligence gathering, but also to target the critical infrastructure of other states and interfere in political processes abroad. Let us not forget that the cyber activities conducted by Russia are also paradigmatic in this respect. Lastly, considering Space as a new warfighting domain, China's conspicuously funded space programme is aimed at developing a range of activities in the 'grey zone'.[23] China continues to develop a range of space interdiction capabilities designed to limit or prevent an adversary's use of space assets during crises or conflicts. The People's Liberation Army has historically managed China's space programme and continues to invest in improving China's capabilities in space Intelligence, Surveillance, Reconnaissance, satellite communications, satellite navigation and meteorology, as well as human spaceflight and robot space exploration.[24] China utilises its orbital and terrestrial resources to achieve its civil, economic, political and military goals and objectives. People's Liberation Army (PLA) strategists consider the ability to use space systems and to deny their use to adversaries as strengths in the conception of modern, computerised warfare, and therefore, the Chinese Armed Forces are pursuing a programme to strengthen its military space capabilities, in contradiction to the government's statement against the militarisation of space. Space operations are likely to be an integral component of other PLA campaigns and will play a key role in enabling

[20] Cristadoro 2021.
[21] Cooper 2018.
[22] Cooper 2018.
[23] Harrison et al. 2019.
[24] Office of the Secretary of Defense 2017.

suitable actions to counter third-party intervention during military conflicts. In addition to the research and possible development of satellite jammers and directed energy weapons, China has likely made progress on kinetic energy weapons, including the anti-satellite missile system tested in July 2014.[25] Beijing is conducting increasingly sophisticated satellite operations and is likely experimenting with dual-use technologies for use in orbit that could be applied to space interdiction missions. The PLA's Strategic Support Forces, established in December 2015, play a leading role in managing Chinese aerospace warfare capabilities.[26] Commercial satellite imagery has shown Chinese military grade jamming equipment deployed on islands in the South China Sea, which can be used to interfere with communications, Positioning, Navigation and Timing (PNT) signals or any other satellites in the region.[27] China has also been involved in using its cyber capabilities to target space systems. Importantly, although China is the state with the greatest capacity to exploit the "grey zone", it has chosen not to intervene indiscriminately in all areas. This apparent restraint requires further reflection on whether China feels inhibited by U.S. actions or is simply self-regulating for other reasons. If the latter is true, these reasons can be identified and understood and could offer several elements to dissuade China from applying its tactics in the "grey zone" in the future.

Hezbollah and Tehran

Iran's support to proxy groups acting in Lebanon, Syria, Iraq and Yemen is one of its most effective tools to achieve its national interests by fighting in the 'grey zone'. The Islamic Revolutionary Guards Corps (IRGC), the notorious Pasdaran, is the paramilitary organisation executing Iranian proxy policies, with close ties to groups such as Hezbollah in Lebanon, the Houthis in Yemen, the National Defence Force Militia in Syria and the Badr Corps in Iraq, among others.[28] Drawing on its special forces unit known as the Quds Force, the IRGC is able to train and advise its auxiliary forces – estimated at 250,000 fighters – and thus poses a significant threat to Tehran's adversaries in much of the Middle East.

25 Office of the Secretary of Defense 2017.
26 Office of the Secretary of Defense 2017.
27 Gordon–Page 2018.
28 McInniss 2017: 25–33.

The Quds Force was established in the early 1990s to enable the ayatollahs' regime to operate covertly outside Iranian borders. The goal was to build an operational mechanism that would take the Islamic Revolution out of Iran.[29] As part of its ongoing struggle against Israel, Iran's strategy uses proxy organisations for two main reasons. Firstly, because of the considerable distance between Israel and Iran. The more than one thousand kilometres separating the two states constitute an objective operational difficulty for Iran for a direct attack on Israeli territory. Secondly, Iran is very concerned about the Israeli response, should it directly attack Israel. Therefore, the use of proxy organisations negates the difficulties related to the distance between Iran and Israel, effectively engaging the latter on two fronts of struggle, one in the north against Hezbollah in Lebanon and the other in the south against Hamas and Islamic Jihad in the Gaza Strip. This strategy also allows Iran not to be directly involved in the confrontation with Israel.[30] To achieve this goal, Tehran continues to support paramilitary formations under its control in Lebanon and the Gaza Strip and to supply them with various weapons systems, including rockets and missiles.[31] According to Israeli military intelligence, the precision missile programme was designed for two purposes. The first was to reduce the range of fire towards Israel. While, as mentioned, the distance between Iran and Israel is thousands of kilometres, southern Lebanon is only a few hundred kilometres from the nerve centre of the State of Israel in Tel Aviv and Gush Dan. Therefore, while Iran would need to launch long-range missiles to hit Israel, Hezbollah can achieve the same goal from Lebanon with short-range rockets. The second purpose is to move the battlefield away from Iran. Since firing at Israel from Syria and Lebanon may foresee a logical Israeli retaliation against these countries rather than Iran, Tehran is better off financing its proxy organisations and arms supplies, thus avoiding putting itself at risk in the front line of its policy of aggression against the Jewish state. The best-known paramilitary organisation is Hezbollah, which began its military operations following the expulsion of Palestine Liberation Organisation (PLO) forces from Lebanon in 1982 during the First Lebanon War. Inspired by the religious justification of leading Shi'a ideologues such as Ayatollah Khomeini, remember the suicide bombings against Israeli, American and French targets located in Lebanon. Hezbollah succeeded in advancing the status of the

[29] Katz–Hendel 2011.
[30] Eilam 2019.
[31] Bergman 2018.

Shi'a community in Lebanon from a persecuted and deprived community to the most powerful and dominant community in the country, while repressing the Christian community in Lebanon. The Iranians, who have sought to propagate the religious principles that guided the Islamic revolution and improve the quality of life of Lebanese Shi'as, have poured hundreds of millions of dollars into supporting Hezbollah. Thus, Iran has founded many social institutions for the Shi'a in Lebanon, such as hospitals, clinics, universities, cultural institutions, and radio and television stations.[32] In parallel, it has trained and armed Hezbollah members into a military militia serving the IRGC.[33] The organisation has about 20,000 men in readiness, of which 5,000 are elite fighters and between 20,000 and 50,000 are reserve fighters.[34] Hezbollah bases its defence on the civilian population of the area in which it operates. Although Iran's theocratic conception is as far removed from Chinese state atheism as possible, there is an affinity with Mao Zedong's principle of "mingling with the population like fish in the sea" and gaining their consent. In terms of technical-tactical procedures (TTPs), the organisation establishes its headquarters on the lower floors of ten-storey residential buildings and also in residential buildings where it hides weapons such as missiles and rockets.[35] Hezbollah thus exercises a form of deterrence against possible Israeli attacks, which would be subject to harsh criticism by the IC for the 'collateral effects' of such a decision. Hezbollah, however, has also been criticised for its tactical-strategic choice. In response to the criticism, the organisation stated that, considering the weakness of the Lebanese army, it is the only one that can guarantee a buffer between Israel and Lebanon to protect the latter from any Israeli aggression.[36] Although Hezbollah started out as a typical militia to be employed in asymmetric warfare tactics, over time it has evolved into an organisation capable of fighting different types of war. During the Lebanese civil war, when it was but one of many militia groups in the country, Hezbollah mainly launched suicide bombings and frontal attacks on Western and Israeli forces, both methods that, militarily, are neither sophisticated nor efficient. Hezbollah's quiet evolution from a guerrilla force to a military structure capable of applying more conventional TTPs went unnoticed

[32] Harel–Issacharoff 2008.
[33] Katz–Hendel 2011.
[34] Eilam 2016.
[35] Kaunert–Wertman 2020: 99–114.
[36] Harel–Issacharoff 2008.

and only became evident during the 34-day-war against Israel in 2006. The organisation displayed tactics and capabilities far beyond what was expected, to be fully framed in the typology of hybrid warfare. After the Israeli invasion, Hezbollah took full advantage of Lebanon's rocky terrain, ideal for ground movements but impractical for armoured manoeuvres. It has focused its battle-positions on easily defensible hilltop villages, which offer excellent observation and firing ranges and are inhabited by populations sympathetic to its cause. Despite being outnumbered, its units proved to be cohesive, well-trained, disciplined and experienced in how to control territory. Equipped with an effective chain of command and control, thanks to a complex communication system, Hezbollah successfully employed hedgehog defence tactics, creating strongholds in fortified bunkers, like a regular force. During the conflict, it continued to fire rockets at Israel using concealed launchers, even behind enemy lines. None of these tactics are characteristic of guerrilla forces, which usually rely on population-centred methods of concealment. In essence, Hezbollah took Israel by surprise because it acted in a manner that is not really attributable to an irregular fighter, nor to the regular army of a State. In the conduct of Iran's hybrid warfare, cyberattacks and info-ops are also increasing rapidly, as more and more Iranian hackers work to target individuals, companies and government entities around the world, focusing mainly on the Middle East region such as Saudi Arabia and Israel. In particular, Iran carried out a data deletion attack on dozens of Saudi government and private networks between 2016 and 2017.[37] The regime in Tehran exercises tight control over the domestic dissemination of information, restricting television broadcasts, social media use and internet access, which greatly limits foreign influence and promotes pro-regime narratives.[38] Internationally, info-ops have helped Iran perpetuate its image as a regional power, particularly as a challenger to Saudi Arabia and Israel, while simultaneously presenting itself as a reliable international partner. Iran's info-ops also include space as an arena of the 'grey zone'. Indeed, Tehran has on several occasions blocked satellite communication transmissions, as in the case of the interruptions of Voice of America and BBC broadcasts.[39]

[37] Coats 2019.
[38] Eisenstadt 2017: 62–72.
[39] Hicks – Hunt Friend 2019.

Kim against Seoul and Washington

North Korea's main activities in the 'grey zone' include cyber operations, political coercion and military provocations. North Korea has a skilled and sophisticated cyber force capable of carrying out disruptive operations around the world.[40] Notable cyber operations attributed to North Korea include the 2014 attack on Sony, the 2016 cyber heist against the Bangladesh Bank, and the 'WannaCry' malware worm released in 2017.[41] North Korea's political coercion aims to strengthen the regime's position by exploiting U.S. efforts to coordinate with its allies and regional partners.[42] For example, the ongoing trade war between the United States and China has forced the Trump Administration to seek a compromise between engaging in the maximum pressure campaign against Pyongyang and efforts to conclude a credible pact with Beijing on tariffs.[43] The trade war has unintentionally strengthened North Korea's political position by pushing U.S. regional allies, mainly South Korea and Japan, further into China's regional economic sphere of influence. According to Bloomberg columnist Daniel Moss: "The trade war could have been an opportunity to drive a wedge between China and its regional trading partners […]. Yet the Trump administration's irreverence for the collateral damage of its actions might end up drawing China's neighbours closer into its orbit."[44] The South Korean Government's announcement of the launch of an $8 million food aid package for North Korea, a decision supported by President Trump, is one such example of Kim's astute ability to amass a relative political advantage without comparable benefits for Washington and its regional allies.[45] As Brookings expert Jung Pak wrote in 2018: "At a minimum, North Korea is attempting to sow division within South Korea and shape Seoul's policies toward ones that are favourable to Pyongyang."[46] Regarding military provocations, it is sufficient to consider that the North Korean Army has deployed 70% of its forces within 60 miles of the Korean Demilitarised Zone (DMZ). The tactics developed by North Korea in the 'grey zone' also manifest themselves in space, considering that the country is probably the most active satellite system jammer in the world.

40 Chanlett-Avery et al. 2017.
41 Chanlett-Avery et al. 2017.
42 Pak 2018.
43 Bradsher – Sang-hun 2019.
44 Moss 2019.
45 Sang-hun 2019.
46 Pak 2018.

North Korea regularly blocks GPS signals in South Korea, jamming air routes and harbours close to the DMZ.[47] Fundamental, however, is the strategy adopted by Pyongyang through the constant threat aimed at neighbouring 'enemy' countries through missile tests and the proclamation of readiness to use the nuclear weapon.[48] In this, moreover, the North Koreans are on the same line as Russia's current cross-domain coercion strategies. For instance, the Democratic People's Republic of Korea's (DPRK's) short-range ballistic missile (SRBM) tests carried out on 4 May 2019 and 9 May 2019 highlighted the lack of cohesion in the alliance opposing Pyongyang,[49] as well as creating rifts within the U.S. Government itself.[50] Nevertheless, the U.S. was already engaged in coordinating a multinational 'maximum pressure' campaign aimed at deterring North Korea's future nuclear development, bringing the regime's leaders to the negotiating table, and ultimately denuclearising the Korean peninsula.[51] For the foreseeable future, two aspects are likely to influence the U.S. response to North Korean 'grey zone' activities. First, diplomatic grievances between North Korean and U.S. officials threaten to prolong stalled negotiations. The outcomes of talks in Hanoi in 2019 between former President Trump and North Korean leader Kim Jong-un bear witness to this. The second concerns the U.S. – South Korea joint military exercises. According to political analysts, a downsizing of the joint exercises would benefit the strategic objectives of North Korea, Russia and China at the expense of effective multilateral coordination between the U.S., South Korea and Japan. "Any such drawdown would face strong pushback from Congress and Japan, whose conservative government is deeply wary of North Korea's intentions."[52] North Korea's behaviour after the Hanoi summit also suggests that Kim is determined to find 'a new way' to strengthen his international position in the absence of an agreement with the U.S. To this end, Kim's visit to Russia in April 2019 and his continued engagement in China to receive economic support can be interpreted as a strategy to divide the U.S. and its regional allies while finding ways to circumvent international sanctions.[53] Russian investments in North Korea's infrastructure and mineral resources, for example, would strengthen

47 Harrison et al. 2019.
48 ANSA 2022.
49 Denyer–Joo 2019.
50 Sanger et al. 2019.
51 Cha – Fraser Katz 2018: 87–100.
52 The Japan Times 2019.
53 Min-hyung 2019; Herskovitz–Li 2019.

Kim's strategic position by reducing his dependence on a U.S.-brokered deal.[54] Essentially, North Korea's 'grey zone' activities are likely to exploit any glimmer of ambiguity that the U.S. would allow in its regional commitments.

Hamas's Asymmetrical Warfare

Hamas, an acronym of Ḥarakat al-Muqāwama al-Islāmiyya (Islamic Resistance Movement), born at the time of the first Intifada as the Palestinian operational arm of the Jamaʿat al-Iḫwān al-muslimīn (Muslim Brotherhood), has today become the hegemonic Palestinian organisation in the Gaza Strip. From the territories of the Strip it has been waging a war of attrition against Israel for years, consisting of suicide bombings, rocket attacks, incendiary balloons, and infiltration into Israeli territory through tunnels. The EU, the USA and several other states consider Hamas a terrorist organisation, Russia, Turkey, Iran and Qatar diverge from this position. The U.K. only considers the Izz al-Din al-Qassam Brigades, the military wing of Hamas, to be a terrorist organisation. By contrasting guided missiles and drones, hence Israeli technological superiority, with the narrative of the young Palestinian fighter armed with a sling and stones, i.e. the rhetoric of the First Intifada, Hamas puts itself on an asymmetrical war footing and, in terms of communication, in an advantageous position. We are in fact witnessing the reversal of a founding myth of Israel, namely the myth of David against Goliath. The organisation, however, is the author of precisely 'hybrid' actions, as emerges from a deliberately contradictory narrative. The one that places the stone-throwing boy alongside the Izz al-Din al-Qassam brigades' demonstrations of military might, in which Quassam rockets make a fine show. Hamas has an interest in showing itself weak, but also strong, and if then, such a strategy is accompanied by an effective use of the new technologies such as the social networks, the capacity to determine the flows of strategic communication ends up becoming even more incisive and viral. Here, then, is the effectiveness of the image of what appears to be little more than a child, targeting a Merkava tank with a stone throw. The image could be recent or old, it could have been taken in Gaza as in the West Bank, it could even be the result of a skilful photomontage. It does not matter. The point is that it is a recurring image, used by the mainstream media, along with hundreds of other very similar ones, to depict short news reports on events that

[54] Isachenkov 2019.

have been going on since 1948. So what is so special about it? It is simply viral. Viral because it is aimed at left-wing Israelis' sensitiveness and because it does so by evoking the myth of David versus Goliath, overturning it. In a nutshell, it colonises the collective imagination. We can imagine looking for Hamas's model of strategic-communicative rationality, confirming, albeit updating them to the times of social communication, the dynamics of guerrilla warfare and Arab revolt already in use in Lawrence of Arabia's time, i.e. asymmetrical warfare practices, a war fought with armed clashes (Bedouin guerrilla warfare against regular Ottoman troops), but also of semiotic clashes (Lawrence dressed in Arab clothes entering Cairo and announcing to General Allenby the taking of Aqaba), a war therefore to all intents and purposes asymmetrical, made up of weapons and signs (a *semio-war*).[55] It is at this point that the cross-media use of the different platforms available to Hamas intervenes, the social ones such as Facebook, Twitter, the YouTube channel, but also the radio Al Quds and the TV Al Aqsa. The latter two media with signal transmission capacity also in Israel, which become *echo chambers*[56] in which the final addressee receives, among the many, the only informative and media fragments "that confirm the ideological positions already acquired and on which he surrounds himself and feeds".[57] When effective, Hamas propaganda is believed not so much because of the truth or verisimilitude of the message itself, but because it is directed towards a category of receivers – those on the other side of the channel – who already know or suspect those things. Let us now look at the effectiveness of the info-ops carried out using 'human shields'. On 23 August, the Israel Defense Forces (IDF) bombed a residential building (Al Zafer tower), believed to be used as Hamas headquarters, causing its collapse. This incident also provoked international condemnation of Israel, thanks in part to Hamas's communicative ability to accuse Israel of war crimes. What remains is the message that Israel strikes civilian targets, causing innocent deaths and committing war crimes. Exactly the effect desired by Hamas. In the analysis in question, the use and results obtained by Hamas in the use of human shields is emphasised, a fact consistently applied to the following areas:

[55] Fabbri–Montanari 2004: 1–27.
[56] Quattrociocchi–Vicini 2016.
[57] Marino–Thibault 2016: 25–26.

- Placement of rocket launcher, artillery and mortar positions near densely populated areas, often near buildings protected by the Geneva Convention (schools, hospitals or mosques).
- Placement of military infrastructure, command centres, critical infrastructure, weapons depots, close to or near civilian areas or major road junctions.
- Protection of terrorist cells, safe havens or men injured or in danger because they are threatened by targeted killings by the IDF, near civilian, residential or commercial areas.
- Use of civilians, in the event of conflict in the strip, for intelligence tasks. Such reckless use of civilians means that Hamas can play the game with the IDF in a scenario where Hamas always wins. If the use of Israeli military force produces an exponential increase in civilian casualties, Hamas can move the propaganda machine by activating the combined use of social media, TV and independent journalists, having a good game in using the weapon of lawfare to accuse Israel of war crimes against innocent civilians. Otherwise, if Israel depletes its strike force so as not to hit innocent civilians, limiting the strikes as much as possible, Hamas has gained 'reflexive control' (Gerasimov *docet!*).

The practice of using human shields is not something Hamas is at pains to deny. At a press conference in 2018, Khaled Meshaal, the movement's political leader at the time, uttered the following words: "If you [Israelis] are so crazy as to decide to enter Gaza, we will fight you. You will face not only hundreds of fighters, but also one and a half million people, driven by the desire to become martyrs."[58] Another indicative confirmation of this orientation comes from a sentence uttered by Hamas spokesman Mushir Al-Masri in 2006, when the IDF warned of its intention to strike the home of one of the organisation's leaders, Waal Rajub Al-Shakra's in Beit Lahiya.[59] The Hamas spokesman pronounced the following words: "The citizens will continue to defend their pride and their homes, acting as human shields, until the enemy withdraws."[60] Finally, the statement by another Hamas spokesperson, Sami al-Zuhari, dating back to July 2014, thus pronounced in the hottest weeks of the Israeli invasion, is also interesting: "The fact that the

[58] Conference Press 2018.
[59] Al-Aqsa TV 2006.
[60] Al-Aqsa TV 2014.

population is happy to sacrifice themselves against the Israeli planes with the aim of protecting their homes, proves the validity of this strategy. Hamas therefore calls on our people to apply this practice."[61] The strategic communication model adopted by Hamas, largely like that of Hezbollah, is a multivariate model, based on a plurality of supporting media, both traditional and non-traditional, and is aimed both at 'friends', internally such as the Palestinian humma and Arab and Persian sympathisers, and at enemies, mainly Israel and the U.S. If in the past it was the traditional television medium that dominated such as Al Aqsa TV and Al Quds Radio, it was gradually joined by the YouTube medium and then the social networks, where trolls and memes, truth, fake news and misinformation began to work, mainly targeting the public opinions of Western countries and the Arab world, as well as the Israeli pacifist left-wing components. In such a model, dissemination strategies are typically mixed media that represent the coordinated use of several social media, or cross-media focused on a specific channel, e.g. Al Aqsa TV, the primary driver of the communication strategy and social as a means of disseminating the information produced by the primary channel. How can Israel counter these actions? It is clear that the repeated attacks against Al Aqsa TV[62] or Al Quds Radio[63] are not only useless, but even harmful. The message that immediately rebounds is that Israel strikes civilians and silences the media to cover it up. Inevitably, because of these critical issues, one wonders whether Israel has a counter-propaganda system capable of withstanding these new challenges, a system as efficient as its military one. For instance, it would be interesting to investigate, but this inevitably represents a new research question, whether Israel is capable of infiltrating Hamas chats by effectively counterpunching trolling practices, instead of scrambling in a futile and wasteful attempt to dismantle misinformation and virality with philological debunking. On the other hand, traditional military manuals have for decades admitted that guerrilla warfare is answered not by traditional methods, but by counter-insurgency warfare. This learning also applies to the infosphere in which pitting troll against troll is clearly not enough, and where it is necessary to dust off old, tried and tested weapons,

[61] Al-Aqsa TV 2014.

[62] Hit both in 2008 and July 2014, during the 2014 Israel–Gaza conflict by Israeli air strikes that also affected the radio station. In 2014, the TV station continued to broadcast, while the radio station went silent, only to return to the airwaves.

[63] Currently, a powerful antenna provided by Hezbollah re-transmits Radio Al Quds broadcasts from Lebanon into Israeli territory. The Shin Bet alleges that the radio transmissions contain encrypted messages addressed to Hamas fighters infiltrated in East Jerusalem and the West Bank.

such as the 'semiological guerrilla warfare' theorised by Umberto Eco, who stated that "the battle for the survival of man as a responsible being in the Age of Communication is not won where communication starts, but where it arrives".[64] It is interesting to note that, except for Hamas, which represents a non-state entity, all the other situations examined relate to states that have in common that they are not governed by democratic governments. This peculiarity is what allows them to resort so indiscriminately and invasively to hybrid warfare, or at least to act unscrupulously in the 'grey zone'. It is precisely autocratic, theocratic or dictatorial self-referentiality, depending on the nuance that sets the stage for governments themselves to self-justify their aggressive policies towards other states perceived as a threat to their own interests. It is also true that the U.S., the great theorists of these doctrines of contemporary warfare, has also long been engaged in activities that to all intents and purposes prefigure hybrid modes and 'grey' operations in its conduct of foreign policy. In the democratic world, however, they are the exception and not the rule and act by virtue of their superpower role. All other countries in the democratic area that find themselves embroiled in the 'total chaos warfare' taking place on the globe, act according to defensive principles and modes, not offensive ones like those of the various autocracies. Even Israel, for decades engaged in a struggle for its own survival, operates in adherence to defensive and containment strategies. We mentioned the United States as a superpower; American governments have always justified their courses of action by presenting themselves as bearers of the values of freedom and democracy. In truth, even the United States absolutely tends to look after its own interests like almost everyone else, but Washington needs a theoretical framework that gives moral dignity to its behaviour. Actually, it has to be said that there are peoples and cultures that traditionally care little for freedom and democracy; on the contrary, they judge them to be 'disvalues'. We conclude with a reflection that on the surface it has nothing to do with what is discussed in this essay, but only on the surface. The United States is also the home of rock'n'roll, and Western culture is where such music took root and grew. We think back with regret to the words of *Wind of Change* by Scorpions: "Blows straight into the face of time/Like a storm wind that will ring the freedom bell/For peace of mind/ Let your balalaika sing/What my guitar wants to say." How many expectations betrayed and how many dreams of universal peace shattered! True, I recognise

[64] Eco 2021.

that even in the West, there is a lot of rubbish being passed off as music, but unlike in the countries that are the subject of this study, at least here one can choose what to listen to and play.

Conclusion

'Ambiguous war', 'non-linear', 'hybrid', 'grey' war – different ways of referring to wars fought in ways that are now increasingly distancing themselves from traditional conflict concepts and doctrines, both at the strategic and tactical levels. Non-conventional warfare assumes a dominant role and, therefore, the military component in contemporary conflicts often does not wear a uniform or display distinctive symbols. In general, contemporary wars prefigure situations in which a belligerent state or non-state entity deploys military and paramilitary units in a confused and deceptive manner in order to achieve military and political objectives, concealing the direct participation of its armed forces in operations. Alongside combat forces, whether regular or irregular, we find forms of combat ranging from cyber warfare to information warfare, from the unscrupulous use of diplomacy to economic warfare. The United States are the major theorists of this type of conflict, but Russia, China, Iran, North Korea, as well as non-state entities such as Hamas, are the nations that on the world geostrategic scenario for the past twenty years have implemented hybrid combat, in fact triggering real conflicts that, with different forms and modalities, have manifested themselves in different parts of the planet. We are talking about countries where the concept of democracy and human rights is non-existent; it is significant that in a world where war, at least in principle, is repudiated as an instrument for resolving political disputes (let us recall von Clausewitz's definition of it), there are nations that, lacking the humanitarian scruples that are the patrimony of Western culture founded on Law, have found a pragmatic solution to conduct operations that until the recent past would have been openly indicated as full-fledged war actions.

Questions

1. In which forms can the asymmetrical dimension of hybrid warfare evolve as an instrument of struggle by organisations that do not have regular armed forces?

2. Is it likely that negotiation and its procedures themselves become a combat mode of hybrid warfare, depending on the messages they communicate?
3. Can hybrid warfare turn into a form of "total chaos warfare" due to the complexity, variety and quantity of interests and actors involved?

References

ANSA (2022): Corea del Nord, Kim: deterrenza nucleare contro Seul e gli Usa. *ANSA,* 28 July 2022. Online: www.ansa.it/sito/notizie/topnews/2022/07/28/corea-del-nord-kim-deterrenza-nucleare-contro-seul-e-gli-usa_baa60dd8-3b9d-4e52-8709-52f94e6b1a7a.html

Banasik, Mirosław (2015): How to understand the Hybrid War. *Securitologia,* 1, 19–34.

Beech, Hannah (2018): China's Sea Control Is a Done Deal, "Short of War With the U.S.". *The New York Times,* 20 September 2018. Online: www.nytimes.com/2018/09/20/world/asia/south-china-sea-navy.html

Bergman, Ronen (2018): *Rise and Kill First. The Secret Story of Israel's Targeted Assassinations.* New York: Random House.

Bradsher, Keith – Sang-hun, Choe (2019): With Kim's Visit, China Shows US It Has Leverage on Trade. *The New York Times,* 08 January 2019. Online: www.nytimes.com/2019/01/08/business/china-north-korea-kim-trade.html

Cha, Viktor – Fraser Katz, Katrin (2018): The Right Way to Coerce North Korea: Ending the Threat Without Going to War. *Foreign Affairs,* 97(3), 87–100.

Chanlett-Avery, Emma – Rosen, Liana W. – Rollins, John W. – Theohary, Catherine A. (2017): *North Korean Cyber Capabilities: In Brief.* Congressional Research Service. Online: https://sgp.fas.org/crs/row/R44912.pdf

Coats, Daniel R. (2019): *2019 Worldwide Threat Assessment of the US Intelligence Community.* Office of the Director of National Intelligence. Online: www.dni.gov/files/ODNI/documents/2019-ATA-SFR—-SSCI.pdf

Cooper, Zack (2018): *Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare.* Foundation for Defense of Democracies. Online: www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare/

Cristadoro, Nicola (2021): *La mossa del Drago. Strategia politico-militare e guerra di intelligence nella Cina del XXI secolo.* Torino: Edizioni Il Maglio.

Cristadoro, Nicola (2022): *La Dottrina Gerasimov. La filosofia della guerra non convenzionale nella strategia russa contemporanea.* Torino: Edizioni Il Maglio.

Darczewska, Jolanta (2014): The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study. *Point of View,* 42. Online: www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

Denyer, Sinon – Joo, Kim M. (2019): Kim Personally Supervised 'Guided Weapons' Test, North Korea Says. *The Washington Post,* 04 May 2019. Online: www.washingtonpost.com/world/north-korea-fires-several-short-range-projectiles-south-korean-military-says/2019/05/03/511efe92-6e0f-11e9-be3a-33217240a539_story.html

Department of Defense (2018): *Assessment on U.S. Defense Implications of China's Expanding Global Access.* December 2018. Washington, D.C.: Department of Defense.

Eco, Umberto (2021): Vision '67. In Traini, Stefano: *Le avventure intellettuali di Umberto Eco.* Milano: La Nave di Teseo.

Eilam, Ehud (2016): *Israel's Future Wars. Military and Political Aspects of Israel's Coming Wars.* Washington, D.C.: Westphalia Press.

Eilam, Ehud (2019): *Containment in the Middle East.* Lincoln: University of Nebraska Press.

Eisenstadt, Michael (2017): Information Warfare: Centerpiece of Iran's Way of War. In Hicks, Kathleen H. – Dalton, Melissa G. (eds.): *Deterring Iran after the Nuclear Deal.* Washington, D.C.: Center for Strategic and International Studies. 62–72.

Fabbri, Paolo – Montanari, Federico (2004): Per una semiotica della comunicazione strategica. *E/C, Rivista dell'Associazione Italiana di Studi Semiotici,* 1, 1–27.

Frenza, Maxia M. (2019): *Modelli di comunicazione strategica a supporto dell'Hybrid Warfare: l'apparato di propaganda di Hamas.* Roma: Centro di Ricerca sulla Sicurezza ed il Terrorismo.

Gardner, Hall (2015): *Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict.* Research Paper 123, Rome: NATO Defense College.

Gaub, Florenze (2015): *Hizbullah's Hybrid Posture: Three Armies in One.* Paris: European Union Institute for Security Studies.

Gordon, Michael R. – Page, Jeremy (2018): China Installed Military Jamming Equipment on Spratly Islands, U.S. Says. *The Wall Street Journal,* 09 April 2018. Online: www.wsj.com/articles/china-installed-military-jamming-equipment-on spratly-islands-u-s-says-1523266320

Gross, Michael L. (2018): *Fighting without Firearms. Contending with Insurgents and Soft, Non-Kinetic Measures in Hybrid Warfare.* MCDC Countering Hybrid Warfare Project. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/717543/MCDC_CHW_Information_Note-Fighting_without_Firearms-March_2018.pdf

Harding, Brian (2019): *China's Digital Silk Road and Southeast Asia.* CSIS, Commentary. Online: www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia

Harel, Amos – Issacharoff, Avi (2008): *34 Days. Israel, Hezbollah and the War in Lebanon.* New York: Palgrave Macmillan.

Harrison, Todd – Johnson, Kaitlyn – Roberts, Thomas G. (2019): *Space Threat Assessment 2019.* Washington D.C.: Centre for Strategic and International Studies.

Herd, Graeme P. – Akerman, Ella (2002): Russian Strategic Realignment and the Post-Post-Cold War Era? *Security Dialogue,* 33(3), 357–372. Online: https://doi.org/10.1177/0967010602033003009

Herskovitz, Jon – Li, Dandan (2019): *China, North Korea Open New Border Crossing Despite Sanctions.* Online: www.bloomberg.com/news/ articles/2019-04-08/china-north-korea-open-new-border-crossing-despite-sanctions

Hicks, Kathleen H. – Hunt Friend, Alice eds. (2019): *By Other Means. Part I: Campaigning in the Gray Zone.* Washington, D.C.: Center for Strategic and International Studies.

Hoffman, Frank G. (2006): *Lessons from Lebanon: Hezbollah and Hybrid Wars.* Pennsylvania: Foreign Policy Research Institute. Online: www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/

Isachenkov, Vladimir (2019): Russian President Putin Hosts Kim Jong Un for Talks on North Korean Nuclear Standoff. *Time,* 25 April 2019. Online: http://time.com/5577801/vladimir-putin-kim-jong-un-meeting-russia/

Kapusta, Philip (2015): *The Gray Zone.* United States Special Operations Command. Online: https://info.publicintelligence.net/USSOCOM-GrayZones.pdf

Katz, Yakoov – Hendel, Yoaz (2011): *Israel vs. Iran. The Shadow War.* Dulles: Potomac Books.

Kaunert, Christian – Wertman, Ori (2020): The Securitisation of Hybrid Warfare through Practices within the Iran–Israel Conflict – Israel's Practices for Securitising Hezbollah's Proxy War. *Security and Defence Quarterly,* 31(4), 99–114. Online: https://doi.org/10.35467/sdq/130866

Marino, Gabriele – Thibault, Mattia eds. (2016): Viralità – Virality. *Lexia. Rivista di semiotica,* 25–26.

McInniss, Matthew J. (2017): Proxies: Iran's Global Arm and Frontline Deterrent. In Hicks, Kathleen H. – Dalton, Melissa G. (eds.): *Deterring Iran after the Nuclear Deal.* Washington, D.C.: Centre for Strategic and International Studies. 25–33.

Min-hyung, Lee (2019): Kim Jong-un Arrives in Vladivostok for Summit with Putin. *The Korea Times,* 24 April 2019. Online: www.koreatimes.co.kr/www/nation/2019/04/356_267718.html

Moss, Daniel (2019): *With Friends Like the U.S., Who Needs Economic Foes?* Online: www.bloomberg.com/opinion/articles/2019-05-23/japan-south-korea-get-reminder-of-how-powerful-china-s-economy-is

NATO 2022 Strategic Concept. Online: www.nato.int/strategic-concept/

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Monterey: Naval Postgraduate School.

Office of the Secretary of Defense (2017): Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. Office of the Secretary of Defense, May 2017.

Ottaviani, Marta F. (2022): *Brigate Russe. La guerra occulta del Cremlino tra troll e hacker.* Milano: Ledizioni.

Pak, Jung H. (2018): *Kim Jong-un's Tools of Coercion.* Online: www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion/

Quattrociocchi, Walter – Vicini, Antonella (2016): *Misinformation. Guida alla società della disinformazione e della credulità.* Milano: Franco Angeli.

Rusnáková, Soňa (2017): Russian New Art of Hybrid Warfare in Ukraine. Slovak Journal of Political Science, 17(3–4), 343–380. Online: https://doi.org/10.1515/sjps-2017-0014

Sanfelice Di Monteforte, Ferdinando (2020): Scenari di guerra ibrida nel Mediterraneo allargato. *Mediterranean Insecurity,* 22 February 2020. Online: www.mediterraneaninsecurity.it/2020/02/22/scenari-di-guerra-ibrida-nel-mediterraneo-allargato-amm-sq-ferdinando-sanfelice-di-monteforte/

Sanger, Daniel E. – Broad, William J. – Sang-hun, Choe – Sullivan, Eileen (2019): New North Korea Concerns Flare as Trump's Signature Diplomacy Wilts. *The New York Times,* 09 May 2019. Online: www.nytimes.com/2019/05/09/world/asia/north-korea-missile.html

Sang-hun, Choe (2019): Trump Supports Food Aid for North Korea, South Says. *The New York Times,* 07 May 2019. Online: www.nytimes.com/2019/05/07/world/asia/trump-north-korea-food-aid.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer

The Japan Times (2019): U.S., South Korea to Scale Back Large-Scale Spring Military Exercises. *The Japan Times,* 02 March 2019. Online: www.japantimes.co.jp/news/2019/03/02/asia-pacific/u-s-south-korea-scale-back-large-scale-spring-military-exercises/#.XMG1g2hKjcs

The United States Army Special Operations Command (2015): *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014.* Online: www.jhuapl.edu/sites/default/files/2022-12/ARIS_LittleGreenMen.pdf

Thomas, Jason (2020): China's "Fishermen" Mercenaries. *The Weekend Australian,* 02 September 2020.

Walker, Christopher (2018): What is "Sharp Power"? *Journal of Democracy,* 29(3), 9–23.

Jaroslav Kompan – Milan Turaj – Michal Vajda[1]

Operational Environment

With the collapse of the Warsaw Pact in the early 1990s, there was a shift from the concept of conducting large-scale operations against a close-to-peer adversary, as a situation arose with relatively minimal risk of war between states. The overall change was towards multinational peace support operations, i.e. less extensive deployment of military forces within the continuum of conflict.[2] After the events of 11 September 2001, the concept of conducting limited expeditionary operations aimed at acting against irregular forces – counterterrorist and counterinsurgency operations within the framework of conflict stabilisation in Iraq or Afghanistan came to the fore. This led to a change in military thinking, but also in the overall development of the armed forces, whose decisive task, instead of the combat operations, became support for the stabilisation of conflict regions within the framework of international crisis management.[3]

Politics and war

The change in the philosophy of conducting traditional military operations occurred only after the events in Ukraine in 2014. The stability of the external security environment was mainly affected by the dynamics of the development of the security situation in Ukraine and Russian–Ukrainian relations.[4] The above was further deepened in 2022, when Russian military forces invaded the territory of Ukraine. Globally, the core task of the armed forces has come to the fore, namely to guarantee the defence and security of the state against an external armed attack by a foreign power, including against a conventional adversary, which does not only deploy its forces conventionally,[5] i.e. a hybrid adversary in a "hybrid" Operational Environment (hereinafter: HOE). This way of waging

1 Armed Forces Academy of General Milan Rastislav Štefánik.
2 Marek 2019.
3 Andrassy 2019: 80–107.
4 Mušinka 2021.
5 Mattis–Hoffman 2005: 18–19.

war is usually referred to as hybrid war and threats associated with current conflicts as hybrid threats. Due to the blurred or missing boundaries between war and peace, and the involvement of unclear or covert actors, it is not easy to face such threats. Just as hybrid warfare is conducted by a mixture of military and non-military means, the response to hybrid war must include a mixture of military measures complementing a comprehensive package of non-military, i.e. political, economic, diplomatic and other means.[6] A comprehensive understanding of the HOE is almost impossible due to its complexity. It is a difficult task not only during linear-symmetrical conflict, but especially if there is a nonlinear conflict, whether counterinsurgency or hybrid. Another important factor that greatly limits the possibility of understanding all phenomena and contexts in a particular operational environment as thoroughly as possible is time. One could claim that the less time one has to evaluate the operational environment, the more likely it is that the individual elements of the operational environment and their relationships are misunderstood.[7] During recent decades, we have witnessed that conflicts are not conducted in the usual way. Wars are not declared and do not end by a peace agreement. Conflicts are still waged with the use of military instruments, but these are getting increasingly outweighed by non-military means such as economic sanctions, restrictions on the energy supplies, information operations, propaganda and dissemination of misinformation, terrorism and increased involvement of non-state actors. Systematic attacks on states are referred to as colour revolutions, grey zone conflicts, unconventional wars, unrestricted wars, or non-linear wars. The boundaries between peace and hybrid war, combatants and non-combatants are blurred.[8] The fundamental dilemma of conflicts and wars with limited objectives after World War II such as Korea, Vietnam, Afghanistan, Chechnya and Iraq was the achievement of political goals in the country of intervention and also the termination of the deployment of military forces so that their withdrawal did not look like a defeat.[9] Without legitimate and dedicated political support, a military instrument of state power cannot be used for the achievement of a relevant and, at the same time, desired political result. Also, without legitimate support from allies and one's own country, it is impossible to pursue political

6 EEAS 2015.
7 Spilý 2014: 132–140.
8 Hoffman 2007.
9 Kompan–Hrnčiar 2021: 87–107.

goals and effectively use the space and time created by military intervention. Without such support, there is a general perception of partial failure, which results from the different perspectives of politicians and military commanders on their responsibilities and capabilities in times of conflict, war, or intervention. Politicians are necessary for determining political goals, ways and means, but military instruments of power are used to achieve them. Military forces are executing activities in accordance with their standards and political directives, even in very violent conditions, by very violent solutions. Therefore, it is up to the politicians to determine the political outcome of the war, including the hybrid war, which can also be achieved using the military instrument of power.[10] When defining military strategy in hybrid warfare, it is appropriate to understand the characteristic of politics, resulting from the political system and processes and its violent manifestation, which is called war. For this definition, we can consider the quote "war is nothing but a continuation of politics with the admixture of other means"[11] as one of the foundations. War is directly based on the definition of conflict, which is one of three basic relationships and situations, the others being the state of security and crisis situation, which are the result of relations between communities of states, the states themselves, nations, and other elements of the social structure of society. Neither peace nor war exist in their extreme forms. Ideal peace is a utopia, and absolute war is a theoretical construct with unlimited violence. Instead, these terms belong to both ends of the conflict spectrum, expressing the wide variety of evolving conditions existing between states. Somewhere between these terms lies the definition of a hybrid war, when it is already difficult to determine whether we could evaluate the situation as war or as peace.[12] War is generally a conflict between states, organisations, or larger groups of people, characterised by the use of violence or physical force between the warring parties. A typical feature of war is the fact that the parties involved are convinced that the use of military force is the only way to resolve mutual disputes.[13] Traditional definitions of war have focused on armed conflict between states, in which one or both sides usually fight for national survival. Such a conflict is close to the concept of absolute war, a situation that requires the mobilisation of all national resources. However, we could consider hybrid

[10] Kompan 2020: 106–113.
[11] Clausewitz 1946.
[12] Kompan 2020: 106–113.
[13] Vejmelka 2005.

war as an intersection between the economic, social and military domains, so it is a social and military phenomenon simultaneously. Therefore, the use of force in hybrid warfare is determined by broader contexts based on politics and not solely on military capabilities or lack thereof. In a hybrid war, states fight over material interests or values, and opposing social groups compete for resources, identity, religion, or emotional expression. War, including hybrid war, generally ends in destruction, mutual attrition, compromise, defeat, surrender, or simply a pause before its next violent or nonviolent phase.[14] Each war has its specific causes, but in general, one could claim that the most fundamental reason is always the human desire for power. Political conflict usually transforms into war when political opponents sense an opportunity, based on their relative power and understand war as a means to defend and spread their truth and expand their influence. Power is inherently unequally distributed and its distribution varies in time and character from one society to another. Power could be understood as a material component determined by the amount of resources or physical means of coercion in terms of weapons and units. At the same time, we could also understand power as a non-physical intangible component that results from legal, religious and scientific authority, intellectual or social prestige and reputation and that supports the diplomatic or military instrument of power.[15] In its essence, power provides the means to attack and, at the same time, repel the attack of another entity.[16] Politics is thus the process by which power is distributed in human society. A process of distribution that may be relatively fair by consensus, inheritance, election, or tradition. This process could also be chaotic with the use of violence, revolution or struggle. In any case, the dynamics of politics creates a constant pressure on the distribution of power and a change in the power arrangement. Political events are the result of conflicts, that is, the activities of compromising or antagonistic parties and their interactions. We could apply exactly these same characteristics to hybrid warfare, which makes it an instrument for policy enforcement, i.e. power sharing. In its essence, war, and hybrid war as such, is an act of force intended to force adversaries to fulfil someone else's will. Hybrid war could be characterised as a long-term and wide-spectrum organised action on adversaries with social and economic impact, the purpose of which is to achieve a certain political goal or goals. Classical war

[14] Bassford 1997.
[15] Bassford 1997.
[16] Vego 2009.

is a violent manifestation of tensions and disagreements between political groups. It begins when political conflict reaches an emotional level where organised violence is unleashed. In a hybrid war, however, unleashed violence could only be understood as one of the tools and not as the only exclusive tool.[17] In general, we could claim that political leaders use the military instrument of power in hybrid warfare when they consider its political necessity, regardless of whether it is beneficial in the given situation or not. This means that even military strategists in hybrid warfare must fully understand the political objectives, which could sometimes be very emotionally or militarily unclear. They must be able to transform these political goals into military effects that will support the achievement of the desired political outcomes.[18]

Politics and military strategy

We could claim that the strategic environment of hybrid warfare is defined by the nature of politics and the interactions among political entities. Such a complex environment tends to be influenced by dynamic and sometimes contradictory factors that result from the rationality and emotionality of politics. The creator of military strategies should be able to evaluate the importance and peculiarities of these factors and the extent of their influence on the strategic environment of hybrid warfare. Based on the dynamism of the environment, strategies are then created as long-term plans to achieve a political goal or goals.[19] Military strategy in hybrid warfare is part of a national or even international strategy that represents the way in which military power can be generated and deployed and how military instruments support other power instruments to achieve the political goals of a given country or group of countries. Documents that guide military strategy must clearly state how the military strategy will integrate with other non-military elements of the strategy. It is also necessary to clarify the mutual relationship between military strategic goals and the achievement of political-strategic outcomes.[20] The military forces in a hybrid war are basically responsible for creating and maintaining the conditions required by other entities

17 Nemeth 2002.
18 Vego 2009.
19 Bassford 1997.
20 Kompan 2020: 106–113.

or in favour of other power tools. It is highly unlikely that the resulting strategic state will be achieved by military activities alone. After deciding on the final strategic goal (end) and the role of the armed forces in achieving it, resources are allocated and a decision is made on how to appropriately use them. An adequate military strategy in hybrid war depends on the successful alignment of ends (goals), ways (strategic directions) and means (resources):

- Ends (Goals) – the crucial factor in establishing clear and unambiguous goals in hybrid warfare. However, at the strategic level, it is not always possible to establish a permanent objective due to the complexity of the strategic environment. If the strategic objectives are not clearly defined, the initial planning will have to be executed according to a general political directive, which may lead to a partial misunderstanding of the adversary's intentions. There is also a difference between a strategy for the complete achievement of the envisioned end state and a strategy for interrupting the deployment at a strategically convenient moment. Those two differ in character and time frame, and focusing only on the complete achievement of the resulting state could reduce the chance of ending the conflict with lower resources (means) spending.
- Ways (Directions) – if objectives and means are available, a plan is developed to ensure the best use of available resources, including a directive on the use of means to achieve hybrid warfare objectives. Directions could be, for example, strategic plans on countering hybrid threats. Planning should consider the likelihood of change in goals or means, and plans should also be prepared for unexpected events which have to be always expected in a hybrid war.
- Means (Resources) – the means available for the fulfilment of the plan are the resources or capabilities assigned after the process force generation and tailoring the requirements necessary to counter hybrid threats. These means should be used in a way that does not conflict with the strategic objectives within the given policy framework, even if this would not be the most efficient way to use them.[21]

In essence, in hybrid war as in classical war, we could recognise two ways of deploying military force to impose one's own will on the adversary while linking political goals with military strategic ones. The first is based on the

[21] Bassford 1997.

complete elimination of the adversary's military capabilities so that he cannot continue to resist. The second way is to inflict only limited physical losses on the adversary but to emphasise the decline in the morale of the population and combatants or the loss of political will to resist so that he begins to negotiate or immediately accepts the stipulated terms. The first alternative can be called the strategy of annihilation and it is associated with unlimited political goals. This means that we seek out and eliminate the specific military defence capabilities of the adversary, thereby disarming him and giving him no room for negotiation, but only for the unreserved adoption of our will. The second alternative can be called erosion strategy and it represents limited political goals. In this strategy, we try to inflict such losses on the enemy that negotiation and ending the fighting is a more lucrative alternative compared to continuing the resistance. Anyway, regardless of the application of any strategy, the achievement of goals, so-called victory, depends on the use of economic, diplomatic, and informational tools, and the use of military force is only a supporting factor of the other tools.[22] Therefore, a thorough understanding of the interrelationship among political and military objectives is essential for all military strategists in hybrid warfare, whether applying or resisting it. It may be that military factors will guide policy at some point. Political goals, on the other hand, will always influence the nature of the conflict. The more effort is made when the existence of the system is threatened and there is a clear justification for armed intervention, the more obvious the military character of the conflict will be. Based on the end state, the political goals of a certain entity can be divided into limited and unlimited/high-end.[23] Unlimited political goals are aimed at eliminating the adversary as a political entity, it means eliminating political representatives, including political organisational structures. Limited political goals are rather aimed at forcing the adversary to negotiate or accept proposals without eliminating political structures or initiating a process of political change.[24] Based on the above facts, it is clear that unlimited political goals will mostly be supported by a military strategy of annihilation, in hybrid warfare. The strategy of erosion is not initially suitable in achieving unlimited goals, because when the adversary understands that our goal is to eliminate him completely, he will try to use all available resources to avert such a threat and preserve his existence. Limited political goals could

[22] Kompan 2020: 106–113.
[23] Bassford 1997.
[24] Bassford 1997.

be achieved by a strategy of erosion, which in this case is more socially and politically acceptable, and based on lessons identified from recent conflicts, even feasible. In specific cases, it is also advantageous to use a military strategy of limited annihilation, which would be focused only on the military component or even only on specific military capabilities or other capabilities, so the loss of will to resist will be the only possibility to survive.[25] Based on the knowledge gained, we could claim that political and military strategic goals are fundamentally different in hybrid warfare, despite the fact that military strategic goals must be based on political goals. Political objectives should describe a vision of what the desired political outcome state is, i.e. what we want to achieve, including success criteria in hybrid war. Military strategic objectives should define how to achieve the desired political outcome by military instruments of power,[26] even in hybrid war.

Peculiarities of Hybrid Warfare

We could understand war, in accordance with Clausewitz's claim, as a natural and fundamental part of politics,[27] because it represents the basis of politics, that is the struggle for power, and hybrid war is no exception to this claim. War is a long-term organised action, mostly violent, and also mostly between political opponents. According to Clausewitz, the political intention is the purpose, the war is the means, and the means cannot be divorced from the purpose.[28] War, including hybrid war, could therefore be defined as a "policy tool" or even more precisely identified as a tool for solving political disputes.[29] Such an understanding of war can already be found in the work of the Chinese philosopher and military strategist Sun Tzu from the 6th century BC, who claimed that a ruler starts a war by giving orders to his duke. But only the duke will win, whose ruler does not interfere in the command of the army.[30] This means that war without a political decision and determination of goals is not sustainable.

25 Kompan 2020: 106–113.
26 Vego 2009.
27 Clausewitz 1946.
28 Clausewitz 1946.
29 Krejčí 2011.
30 Tzu 1910.

At the same time, but after the start of the war, it is necessary to leave military activities in the competence of military commanders and political activities in the responsibility of politicians. Military and civilian leaders have different competencies, perspectives and responsibilities. Therefore, close cooperation of political and military representatives is necessary so that military forces and means are used to achieve the right political goals in hybrid warfare.[31] War represents total violence and conflict resolution using maximum force.[32] But war is still only one of the means to resolve conflicts, terminal in its essence. First of all, it is necessary to use international law and diplomacy to resolve conflicts. But one should not forget the lessons from history and the statement by the Prussian king Frederick II The Great that "negotiations without weapons is like music without instruments".[33] In determining political goals, especially those that could be achieved by military instruments of power, it is necessary to maintain close cooperation among political representatives and the military component. Maintaining national and military strategies as separate strategies sets the stage for later failure to achieve policy goals in hybrid warfare. Such a separation opens a gap between political goals and military plans, which should be bridged by a strategy that determines exactly how to use military force to achieve the desired political result and not just the military result in hybrid warfare. A military strategy, the application of which military targets are effectively destroyed, is successful from a military point of view, but may fail from a political point of view, unless it also has an impact on the politics of the adversary.[34] Therefore, a thorough understanding of the hybrid operating environment is essential, and not only by military commanders but also by political representatives. The operational environment is generally understood as the sum of conditions, circumstances and influences acting on the deployment of capabilities and reflected in the decision of the military commander. The operational environment is a multidimensional system. Understanding its structure and its internal and external relationships is a determinant for success in modern military operations.[35] It is part of the overall security environment, which expresses the spatial dimension of security, where security actors operate at a specific time

[31] Betts 2002: 23–30.
[32] Krejčí 2011.
[33] Reddaway 1904.
[34] Kompan 2020: 106–113.
[35] Spilý 2014: 132–140.

and with specific security interests. The security environment is the environment in which the reference to social entity asserts its security interests in interaction with the sources (carriers) of security threats.[36] Thus, a change in the security environment will also affect fluctuations in the operational environment, and this will also affect the decision-making of military commanders. For the purposes of a closer understanding of the current hybrid operational environment, it is essential to understand the current security environment with an emphasis on the military strategic environment, because it is the strategic environment that directly determines the strategy, and it shapes the operations that fulfil it.[37] This means that the security environment shapes the operational environment, which influences the decision-making of commanders. Therefore, in hybrid warfare, commanders at all levels of command and control are required to constantly monitor and correctly assess the adversary's objectives in order to avoid surprise and at the same time to maintain the ability to conduct sustainable operations in the designated operational environment. The adversary usually tries as a priority to disrupt the ability to move and manoeuvre in all domains,[38] which causes a delay or even failure to carry out military operations,[39] and thus also a failure to support other instruments of power. At the same time, the adversary is interested in disrupting the command and control system, which causes disruption of the entire decision-making cycle of observation, orientation, decision and action, and thus the loss of initiative and pace of military operations. This could be caused, for example, by disrupting the global positioning system, cyberattacks,[40] data piracy, neutralisation of the transmission infrastructure (satellites, transmitters), or attacks on power production or transportation networks.[41] The study of modern conflicts shows that they mostly start and end in the land operational domain.[42] Therefore, their solution often requires the deployment of such military force and such military capabilities that are able to implement control and manoeuvre in the land operational environment and at the same time to maintain contact with the population in the given domain. The land environment is characterised

36 Žídek–Cibáková 2009.
37 Department of the Army 2019a.
38 Department of the Army 2019a.
39 Asymmetric Warfare Group 2016.
40 *Bezpečnostná stratégia Slovenskej republiky* 2021.
41 Van Coppenolle et al. 2022.
42 IISS 2020.

by a multifaceted morphology and varying physical properties; therefore, its control should be carried out in such a way as to create conditions for further activities. When planning and executing operations, it is also appropriate to consider the fact that the land environment is a permanent living space for the population, which brings a specific measure to conducting operations.[43] Timely and accurate deployment of adequate military forces, as well as maintaining their mobility, protection and sustainability is essential for the success of operations.[44] This is because the conduct of operations in a hybrid war, especially in a land environment, is characterised by the following aspects, which can also be called challenges for the deployment of military forces in a hybrid operational environment:

- Varying density of deployed forces and resources – due to a non-linear operational environment, which also causes dispersion of efforts and makes it difficult to focus and concentrate forces, and at the same time places high demands on freedom of movement and manoeuvre. Therefore, a high level of unit mobility, reliability, communication and interoperability is required, which makes it possible to increase the level of coordination between operational factors of time and space.
- Immediate sharing of acquired data – has a decisive impact on the conduct of operations in the land environment, as it ensures a higher degree of freedom of movement in the area of operations.
- Conducting operations inside an environment shaped by human activity – from minimally shaped (e.g. agricultural landscape) to extremely changed (megalopolis), which requires a complex change in the methods of deploying forces and enormous demands for shaping such an environment in the event of its degradation. Part of the response is also the creation of new military concepts such as NATO's concept for conducting expeditionary network-centric combat operations. These operations are led by task groups of very high readiness based on ground forces (battalion and brigade combat groups), which are able to react almost immediately, effectively and precisely to threats even on the NATO periphery.[45]

[43] Rolenec et al. 2019: 33–40.
[44] Podhorec 2012: 41–50.
[45] Schultz 2017.

- Rapid change of the situation – caused by technical and technological development, which places high demands on rapid decision-making, increased protection of forces against high-precision weapons and continuous deployment of available sensors, because the reaction time is significantly reduced.[46]
- Development of technologies and the development of new weapon systems – these significantly limit the manoeuvre in the area of operations (concepts of "Anti-access – Area denial")[47] which instead of restricting the manoeuvre in an area, act rather point-wise and precisely on the components of the forces, which requires a great effort to support mobility to ensure a hidden and dynamic manoeuvre. At the same time, the need for constant movement also comes to the fore, because the development of new types of nuclear warheads, may lead to a return to the concept of their tactical use.[48]

The development of the operational environment of hybrid warfare directly affects the change in the focus and the way the military instrument of power is used. Conventional and hybrid threats and the conduct of high-intensity conflict operations aimed at defeating adversary conventional forces from the territory of an attacked NATO member state are coming to the fore.[49] Military activities are inherently complex and require the joint action of all actors in the crisis area. Military activities, even in hybrid warfare, dynamically apply combat power, but this power must be legitimate, consistent in targeting, stoppable, controllable and generated specifically and at the same time adequately for each specific situation. Following the nature of the hybridization of conflicts, it is necessary for military activities to be in full synergy with other non-military activities, as part of a comprehensive approach to solving the emerging crisis. The general goal of military activities is to gain a military advantage over the adversary. This advantage could be achieved by a complex combination of the following two types of activities, namely:

- conventional kinetic military activities – focused on the physical part of the hybrid operational environment

[46] Gressel 2020.
[47] Jenzen-Jones – Lyamin 2014.
[48] Lowther 2020.
[49] Asymmetric Warfare Group 2016.

– information activities – focused on the perception of the hybrid operational environment, i.e. the mostly non-physical component of the hybrid operational environment[50]

Both types of activities will always produce an effect that will be followed by a dynamic interaction between the actors of this process, in some cases difficult to predict. Therefore, success in the hybrid operational environment will require finding the right balance between both types of activities, including through the appropriate alignment of operational factors in a hybrid operating environment.[51]

Perception of operational factors

Due to changes in the operational environment and the hybridisation of conflicts, military operations could also be conducted against organised non-state armed forces (proxy groups, mercenaries). The immediate goal of military forces is to maintain their own freedom of action and limit the freedom of action of adversary forces and their freedom of movement. Operations are conducted at a high pace and this increases the demand for their security (e.g. logistics, information collection). When operating in such an environment, it is necessary to consider the goals of the adversary, which will mostly be aimed at limiting and influencing the operations themselves or at least taking advantage of instability, using any means (terrorism, criminal activities, disruption of public order, etc.) in all military domains of a hybrid operational environment, including informational one.[52] Effective application of the military instrument should be aimed to use the hybrid operational environment to their advantage. Therefore, it is necessary that operational factors such as time, space, force and information are perfectly coordinated during military operations in hybrid warfare. Military commanders must constantly assess the relationship of time, space and force, including in relation to the informational environment and information. The correct alignment of presented factors creates the conditions for success in military operations.[53] A fundamental requirement of military operations in

[50] Department of the Army 2019a.
[51] McCuen 2008: 107–113.
[52] Hoffman 2007.
[53] Vego 2009.

hybrid warfare is to obtain and maintain freedom of action, i.e. the ability to make a variety of critical decisions to achieve assigned military objectives. And it is precisely the appropriate balance of individual operational factors that is the primary aspect of success.[54] The factor of space includes the land, sea, air and space domains, including all their distinctive features that affect the deployment of military forces. If the space factor is not correctly and realistically evaluated or is completely ignored, military operations fail in hybrid warfare. The stated premise is based on the fact that space will always be the source and at the same time the goal of military operations. The goal is that without control of the space, the execution of military operations is greatly limited or impossible. It becomes a resource due to the need for sufficient space to deploy and concentrate military forces, perform manoeuvres and conduct operations. Space must therefore be controlled to such an extent that military objectives can be achieved in hybrid war. Military commanders should be able to understand the basic characteristics of the space in which they will conduct operations of hybrid warfare, its dynamic and topographical components and the distances between areas of interest. The basic historically proven logical parallel applies that larger military forces require more space for movement and manoeuvre. Space, with its distances and physical characteristics, is therefore a critical factor for the deployment of military forces in a hybrid operational environment. Of course, we could evaluate the factor of space as essential, but we do not evaluate it as the most important, because only the factors of time and force add importance to it.[55] The factor of time is very closely connected with the factor of space, but time, unlike space, is much more dynamic and especially unrepeatable. The loss of space is replaceable because space could be regained or at least shaped to one's advantage, but the loss of time provides a definite advantage to the adversary in hybrid warfare. In its essence, the parallel applies that the larger the force, the more time it needs to be deployed in an operation, and this is further amplified by the size of the space in which it operates or in which it is to be deployed. Since World War II, it has been obvious that military units spend several times more time in preparation and moving than in conducting the activity itself.[56] This brings with it the risk that even the smallest incident such as the

[54] Vego 2009.
[55] Vego 2009.
[56] Lawrence 2017.

restriction of movement can disrupt the temporal sequence and synchronisation of the subsequent combat activity, thereby making it difficult to achieve military objectives. When planning military activities, a certain time flexibility is left for unforeseen circumstances (threats or opportunities), but in standardised activities there is reliance on a norm, which may not be plausible for a specific hybrid operational environment. With the development of technologies, the importance of time as an operational factor also comes to the fore. Technologies provide the ability to move quickly, continuously collect and process information, and provide an advantage over a technologically inferior adversary, but against peer adversaries, their advantages become disadvantages such as overloading systems, limiting mobility. In any case, the time gained, even if relative, must always be used to gain an advantage, without any hesitation or delay. Optimising one's own internal processes including decision-making, activation time, reaction time, and at the same time disrupting the same processes of the adversary and thereby the adversary will relatively lose the initiative seems to be the most suitable way of gaining time.[57] The time factor can be considered fundamental in the hybrid operational environment. Documented by modern operations, where technologically advanced military forces were able to overcome large distances in a relatively short time, e.g. coalition invasion of Iraq (more than 500 km in 20 days)[58] or control a large country, e.g. Operation Serval in Mali.[59] In general, we could say that the ability to act faster than the adversary brings a decisive advantage. A numerical or spatial disadvantage can be partially or completely offset by the ability to more quickly achieve the assigned objectives in a limited time. The force factor (understood as available forces, e.g. military forces) represents, in its narrowest sense, the military instrument of power. Available forces are not only limited to military forces, but also to other components which are contributing to the overall success. In general, we could say that the greater the amount of available forces available compared to the adversary, the more freedom of action the commander has in hybrid warfare.[60]

[57] Vego 2009.
[58] Iraq War 2003–2011.
[59] Shurkin 2014.
[60] EEAS 2015.

Holistic view of domains

We could consider the factors of space, time and force traditional. In contrast to them, the factor of information represents a factor that is inherently different from others. It is a consequence of the controllability of information, i.e. the possibility to significantly disrupt or direct the flow of it, and at the same time the indeterminacy and immeasurable nature of what information is. Information is always a source of power, but especially in the current information age, it can bring confusion and a source of system overload. A proper assessment of a force, space and time cannot be made without accurate information about all important aspects of the hybrid operational environment and operational situation. Accurate, timely and reliable information is fundamental to the decision-making process and it could also affect the morale, force cohesion and support of the population. Thus, the hybrid operational environment is an environment directly affected by the hybrid war and all instruments of power are applied in it. It contains all actors and their activities. It includes all physical and non-physical spaces and factors that are relevant to all domains (sea, land, air, space, cyber and information). The operational environment, and thus also the hybrid operational environment, is usually described as a set of interconnected elements, namely political, military, economic, social, informational and infrastructural, including physical environment and time, also known as PMESII-PT (hereinafter: PMESII-PT, to be described later in detail). By analysing PMESII-PT, it is possible to achieve an understanding of the hybrid operating environment, which creates conditions for synchronised and adequate creation of effects using instruments of power. By the correct application of instruments of power and additional capabilities aimed at creating effects on PMESII-PT elements, it creates the conditions for achieving the projected political outcome. This means that a thorough understanding of the hybrid operating environment is critical to the successful application of instruments of power, including the military one. It is essential that the military forces have an analytical tool in place to assess the operational environment to the required and possible extent. Although some authors claim that analytical tools evaluating the operational environment in a symmetric conflict cannot sufficiently analyse the operational environment in an asymmetrical conflict, we dare to argue that they can serve as a starting point for an overall understanding of the operational environment. And it is time that is the factor that will decide to what depth the crew manages to understand such a complex operational

environment.[61] When choosing the appropriate analytical tool, care should be taken of its relative complexity. It should include as much of the overall operational environment as possible in its analysis steps. The chosen analytical methodology has to be able to describe all relevant aspects of the operational environment providing commanders and staff with a comprehensive understanding of it. A comprehensive understanding of the operational environment is necessary for supporting the planning staff activities and for shaping how the commander and staff conceptualise what relevant actors can and will do. The chosen analytical methodology has to be a continuous process consisting of sequential steps that ensures a systematic assessment of all relevant aspects of the operational environment and the relevant actors. In the first step we will describe and evaluate the operational environment, in the second step we will evaluate the actors in it. The analytical task for step one is to develop a geospatially based perspective of the operational environment overlaid with a cyberspace perspective and the information environment. The operational environment consists of four physical domains, a cyber domain and an information environment. Physical domains consist of land, air, maritime and space domains. Domains affect each other, and none of them can exist in isolation. Since the physical aspects of the operational environment are not homogenous, various land and maritime areas may require greater or lesser descriptions depending on the relative geographical complexity of the region. The information environment connects and penetrates through each domain.

The relationships between each domain and the information environment are shown in Figure 1. Each domain consists of physical areas that need to be identified and analysed. Physical areas include a defined operating area consisting of the associated areas of influence and interest that is necessary to conduct operations within the operational environment. Depending on the nature of the mission/operation, the balance of the analytical effort may not be equally distributed between the domains.[62] Description of physical areas within the operational environment considers specific environmental factors. These factors include but are not limited to:

- terrain, topography, hydrology, meteorology, oceanography and space, surface and subsurface environmental conditions (natural or human-made)

[61] NATO 2016.

[62] Department of the Army 2019b.

- distances associated with the deployment and employment of forces, the location of bases and ports, other supporting infrastructure
- METOC and space environmental factors include the entire range of atmospheric (weather) phenomena, from the sub-bottom of the Earth's oceans to the top of the atmosphere and space environment (space weather)[63]

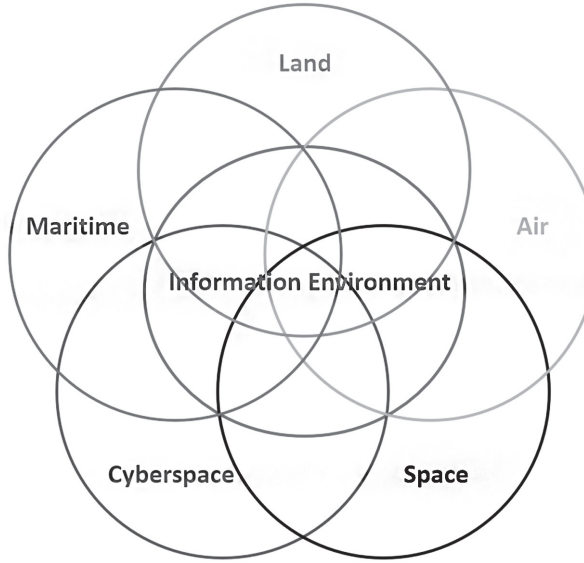

Figure 1: Holistic view of the operational environment
Source: Compiled by the authors

The land domain is the most frequently evaluated domain due to its high population density per square kilometre. Descriptions of the operational environment's land domain are focused on terrain features. Descriptions also include infrastructure aspects of the terrain as well as human and information dimensions.[64] Very important is to always consider the effects of weather as well as changes that may impact operations. It is also important to analyse the combined effects

[63] Department of the Army 2019b.
[64] Skalický–Palasiewicz 2017: 276–280.

of wind, temperature, humidity, sunlight, topography and precipitation, and their impact on a system or network. The results of land domain analysis provide us with the basis for determining which courses of action can best exploit the opportunities the terrain provides and how the terrain affects the actor's available courses of action.[65] The maritime domain is comprised of the world's oceans, seas, bays, estuaries, islands, coastal areas and littorals. In open ocean areas, distant landmasses and supporting shore infrastructure may impact operations primarily due to the range of an actor's systems and sensors. Littoral areas may contain geographic features such as straits or chokepoints that restrict operations. The analyst should be aware of the legal arrangements that apply to the actors in this domain.[66] The aspects of the maritime domain should be evaluated to determine how they impact relevant actors and courses of actions. The evaluation of potential key geography must be based on the degree to which such maritime features control or dominate the operational environment or provide a marked advantage. The locations of naval bases should be evaluated in relation to their ability to support sea control or amphibious operations. During amphibious operations, the evaluations of the maritime and land domains should be combined to identify amphibious landing areas that not only can be supported from the sea, but also connect with advantageous land avenues of approach leading to key terrain objectives.[67] The air domain is the operating medium for fixed-wing and rotary-wing aircraft, air defence systems, unmanned aircraft systems, cruise missiles and ballistic and anti-ballistic missile systems, which only operate in this domain. Aerial avenues of approach are different from maritime and ground avenues. Nevertheless, the air domain is partially influenced by surface characteristics. Additionally, the effects of weather conditions on the air domain are particularly crucial.[68] The space domain is the part of the operational environment for satellites, spaceships, space stations, air defence systems, and ballistic and anti-ballistic missile systems that operate within space. Actors that have access to the space domain are afforded a wide array of options that can be used to leverage and enhance capabilities. Every actor potentially has access to the space domain through the purchase of services.[69] Thus, the monitoring and

[65] Rolenec et al. 2019: 33–40.
[66] Department of the Army 2019b.
[67] Department of the Army 2019b.
[68] Department of the Army 2019b.
[69] Vyklický et al. 2022: 3–20.

tracking of relevant actors' assets is necessary for a complete understanding of the operational environment. Space capabilities have proven to be significant multiplier when integrated into operations. Space capabilities include global communications; positioning, navigation and timing (PNT) services; environmental monitoring; and space-based intelligence, surveillance, and reconnaissance.[70] The importance of the cyber domain is significant today. Most of non-kinetic and kinetic actions too are conducted in the cyber domain. There is a prediction that the core operations of the next warfare generation will be conducted in the cyber domain. This domain consists of all interconnected networks of information technology, including systems and networks, which are separated or independent. The cyber domain encompasses all forms of digital activities. Each of the physical domains mentioned above has specific characteristics in which the cyber domain helps actors apply power or influence the operational environment. Operations in the operational environment are increasingly interwoven with or at times can be dependent on the cyber domain. Cyber as a domain go beyond the Internet and everything connected to it, including standalone and intermittently connected networks and other digital hardware and systems.[71] A description of the information environment is paramount for a thorough understanding of the operational environment. The current state of the information environment, communications means and methods, sources, influencers, cognitive patterns, social-cultural perspectives, historical narrative and many other aspects are intrinsic to the operational environment. Publicly available information can provide insight into many factors affecting the operational environment. It can provide baseline information about public perception and immediate identification of events. The information environment is the aggregate of individuals, organisations and systems that collect, process, disseminate, or act on information and includes the cyber domain. Both friendly and adversary forces are aware of the significance and reach of information-related capabilities to gain an asymmetric advantage in the information environment.[72] The domains make it clear how important it is to identify and evaluate the actors within the operational environment to include their capabilities and limitations, their current situation, centres of gravity, doctrine, patterns of operation, as well as tactics, techniques and procedures. Analysts need to identify all relevant actors within the operational

[70] Department of the Army 2019b.
[71] Department of the Army 2019b.
[72] Department of the Army 2019b.

environment that may positively or negatively impact the accomplishment of the operation. These actors may include, but are not limited to adversary forces, the populace or segments of the populace, government, non-governmental and inter-governmental organisations.[73]

Analytical methodologies applied

Applied analytical methodologies should aid in determining the actor's doctrinal way of operating and observed patterns of operation or potential deviation from observed patterns under similar conditions. Analytical methodologies are normally completed prior to the operation, and are continuously updated during operations. They can be applied independently but can also be combined to provide a more comprehensive and holistic view of the operational environment. Analytical methodologies that could aid in determining and evaluating actors include, but are not limited to human network analysis, centres of gravity analysis and current situation.[74] For human network analysis there are two analytical methodologies that can be used. The first is political, military, economic, social, informational and infrastructural plus physical environment and time (PMESII-PT), the second is area, structures, capabilities, organisations, people and events (ASCOPE). The relevance of PMESII-PT elements and characteristics will depend upon the specific situation associated with each operation. Some of the characteristics that may be considered significant during a sustained humanitarian relief operation may receive far less emphasis during combat operations against a single conventional adversary. Therefore, a tailored approach is imperative for the analyst.[75] The methodology allows for adaptation to the specific operation and situation within the operational environment. Based on the mission analysis, analysts will need to decide on how to best optimise their use of time and intelligence resources. This may involve decisions on what part of the methodology they need to place the most emphasis as well as the application and internal sequencing of the methodology itself. PMESII-PT is used to describe

[73] Skalický–Palasiewicz 2017: 276–280.
[74] Spišák 2016: 136–141.
[75] Skalický–Palasiewicz 2017: 276–280.

the operational environment with eight interconnected elements which are known as operational variables.[76] The PMESII-PT factors include:[77]

- Political – describes the distribution of responsibility and power at all levels of governance including formally constituted authorities as well as informal or cover political powers. Political factor includes advisors, governors, mayors, political interest groups, cabinet officials, courts and policy documents.
- Military – explores the military and paramilitary capabilities of all relevant actors such as enemy, friendly and neutral in a given operational environment. Military factor includes individual leaders at all levels, plans and orders, defence ministry, command and control headquarters, air defence systems, artillery maintenance facilities, ammunition storage points and key terrain.
- Economic – encompasses individual and group behaviour related to producing, distributing and consuming resources. Economic factor includes banks, corporations, trade unions, contracting firms, marketplaces, shipping and distribution facilities, smugglers, automated teller machines, commercial depots, organised crime activities, agriculture and internet-based companies.
- Social – describes the cultural, religious and ethnic makeup within an operational environment and the beliefs, values, customs and behaviours of society members. Social factor includes ethnic groups, clans, social media groups of interest, tribes, religious groups, unions, associations, sports clubs, schools, cultural centres, health and welfare facilities.
- Informational – describes the nature, scope, characteristics and effects of individuals, organisations and systems that collect, process, disseminate or act on information. Informational factor includes plans and orders, newspapers, newsletters, information ministry, television networks, computer networks, information technology centres, intelligence agencies, leaflets, postal facilities, radio stations, national or influential speciality magazines or periodicals, social media applications, and other existing information infrastructure and mass communication capabilities.
- Infrastructural – is composed of the basic facilities, services and installations needed for the functioning of a community or society. Infrastructural

[76] Hrnčiar 2018: 87–92.

[77] Department of the Army 2019b.

factor includes nuclear power plants, hydroelectric dams, gas pipelines, aqueducts, waterways, pumping stations, rail yards, airports, port facilities, relevant factories, hospitals, schools, civil defence shelters, garbage disposal systems, highways, bridges, tunnels, dykes, sewage systems, storm drains, global system for mobile communication masts and server parks.
- Physical environment – includes the geography and manmade structures, as well as the climate and weather in the area of operation. All products and analysis done in the first step could be used.
- Time – describes the timing and duration of activities, events or conditions within an operational environment, as well as how the timing and duration are perceived by various actors.

ASCOPE is an additional analytical methodology consisting of six elements that should be considered when conducting analysis. ASCOPE is typically used in conjunction with the PMESII-PT. ASCOPE is leveraged by the intelligence staff at any level to view the operational environment from the perspective of the populace. ASCOPE places emphasis on the cultural and human parts of the environment. PMESII-PT findings can be augmented with an ASCOPE-directed view of the same data, creating a more accurate and complete understanding of the operational environment. ASCOPE elements are:
- Area – includes districts, market places, picnic areas, irrigation networks, parks, squares, cities and rural areas.
- Structure – includes prisons, police headquarters, banks, churches, courts, roads, cell towers, municipal buildings, supermarkets and tollbooths.
- Capability – includes dispute resolution, recruiting, access, means of justice, maintenance, financing, governance, policing and disaster relief.
- Organisation – includes government organisations, non-governmental organisations, host nation forces, bankers, religious leaders, builders and criminal organisations.
- People – include governors, host nation security forces, bankers, gangs and contractors.
- Event – includes elections, kinetic events, drought, weddings, funerals and festivals.[78]

[78] Department of the Army 2019b.

Combining PMESII-PT and ASCOPE into a PMESII-PT–ASCOPE Matrix helps to get an understanding of the operational environment cantered on human networks. Normally analysts use a PMESII-PT–ASCOPE matrix for the identification and analysis of friendly, adversary, neutral, or other actors. Understanding the changing interactions of these actors with each other and how their relationships and interdependencies change over time helps to understand the operational environment. Based on the data from PMESII-PT–ASCOPE correlation analysis we can conduct human network analysis in order to visualise and describe the interaction between actors and their relationship to other nodes like regions, natural resources, municipalities, equipment and software, that all contribute to a holistic view of the operational environment. A network perspective is based on a node-link analysis. This helps the commander and staff to visualise potential or actual strengths weaknesses, interdependencies key nodes and centres of gravity. This visualisation along with other factors will contribute to the development and analysis of courses of action. To describe and display how each actor interrelates with other actors by using a network perspective helps intelligence analysts to understand the operational environment in a more focused manner.[79] Based on the network analysis we are able to identify the actor's centres of gravity. A centre of gravity is the actor's source of power and is essential for an actor's ability to influence the operational environment. The actor relies on it for resources, recruiting, support, freedom of action and movement, continued willpower and moral justification. If the centre of gravity is under pressure or damaged by another actor, the entire network will be affected. A centre of gravity is always linked to the actor's objective. If, at some point, the actor's objective changes, the centre of gravity does not necessarily change as well. Taking away an actor's access to a centre of gravity or impeding the function of it will always affect the network. However, a resilient actor may be able to revert to a different source of power once the original identified centre of gravity is no longer available or effective.[80] There are a lot of analytical methods used for the centre of gravity analysis like the strategy rings model or fractal analysis process. But the most effective method for analysts to identify an actor's centre of gravity is to use the CG–CC–CR–CV model:

- Centre of gravity (CG) – the source of power that provides moral or physical strength, freedom of action, or will to act.

[79] Department of the Army 2019b.

[80] Spišák 2016: 136–141.

- Critical capability (CC) – a means that is considered a crucial enabler for a centre of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s). It is described by using a verb.
- Critical requirement (CR) – an essential condition, resource and means for a critical capability to be fully operational.
- Critical vulnerability (CV) – an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. It is described by a noun.[81]

A centre of gravity typically will not be a single node in the system, but will consist of a set of nodes and their respective links. However, a single node might be considered a centre of gravity as an exception. For example, when the adversary senior military leader is also the political leader, and the nature of the adversary's political and military systems is such that the leader's demise would cause support for the conflict by other leaders in these systems to collapse. A proper analysis of an actor's critical factors must be based on the best available knowledge of how actors organise, fight, think, make decisions, and on their physical and psychological strengths and weaknesses. Analysts must understand an actor's capabilities and vulnerabilities, and factors that might influence an actor to abandon or change strategic objectives. Analysts must also envision how friendly forces and actions appear from the actor's viewpoint. Otherwise, analysts may ascribe to actors' particular attitudes, values and reactions that mirror their own.[82] The current situation provides an understanding of the present context, including all actors and all PMESII-PT factors of the operational environment. At the operational level, it will consist of several displays and descriptions of all relevant perspectives of each actor, including desired end states, modus operandi, capacities, support and training level and all other relevant elements of the operational environment, to include the impact of politics, social and economic considerations. Intelligence processing (collation, evaluation, analysis, integration, interpretation) is done to extract relevant information to explain the current situation, its dynamic and changes from the historic situation.[83]

[81] Department of the Army 2019b.
[82] Skalický–Palasiewicz 2017: 276–280.
[83] Skalický–Palasiewicz 2017: 276–280.

The analyst will need to consider the following factors in assessing the current situation of the actors:

- composition
- disposition
- capabilities
- tactics, techniques and procedures
- logistics
- combat effectiveness
- command and control systems
- personalities
- potential courses of actions
- other additional information and data

Conclusion

In this chapter we aimed to outline characteristics of the operational environment as a cornerstone for a package of possible military response options applicable in the context of hybrid warfare. Thus the authors firstly presented the frame of the concept into space, actors and methods commonly used. The need to respond to hybrid threats in a hybrid way, ideally proactive and not reactive was emphasised, which was followed by a discussion of the basic pillars of successful responses to hybrid threats. The formulated strategy to respond to hybrid warfare should in all circumstances be nationally apolitical and must be based on defined political goals. The goal of the strategy is to initiate military activities and identify the military outcome state, which is sometimes at odds with democratic politics, which is based on avoiding constraints and seizing opportunities. Politicians try to find ways to keep divergent interests in consensus, which means avoiding long-term and resource-intensive conflicts until absolutely necessary. Therefore, it is essential for military commanders to understand the essence and nature of politics and the interests of the political subjects who are leaders in the conduct of war, even hybrid war. It must be clear that the most fundamental aspect of military strategy in hybrid war is answering the fundamental question of how to effectively use military means to achieve political goals. Other instruments of power should be able to exploit success from all alternatives of conducting military operations and at the same time ensure a quick and decisive conflict resolution based on the use of new knowledge and ideas so that the strategic interests

of the state are achieved. The hybrid operational environment creates military instruments of power dilemma of balancing their combat capabilities with other capabilities. The development of military technologies allows commanders to look for alternative concepts of deployment. This means that while the armed forces must be able to conduct decisive combat operations against adversary armoured forces, on the other hand, they are more likely to be deployed in crowd control as part of peace support or humanitarian operations. Comprehensive preparation of the operational environment is a demanding and very responsible activity. It requires a systematic approach and the use of appropriate analytical methods, procedures and tools. The result of a comprehensive preparation of the operational environment is a set of information about the physical environment in each domain and an explanation of how the physical environment, including the weather, involves conducting any activities. The next result of comprehensive preparation of the operational environment is to identify all actors and their properties, identify the centres of gravity and describe the current situation of each actor. All results of comprehensive preparation of the operational environment will serve commanders to determine the correct military response.

Questions

1. Which are the challenges for the deployment of military forces in a hybrid operational environment?
2. Which domains HOE consist of?
3. What are the definitions and purposes of PMESII-PT and ASCOPE analysis during the Intelligence preparation of the HOE?
4. Which are the most common features of the concept of hybrid warfare?

References

Andrassy, Vladimír (2019): Slovenská republika v operáciách NATO po summite vo Varšave. *Politické vedy,* 22(1), 80–107.

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

Bassford, Christopher (1997): *Policy, Politics, War and Military Strategy.* Online: www.clausewitzstudies.org/readings/Bassford/StrategyDraft/ index.htm

Betts, Richard K. (2002): The Trouble with Strategy: Bridging Policy and Operations. *Joint Force Quarterly,* Autumn–Winter 2002, 23–30.

Bezpečnostná stratégia Slovenskej republiky (2021). Online: www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf

Clausewitz, Carl von (1946): *On War.* Online: www.gutenberg.org/files/1946/1946-h/1946-h.htm

Department of the Army (2019a): *The Operational Environment and the Changing Character of Warfare. TRADOC Pamphlet 525-92.* Online: https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf

Department of the Army (2019b): *Intelligence Preparation of the Battlefield.* Washington, D.C.: Department of the Army. Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31379-ATP_2-01.3-001-WEB-4.pdf

EEAS (2015): *Countering Hybrid Threats.* Online: www.statewatch.org/news/ 2015/may/eeas-csdphybrid-threats-8887-15.pdf

Gressel, Gustav (2020): *Military Lessons from Nagorno-Karabakh: Reason for Europe to Worry.* Online: https://ecfr.eu/article/military-lessons-from-nagorno-karabakh-reason-for-europe-to-worry/

Hoffman, Frank (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

Hrnčiar, Michal (2018): The Counter Insurgency Operating Environment. *International Conference: The Knowledge-Based Organization,* 24(1), 87–92. Online: https://doi.org/10.1515/kbo-2018-0013

IISS (2020): *The Armed Conflict Survey.* London: The International Institute for Strategic Studies.

Jenzen-Jones, N. R. – Lyamin, Yuri: *The Hoplite.* Online: http://armamentresearch.com/type-84-scatterable-anti-tank-mines-in-syria/

Kompan, Jaroslav (2020): War and Politics. In *Security Forum 2020: 13th Annual International Scientific Conference Proceedings.* Banská Bystrica: Univerzita Mateja Bela. 106–113.

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.

Krejčí, Oskar (2011): *Válka.* Praha: Professional Publishing.

Lawrence, Christopher A. (2017): *War by Numbers. Understanding Modern Warfare.* Nebraska: Potomac Books.

Lowther, Adam (2020): Why We Need the W76-2 Low Yield Nuke. *Breaking Defense,* 02 March 2020. Online: https://breakingdefense.com/2020/03/why-we-need-the-w76-2-low-yield-nuke/

Manea, Octavian (2015): Hybrid War as a War on Governance: Interview with Mark Galeotti. *Small Wars Journal,* 18 August 2015. Online: https://csc.asu.edu/2015/08/23/manea-interviews-galeotti-on-hybrid-war-at-swj/

Marek, Ján (2019): *Mierové operácie OSN.* Liptovský Mikuláš: Armed Forces Academy of General Milan Rastislav Štefánik.

Mattis, James N. – Hoffman, Frank (2005): Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine,* 132(11), 18–19. Online: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf

McCuen, John (2008): Hybrid Wars. *Military Review,* March–April 2008, 107–113. Online: https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/ 237

Mušinka, Michal: (2021): Konflikt na Ukrajine a jeho dopad na bezpečnosť EÚ. In *Národná a medzinárodná bezpečnosť 2021.* Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika.

NATO (2016): *Warsaw Summit Communiqué.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. Online: www.nato.int/cps/en/natohq/official_texts_ 133169.htm

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Monterey: Naval Postgraduate School. Online: https://calhoun.nps.edu/handle/10945/5865

Podhorec, Milan (2012): The Reality of Operational Environment in Military Operations. *Journal of Defense Resources Management,* 3(2), 41–50. Online: http://journal.dresmara.ro/issues/volume3_issue2/02_podhorec_vol3_issue2.pdf

Reddaway, William F. (1904): *Frederick the Great and the Rise of Prussia.* New York: G. P. Putnam & Sons.

Rolenec, Ota – Palasiewicz, Tibor – Šilinger, Karel – Žižka, Pavel (2019): Supporting the Decision-Making Process in the Planning and Controlling of Engineer Task Teams to Support Mobility in a Combat Operation. *International Journal of Education and Information Technologies,* 13, 33–40.

Schultz, Teri (2017): NATO in Europe Needs 'Military Schengen' to Rival Russia. *DW,* 09 December 2017. Online: www.dw.com/en/nato-in-europe-needs -military-schengen-to-rival-russian-mobility/a-40470302

Shurkin, Michael (2014): *France's War in Mali. Lessons for an Expeditionary Army.* Santa Monica: RAND. Online: www.rand.org/pubs/research_reports/RR770.html

Skalický, Pavel – Palasiewicz, Tibor (2017): Intelligence Preparation of the Battlefield as a Part of Knowledge Development. *International Conference: The Knowledge-Based Organization,* 23(1), 276–280. Online: https://doi.org/10.1515/kbo-2017-0045

Spilý, Peter (2014): Insight into Contemporary Operational Environment. *Security Dimensions: International and National Studies,* 1(11), 132–140.

Spišák, Ján (2016): Operational Thinking and Its Application in Operational Design. *International Conference: The Knowledge-Based Organization,* 22(1), 136–141. Online: https://doi.org/10.1515/kbo-2016-0025

Tzu, Sun (1910): *The Art of War.* Online: www.gutenberg.org/files/132/132-h/132-h.htm

Van Coppenolle, Hermine – Haesebrouck, Tim – Taghon, Servaas (2022): *The War in Ukraine.* Online: https://biblio.ugent.be/publication/8751754

Vego, Milan (2009): *Joint Operational Warfare. Theory and Practice.* Newport: Naval War College.

Vejmelka, Oto (2005): *Vojenský výkladový slovník vybraných operačních pojmů.* Vyškov: Správa doktrín Ředitelství výcviku a doktrín. Online: www.researchgate.net/profile/Adnan-Dzafic/publication/365437381_security-forum-2020_THE_HETERONOMY_IN_BOSNIA_AND_HERZEGOVINA/links/6374ed712f4bca7fd0667951/security-forum-2020-THE-HETERONOMY-IN-BOSNIA-AND-HERZEGOVINA.pdf#page=108

Vyklický, Vladimir – Procházka, Josef – Pikner, Ivo (2022): Approaches to Modernizing the Land Forces of Selected Countries. *Vojenské rozhledy,* 31(1), 3–20.

Žídek, Rudolf – Cibáková, Silvia (2009): *Bezpečnosť štátu.* Liptovský Mikuláš: AOS.

Romana Oancea – Ilie Gligorea – Aurelian Raţiu
– Isabela Dragomir[1]

Cybersecurity

Nowadays, the Internet is integrated into society both through social interaction and business transactions, so the need for data protection and security has become increasingly important. In addition, not only computers, but also most hardware devices are networked, and regional geographical boundaries are no longer maintained. Communication and/or interaction between different countries is now very easy and the protection of data flow has become a concern for all countries and organisations.[2] The change in paradigm regarding the environment in which everyday activities relate to work, communication, collaboration, and even learning are carried out, has led to an increase in the amount of illicit activity on the Internet. In addition, increased speed, anonymity and national laws that are not always applicable to the Internet have brought about changes in the typology of cyberattacks. To underline the seriousness and danger the society is experiencing today, the concept of cyberspace has been introduced and defined as "the interdependent network of information technology, infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical infrastructure industry".[3]

Cybersecurity fundamentals

In NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), cyberspace "is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks".[4] In other words, cyberspace is "the interdependent network of information technology infrastructures",[5] which makes it the arena for political, economic and

[1] "Nicolae Bălcescu" Land Forces Academy.
[2] SWD 2020.
[3] The White House 2008: 3.
[4] Klimburg 2012: 8.
[5] The White House 2008: 3.

military interaction and some actions in this space can have a negative impact on social stability, national security and economic development. In cyberspace, digitalised data is created, stored and shared by using an infrastructure that allows data flow.[6] This environment is prone to cyberattacks, cybercrime and de-cyber warfare. When discussing cybercrimes, we generally refer to attacks launched by individuals for financial gain, while cyber warfare actors, such as states or governments aim for political advantage, strategic advantage or destabilisation.[7] The purpose of cyberspace actions by one state or group against another focuses on a broad spectrum of threats that can harm a nation's interests. Threats range from espionage to illicit actions directed at critical infrastructure that can destroy, disrupt or destabilise the work of structures vital to society. Cyberattacks have recently increased in intensity and complexity and have a variety of targets. The difference between the terms cybercrime and cyber warfare is delineated by the motivation of the actors involved, the situation and the context in which they operate. Actions in cyberspace, referred to as cyber warfare, are a form of hybrid warfare and aim to weaken the enemy country by compromising its core systems. In addition, these actions are supported by organised groups or states and are generally identified only after significant damage has already been done. Cyberwar incidents are increasing, not only among states, but also among terrorist groups and political or social organisations. The tools and techniques are the same regardless of whether the cyber incident is classified as cybercrime, cyber warfare, cyberterrorism or hacktivism. However, cyber warfare involves more resources and time. The complexity of actions in cyberspace and the negative effects they have in all areas have made cybersecurity a priority on the international agenda. Due to the necessity of digitalisation for all sectors, cyberspace has become the area of choice for the conduct of most of the activities. "Cyberspace is, in all truth, the battlefield on which the war of the future is currently being fought."[8] By utilising this environment, cyber operations will probably play a vital role in hybrid warfare, especially for mass manipulation and intelligence gathering, espionage, sabotage or economic disruption, destroying military resources or organisations, and targeting critical infrastructures that are vital for a developed society. In order to counter or reduce cyberattacks, actors such as the EU, NATO or the USA are focusing their efforts on ensuring

6 Singer–Friedman 2014.
7 Polyakova et al. 2021.
8 Cunningham 2020: 2.

a high level of cybersecurity by improving cyber resilience and incident response capabilities.[9] "If you know the enemy, and know yourself, you need not fear the result of a hundred battles. If you know yourself, but not the enemy, for every victory gained, you will also suffer defeat. If you know neither the enemy nor yourself, you will succumb in every battle."[10] Cybersecurity is a great umbrella term referring to protect the confidentiality, integrity and availability of system, data and information. So, when the data is transmitted through the Internet or when data is saved locally on a device, it needs to be protected. Protected data means maintaining confidentiality, integrity and availability.[11]

Figure 1: The CIA Triad
Source: Cyber One 2019

The CIA (Confidentiality, Integrity, Availability) model describes three important goals of cybersecurity such as confidentiality, integrity and availability:[12]

- Confidentiality – means that the information is not accessible for unauthorised access even if the access is required by devices, processes or people. In other words, confidentiality means keeping data and information secret. The main way confidentiality is accomplished is through encryption. Confidentiality is a complex task which presupposes that information and data need to be protected against unauthorised

[9] European Parliament 2022.
[10] Tzu 1910.
[11] Oriyano–Solomon 2020.
[12] Chai 2021.

access, data is not intercepted by a third party, only authorised people can access data, and that there must be a mechanism that allows the verification of the identity of the entity with access.[13] By way of example, a breach of confidentiality means that someone gains access to information which they should not have access to, regardless of whether the breach is voluntary or involuntary.

- Integrity – refers to the authenticity of information, provided the information is not altered, and the source of information is genuine. It means that data and information in transit, saved or processed has not been altered accidentally or intentionally.
- Availability – means that information, services or resources are accessible to authorised users. Availability can be defined as timely access to genuine data and information for authorised users.

Different tools can be used to ensure the confidentiality, integrity and availability of information. Each tool can be utilised as a part of the information security process. Authentication, authorisation and nonrepudiation are tools which can be used to maintain system security with respect to the CIA triad:[14]

- Authentication – involves proving the user's identity. Authentication can be accomplished by identifying someone through one or more of three factors such as something they know (a password or a private key), something they have (a physical key, a smart card), something they are (face, fingerprint), or something they do (how they walk, how they pronounce a passphrase). For security reasons, combinations of two or more elements of these categories are used (2FA – two factors authentication) in order to prove the user's identity.
- Authorisation – is the step that follows authentication. Authorisation refers to the specific permissions that a particular authenticated user should have, given his/her authenticated identity. Each user or process has associated privileges, so authorisation means establishing privileges. For instance, in case of cyberattacks, the hacker has the target's privileges. If the user used an administration account, the hacker has all the privileges, and they can do everything. In planning authorisation, it is important to follow

[13] Shakarian et al. 2015.
[14] Graham et al. 2011.

the principle of least permissions – each person should have only the permission that she/he needs to do their job.
- Auditing – is collecting information about an individual's activities. Specifically, tracking is similar to Auditing. Every action made by a user is recorded in log file and these files can be analysed.

In sum, authentication proves the user's identity, authorisation assigns permission to individuals, and auditing analyses the user's behaviour and activities.

Types of cyberattacks

The cybersecurity kill chain stages model, derived from the military model of anticipating possible enemy actions in order to neutralise the target, is the basic model used for tracking and preventing cyber intrusions at various stages.[15] In defence strategy, the goal is to understand how the enemy will act and then move on to identify the appropriate technique. The instrumentation of a cyberattack is time-consuming and involves the use of various techniques depending on the vulnerabilities identified in the host systems. Cybersecurity kill chain provides an overall picture of the phases commonly invoked in a cyberattack. In general, a cyberattack, whether it is an illicit action against a person, group, organisation or nation includes the following steps:[16]

- Reconnaissance – it involves passive information gathering without interaction or potential exploratory contact with the victim by using a phishing technique. Public sites such as Facebook, Twitter, LinkedIn or official sites are generally used to collect information regarding a potential victim, in order to identify his/her possible weaknesses.
- Scanning – acquiring more technical detailed information. Most activities are focused on identifying weaknesses in target systems, such as configuration settings. Known vulnerabilities, applications and weaknesses in general depend on the software or hardware components installed on the target device.

[15] Diogenes–Ozkaya 2019.
[16] *ATT & CK Matrix for Enterprise* s. a.; Diogenes–Ozkaya 2019; Oriyano–Solomon 2020.

- Weaponisation – different "weapons" are built in order to attack the victims at different stages. The instruments created for this purpose depend on the vulnerabilities identified after scanning. For instance, an infected file can be created and sent to the victim.
- Infiltration and Privilege Escalation – trying to exploit one or more identified vulnerabilities in order to gain access to a resource and then escalating access privileges. Hardware, software and human factor vulnerabilities are exploited in order to gain access. Of the three types of vulnerabilities, humans are the most vulnerable, so they can be targets of social engineering attacks such as phishing, spear phishing, etc., for gaining access. Often network access can be done through unprivileged access which restricts or makes it impossible to run a malicious code and an account with higher privileges is sought. Privilege escalation can be both vertical and horizontal. For vertical escalation, an attacker needs to perform actions that involve administrative access, so the purpose is to gain admin privileges higher level rights. In horizontal escalation, the attacker uses a normal account to access an account with high privileges. The purpose is not to upgrade the privilege of an account, but to access an account with higher privileges.
- Exfiltration – is the phase where the adversaries apply different techniques to steal data, modify or delete sensitive files, or obtain configuration information. The action depends on the purpose of the attack. Once an attack has reached this phase, it is considered successful. The exfiltration of the data identified in the system can be done either via email, downloaded directly to another device or saved on external drives, or using malware to infect a target and send the data from the victim's computer.
- Access extension – additional exploit can be installed in order to grant permanent access to the system. In general, techniques such as rootkit or similar tools are used to provide easier silent access.
- Assault – the purpose of this stage is to cause damage by removing or modifying critical configuration files or parameters in order to alter the way in which a device operates. This stage is not present in all attacks.
- Obfuscation – is covering the tracks, which is often a very important step especially when the aim is to collect information and return to the system in the long term or when the action is to remain "secret". This is one of the most difficult steps and it requires advanced technical knowledge.

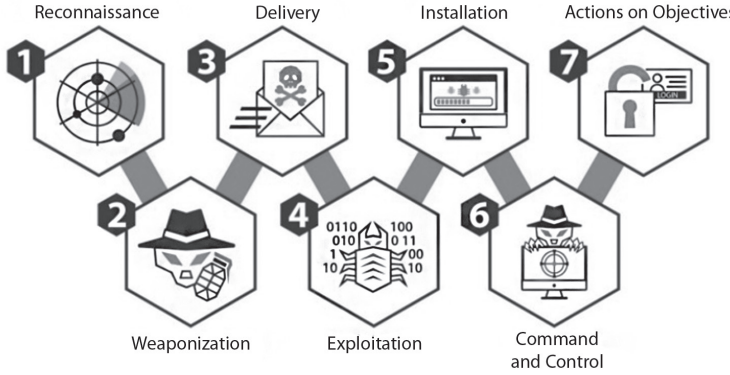

Figure 2: Cybersecurity kill chain stages developed by Lockheed Martin, 2011
Source: ATT & CK Matrix for Enterprise s. a.

A cyberattack and a cyber defence could be conducted at any scale: from the state level by the military to an organisation or even an individual level. The steps to instrument the tactics used in the cybersecurity kill chain also apply to illicit actions initiated by one state against another nation. When referring to nation state threat actors the most common tactics are:[17]

- Propaganda and information propagation – attempting to control people by spreading lies in order to make people lose trust in their country.
- Espionage, reconnaissance and information gathering between countries – monitor other country's communication systems to steal secrets, data or information.
- Sabotage – the competitors can take advantage of information theft in case of research and development, or military, economic or technological data.
- Denial-of-service (DoS) or Distributed DoS attacks – flooding a server with illegitimate requests in order to prevent it from responding to the legitimate ones.
- Malware – can disturb the proper functioning of the critical infrastructure.

The motivation for these types of attacks can be military if the aim is to control key elements of an enemy nation, or civilian if the target is a critical infrastructure with direct impact on society, or hacktivism if the aim is related to ideological

[17] Geers 2008; Fortinet 2022.

promotion. Propaganda used in psychological warfare uses misinformation as a method to create panic among the population or to manipulate their behaviour. The most common medium for propaganda is social media and the internet. Social networks such as Twitter, Facebook, LinkedIn, Instagram, etc. are often used to manipulate public opinion, spread diverse political views and even go "deep behind enemy lines".[18] In the digital society, there are not any totally effective methods of countering propaganda unless the rights to information and free expression are violated. There are states such as Russia, China or North Korea that are trying to secure their national information space by introducing suppression measures targeting social networks and media.[19]

Figure 3: Disinformation and propaganda
Source: Bayer 2019

There are situations when both Russia's and China's internal and external efforts have been effective. Propaganda and disinformation serve multiple purposes and even use political bots to intentionally distribute false information on and through social media.[20] Disinformation campaigns are often used in hybrid attacks and lately there has been an increase in the number of attacks given that the majority of daily activities take place mainly online. The availability of services and resources can be an issue in the case of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. A DoS attack occurs when a legitimate user is

[18] Bayer 2019: 38.
[19] Geers 2008.
[20] Bayer 2019; Woolley 2020: 89–110.

unable to access information, resources, devices or services due to the actions of malicious cyber threat actors that generate synthetical traffic.[21] For instance, due to the DoS attacks, legitimate users have no access to the information displayed on a website, or they cannot use the email service or their online account. DoS are considered effective weapons in cyber warfare. DoS attacks involve flooding the target host or network with illegitimate requests and the target cannot respond to legitimate requests made by legitimate/regular users. A more complex type of DoS attack, using multiple hosts to launch the malware, is the DDoS attack, which has a similar effect – overloading and crashing, or lowering the target's performance intentionally. The essential difference between a DoS and a DDoS attack is that instead of launching an attack from one location, the target is attacked by using multiple connected devices. DDoS attacks typically use botnets. A botnet is a collection of compromised computers often referred to as 'zombies', infected with malware that allows an attacker to control them.[22] The attacker controls and coordinates all the infected hosts in a DDoS. The infected hosts are usually called zombies.

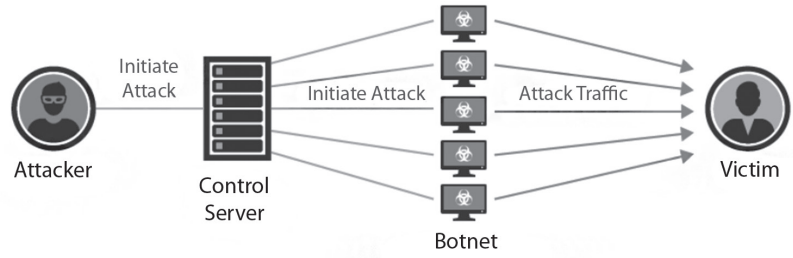

Figure 4: A Distributed Denial-of-Service Attack
Source: Imperva 2017

DDoS attacks are often considered effective weapons due to the technical requirements and low costs, but the effects can be very serious. These attacks are frequently launched by hackers wishing to express their ideological disagreement, or by other groups that intend to limit access to information, to disrupt communication, to paralyse the activity of websites or even of critical

[21] CISA 2021.
[22] Radware s. a.

infrastructure in an "enemy" country.[23] Espionage is a common practice in the military as well as in industry, economics or technology and focuses on:[24]

- stealing state secrets and trade secrets
- intellectual property rights
- sensitive information in strategic fields

Threats to cybersecurity are on an upward trend and, in addition, the complexity and impact of cyberattacks is increasing. Furthermore, as the problems facing society become more complex and diverse, companies are forced to operate predominantly online. It has been observed that cyber espionage has received a boost and new opportunities for cyber criminals have emerged.[25] A cyber sabotage attack can be defined as an illicit action financed or coordinated by a state actor against a country aimed at disrupting communications services, economic activities, military activities or at destroying critical infrastructure. This type of attack may have physical consequences.[26]

Cyberattack case studies

The battle for supremacy is fought in every field, be it military, economic or technological. For instance, Russia is trying to improve its power position across the globe through its cyberspace-funded actions, as demonstrated by its attacks on Estonia, Crimea and Ukraine. Moreover, it is conducting a powerful influence and disinformation campaign using social media. China is concentrating its efforts on stealing intellectual property based on illicit actions in cyberspace to provide economic comfort and/or technological progress. Government organisations in North Korea have made a name for themselves by launching cyberattacks especially on entities that attempt to denigrate their national image.[27] After a successful cyberattack, it is quite difficult to identify how it was orchestrated and especially who the actors directly involved were. Thus, if the attack is not claimed by any state or group, assumptions are made to identify the actors

[23] Radware s. a.
[24] Enisa 2020.
[25] Enisa 2020.
[26] Molina 2022.
[27] Cunningham 2020.

depending on the mode of attack, the geopolitical context and the evidence identified. There are quite a few instances where the U.S. or U.S. governmental organisations have been accused of unlawful actions directed against a state or a nation. Articles in specialised literature point out that cyber warfare started in 2010 with Stuxnet, considered the first cyber weapon to cause physical damage, which was allegedly launched by the U.S. against Iran's nuclear program.[28] After this incident, the series of cyber warfare attacks continued and most of them were instrumented using developed malicious code, such as Trojans, worms, or combinations thereof. Propaganda is an old tactic used in modern warfare by many states. If radio and television were used in the Cold War, nowadays propaganda also employs modern electronic techniques to manipulate or influence people's perceptions. The techniques used in propaganda vary depending on the goal to be achieved, so stealing and revealing private information, hacking different devices, creating and spreading fake news are the most common techniques targeting politicians, influential people or private organisations.[29] Propaganda is considered a type of cyberattack because social media landscape allows misinformation to spread further and possibility to create social network false accounts. In addition, using bots to spread false information, database and device hacking for stealing critical data, recruiting new members into violent and dangerous movements by using social network are specific to cyberattacks approaches. Disinformation and propaganda campaigns have Russia as the main actor. Russia has frequently been suspected of using fake social media accounts for disinformation and propaganda campaigns. Many of the disinformation campaigns by various Russian groups have been aimed at influencing public opinion and undermining the credibility of governments in several countries such as the United Kingdom, the United States and the European Union.[30] The campaigns have been carried out at crucial moments, especially in the run-up to elections, and have used social media as a landscape.[31] After a series of attacks that were instrumented using various social networks and aimed at misinforming and undermining public confidence in national values, Facebook and Twitter started to develop new technologies to reduce propaganda through social networks. Methods of protection against propaganda are primarily concerned

[28] CSIS 2022; Cunningham 2020; Fortinet 2022.
[29] Trend Micro 2017.
[30] CSIS 2020.
[31] Satariano 2019; Stubbs 2020.

with public awareness. People need to be informed about the repercussions that can arise if seemingly harmless information is shared on social media, the common practices used by malicious individuals or groups on social media, and the possibilities for securing information saved on various devices. Even more so, information should only be retrieved from trusted sources. Starting with the Internet era, there have been many cyber incidents politically motivated that were aimed at data and information theft in order to gain technological knowledge or other states' secrets. When these espionage actions are planned and/or supported by the nation, intangible damage often cannot be estimated at first assessment. Some of the most notorious attacks, which have been supported by state actors and which have taken cyber espionage to another dimension are Operation Aurora (2010) and Red October (2012). Operation Aurora was a series of cyberattacks from China that targeted U.S. private companies such as Google, Yahoo, Dow Chemical, etc., and the goal was to steal trade secrets.[32] On January 2010, Google announced that it had been the victim of a cyber espionage attack launched by China and multiple Google email account had been hacked into. After the announcement made by Google, several companies publicly admitted that their systems had also been hacked by the same adversary. The attack was very complex. During the first stage – reconnaissance – company or other official websites were most likely browsed for employee information, focusing especially on email addresses. Then, networks were scanned for hardware and/or software vulnerabilities. During the weaponisation stage, a Trojan (Hydraq Trojan) designed to steal intellectual property was most likely constructed.[33] The Trojan was based on a software vulnerability identified in Microsoft Internet Explorer so that in the first phase all Windows-based systems were affected. It is assumed that the attack was based on a link from a 'trusted' source to a malicious website. Employees, following spear phishing campaigns via email or chat, received a link to a malicious website hosted in Taiwan. By exploiting a vulnerability in the Microsoft Internet Explorer browser, a malicious JavaScript code (Hydraq Trojan) was downloaded locally, where it executed another exploit that had the ability to open a backdoor on a compromised system, enabling the attackers to receive unauthorised access to the

[32] Council on Foreign Relations 2010.
[33] Shakarian et al. 2015.

system.[34] Probably only privilege escalation was required to move from unauthorised access to locating the intellectual properties repository and stealing company secrets. After investigating the attacks, the indicators pointed that Operation Aurora was executed with the full knowledge or even under the directive of the Chinese Government and the attack target.[35] To reduce and minimise the damage in case of espionage attacks, it is recommended that applications be updated regularly, and sensitive information be secured. In addition, employee awareness sessions about spear phishing or email attachments or links can make the difference between failure or success for a hacker. A typical example of espionage is the cyberattack called Red October. Red October was a large cyber incident whose main objective was to gather intelligence from diplomatic, governmental and scientific organisations in different countries. It was discovered in October 2012 by a team from Kaspersky, a Russian company. It is believed that the attack was launched in 2007 or earlier against Eastern European countries, former USSR Republics, countries in Central Asia and others. In the first stage, before launching the attack, the victims were carefully selected and analysed, then after the reconnaissance and scanning stages, the weaponisation stage was carried out. In the weaponisation stage, a malware was built, consisting of distinct modules with various objectives and functions such as to steal encrypted files or to recover and steal deleted files, to recover deleted files from an USB stick, to monitor when a USB stick is plugged in, etc. For the malware to reach the system and infect a target, spear phishing email was used and vulnerabilities in MS Office and Microsoft Excel were exploited. Once a system has been infected, attackers have often used information exfiltrated from the infected target so as to get into other systems. Targets were not only traditional workstations, but also mobile devices because the malware was designed so that it was able to steal information from mobile devices, and the malware was also able to steal information from various configuration equipment such as routers or switches. A detailed analysis of the malware indicated that Russia was behind the espionage attack dubbed Red October.[36]

[34] Enigma Soft 2010.
[35] Shakarian et al. 2015.
[36] Kaspersky Lab 2013.

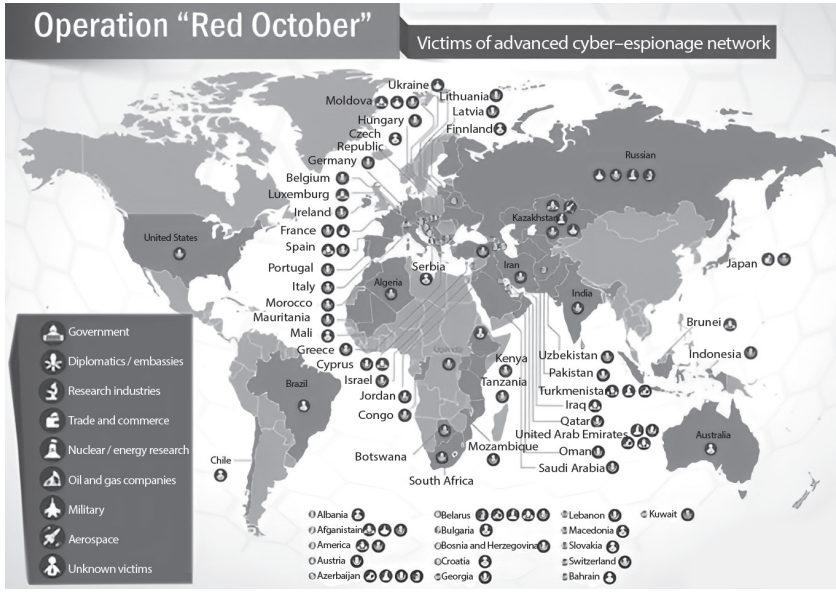

Figure 5: Victims of Red October
Source: Max 2013

These cyber espionage attacks were the first in a series of large-scale attacks, but events have not stopped. Lately, the number of nation states backed cyber espionage attacks targeting the economy are on the rise and this trend is likely to continue.[37] Protection methods, which could reduce or minimise the risk of a cyber espionage attack, primarily involve creating security policies for employees, actions and the organization and training staff on the policies developed. Regular assessment of risks and vulnerabilities to identify possible security breaches and, last but not least, regular updating of installed software.

DoS and DDoS attacks can be weapons in cyber warfare and are intended to disrupt communication channels between government institutions and citizens in order to decrease public confidence, demoralise residents and introduce an element of panic and instability. In addition, they aim to disrupt critical infrastructure such as energy utilities, transportation, hospitals, banks, water supply and so on, and produce panic, chaos and instability. In other words,

[37] ENISA 2020.

DoS attacks prevent legitimate users from accessing services or resources of a website by flooding it with fake requests. Servers are unable to deal with a large number of illegitimate requests and cannot distinguish between a legitimate and an illegitimate request, and, consequently, they become inoperable. These types of attacks disrupt critical operations and block access to website by both military and civilian people.[38] DoS and DDoS attacks are quite common because they are not necessarily costly and there are services that allow DoS attacks to be launched. Moreover, botnet codes can be found on the Dark Web. Among the string of attacks aimed at destabilising lines of communication between government and citizens are:[39]

- The May 2007 attack on the websites of the Estonian government institutions, following the decision by Estonian officials to move the World War II bronze memorial statues.
- The 2008 cyberattack targeting the websites of government institutions in Georgia. The attack took place in the immediate aftermath of the war between Russia and Georgia.

In April 2007, a series of DDoS attacks were launched against Estonian websites following the government's decision to relocate the bronze statue of the Soviet Soldier in the centre of Tallinn. For Russian minorities, the statue represented 'liberation', while for many Estonians it represented Moscow's dominance and oppression; therefore, the relocation led to disputes between the police and the opponents of the government's decision.[40] In addition, the economic relations between the two states were deteriorating, various events were directed at Estonian embassy employees in Moscow and ethnic tensions in Estonia led analysts to assume that Russia was directly involved, but it remained only at the level of supposition because Russia never admitted its direct involvement.[41] Amidst internal and external discontent, between 27 April 2007, and 18 May 2008, Estonia faced a series of DDoS attacks aimed at rendering government websites unavailable and paralyzing various communication networks. The first attacks were carried out from IP addresses outside Estonia, but later attacks were also launched from inside the country. Hackers provided people involved in the

38 Imperva s. a.
39 SUNY 2022.
40 Ottis 2008.
41 Herzog 2011: 49–60.

'movement against Estonia' with clear instructions on how DDoS attacks can be launched, and websites have also been set up for this purpose. All instructions were in Russian and advised people how to attack government websites with ping flood, UDP floods,[42] email spam, etc. which indicated that the Russian Government itself was behind the groups. The peak of the DDoS attacks on Estonia was considered to be 9 May 2007, the day when Russians celebrate 'Victory Day'. On May 19, the attacks suddenly stopped.[43] Typically, DDoS attacks are intended to distract the attention of the victim from the hacker's true motive because, while the victim is focusing on the DDoS attack, other illicit actions, such as collecting sensitive information, may be undertaken. After the attack Estonian officials asked Russia to investigate Russian IPs, but no response to the request was received. Experts from the EU and NATO were brought in to prove the Russian involvement in the attacks on Estonia, but the Kremlin's involvement could not be clearly proven.[44]

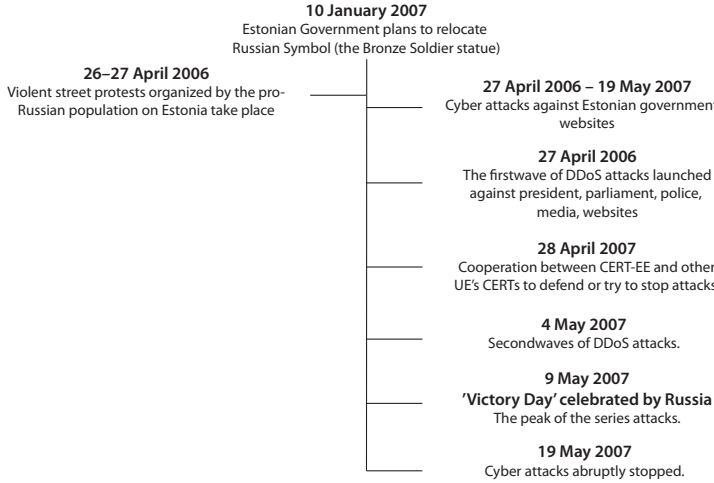

Figure 6: Timeline of the DDoS key element attack on Estonia 2007
Source: 2007 Cyber Attacks on Estonia

[42] Types of DoS or DDoS attacks. The target is overwhelmed with specific illegitimate requests and becomes inaccessible to legitimate requests.

[43] Herzog 2011: 49–60.

[44] Herzog 2011: 49–60.

Following the DDoS attacks against Estonia, NATO and EU member states' agenda included discussions on new cybersecurity guidelines and punishments for nations that engage in digital warfare. In addition, the 2008 Bucharest Summit created the Cyber Defence Management Authority in Brussels (CDMA), tasked to "centralize cyber defense operational capabilities across the Alliance" and established the Cooperative Cyber Defence Centre of Excellence (CoE) in Tallinn, responsible for the "development of long-term NATO cyber defense doctrine and strategy".[45] Furthermore, in May 2008, the Estonian Ministry of Defence implemented the National Cyber Security Strategy.[46] On 8 August 2008, Russia decided to go to war on the side of South Ossetia, in response to Georgia's military actions against the separatist Ossetian regime. Against this background, Georgia detected a series of DDoS cyberattacks against government and media websites. The aim of these cyberattacks was to isolate Georgia from the global community and "silence" important Georgian media organisations. The DDoS cyberattacks against Georgia were carried out in two phases:[47]

- In the first phase, DDoS attacks against government and media websites were reported, that were carried out using botnets. A botnet is a malicious piece of code able to infect other computers and turn them into 'zombies' so that they can be coordinated from a central 'command and control' server.
- During the second phase, the list of victims of DDoS attacks was extended. In addition to government and media victims, the list included financial, business and education institutions. Moreover, public email addresses were used for spam email campaigns and SQL Injection attacks were launched in order to identify as many possible recruits' emails as possible.

During these phases, a number of individuals were recruited and trained to continue to launch DDoS attacks against Georgia. As with the attacks against Estonia, recruits were instructed on how to launch targeted attacks and websites were created containing tools for launching DDoS attacks from private machines. Among the websites accessed by the recruits were StopGeorgia.ru and XAKEp.ru.[48] During the attacks, the websites in Georgia were temporarily unavailable,

[45] Hughes 2009: 2.
[46] *2007 Cyber Attacks on Estonia.*
[47] Kozlowski 2013: 237–245.
[48] Shakarian 2011: 63–68.

which meant that communication in the country was severely disrupted, which also affected the government's link to the outside world. Moreover, fake messages were displayed on the official websites that were still 'working'. The DDoS attacks against Georgia which aimed to "isolate and silence", suggest coordination between ground military operations and cyberattacks, although Russia did not want to be associated with the cyberspace activities. There is a difference in analysis as compared to the Estonian attacks for "the Russian cyber campaign in Georgia in August 2008 represents actions occurring simultaneous with major conventional military operations".[49] No clear evidence was found that the DDoS attacks against Estonia and Georgia were supported by the Russian Government. However, given the context and the relations between the two countries, the support of Russia for the Russian group that 'orchestrated' the attack is not entirely ruled out. In 2017, Russia's military admitted the scale of its information warfare effort, which makes the assumptions about the Russian involvement to become more certain. The 2022 events in Ukraine demonstrated the effectiveness of state-sponsored attacks in launching politically-motivated DDoS against critical infrastructure and government institutions.[50] In 2010, a malicious software worm called Stuxnet disrupted the Iranian nuclear program and the Stuxnet worm was detected in multiple computers in Iran. The main target of the attack was aimed at centrifuges used in the uranium enrichment process at the Natanz nuclear power plant in Iran, and the purpose of the worm was not espionage but sabotaging the production of enriched uranium.[51] At the time, Iran did not officially state the reason why some of the nuclear power plants temporarily stopped production. The biggest problem stems from the way programmable logic controllers (PCLs) that control the automation of physical manufacturing systems were accessed, controls that are also used to automate nuclear centrifuges, located in top-secret locations and not connected to the Internet. The Stuxnet worm was distributed only via infected USB sticks and exploited four 'zero-day' vulnerabilities[52] in the Windows operating system.[53] Moreover, the malware used two valid digital certificates from manufacturers

[49] Shakarian 2011: 68.

[50] Nicholson 2022.

[51] Baezner–Robin 2017.

[52] A weakness of a system discovered and not patched yet. These types of vulnerabilities are often used by cyberattacks and the attacks are called 'zero-days'.

[53] Naraine 2010.

JMicron and Realtek – one of the largest hardware manufacturers.[54] In the Windows operating system, a valid digital certificate is required when installing a driver and digitally signed software is considered 'clean' by antivirus or anti-malware solutions. In addition, using a digital certificate from a trusted manufacturer extends the time in which the virus can be detected. The existence of valid certificates in Stuxnet allowed the installation of the worm in computers when the USB stick was used, and then the search for Siemens Simatic WinCC/Step 7 software, an application used in the control of industrial equipment.[55] Windows vulnerabilities were exploited because programmable controllers are generally programmed from computers not connected to the Internet. If the logic components could be programmed via other operating systems, appropriate vulnerabilities associated with the desired system were certainly used. Although it is not known exactly when the programming of the Stuxnet worm began, there are sources that claim that it had been worked on as a team, for at least two or three years[56] or even as early as 2005,[57] so that after the classic reconnaissance and scanning stages, the weaponisation was completed. It can be assumed that the team members either had advanced knowledge of programming and industrial control systems developed by Siemens – an unlikely assumption – or they documented and identified vulnerabilities, or pieces of code capable of exploiting certain security holes. After identifying vulnerabilities in the Siemens physical equipment, vulnerabilities in the Windows operating system – the system used to connect industrial control systems – were sought. The identification of the four 'zero-day' vulnerabilities certainly led to the next step – the theft of valid digital certificates. For the theft of the certificates, a physical entry was probably performed. Analysing the modus operandi as well as the architecture of the systems that control the centrifuges used in the production of the enhanced uranium, it is likely that the infiltration stage initially used an attack directed at one or more material suppliers and equipment manufacturers, and then followed a waiting period before the Stuxnet worm reached its final target. Based on the modules identified in the worm, sources claim that the attack against Iran's nuclear program was carried out in three stages:[58]

[54] Eset 2010.
[55] Falliere et al. 2011.
[56] Baezner–Robin 2017.
[57] Fruhlinger 2022.
[58] Teixeira et al. 2015: 149–183.

- After entering the system via an infected USB stick, on the machine or network using Windows as operating system, the worm replicates itself.
- It looks for a specific software such as the Siemens Step 7 software, based on Windows, and used for programming industrial control systems (Supervisory Control and Data Acquisition – SCADA) that operate hardware equipment in particular, nuclear centrifuges used to enrich uranium.
- It compromises all programmable logic controls using 'zero-day' vulnerabilities that have not yet been publicly identified and modifies the operating parameters of the centrifuges, resulting in their destruction.

The detection of abnormal behaviour for the sample file received by VirusBlockAda, a Belarusian antivirus company, in June 2006, coincided with the date when the digital certificates expired. A month later, an announcement was made public notifying the company of 'zero-day' vulnerabilities being exploited, and the antivirus community began investigating this highly sophisticated malware. It is only in the closing months of 2010 that Iranian officials admitted that nuclear power plants have been infected with a virus and in November 2010, they completely shut down the Natanz plant without making public the reason. The detection of the Stuxnet cyberattack represented a reason for concern in most countries around the world as the attack was labelled as cyber "terrorism" and is considered to have paved the way for cyber warfare.[59] No state claimed responsibility for the attack, and in addition, no member of the team that worked on Stuxnet has been identified. The effects were both political and social and had a strong economic impact for Iran. Socially, fear and a strong sense of insecurity spread among the population because strategic points, where the level of security was considered to be the highest, were attacked. Although the final target was Iran, many computers around the globe were infected, creating the same sense of global insecurity among the worldwide population. The economic impact was disastrous for Iran, which had to delay its nuclear program and invest in security and cybersecurity measures. After the Stuxnet attack one question needs to be answered, namely: "Will cyber weapons such as Stuxnet proliferate?" Cybersecurity experts believe, however, that there is a possibility that Stuxnet variants will become common.[60]

[59] Kaspersky 2012.

[60] Shakarian et al. 2015: 14.

Defensive approaches of cybersecurity

If we refer to the measures that need to be taken to reduce or minimise risk in the face of cyberattacks or to increase the resilience of organisations or countries to threats in cyberspace, we need to refer to collective measures and then to measures that any organisation needs to consider, especially given that the cyber threat landscape is aggravated by geopolitical tensions. Cyberspace vulnerabilities can be reduced if the following minimum measures are observed:[61]

- increasing the security of information
- implementing data security standards
- increasing the number of specialists in the cybersecurity field
- coordinating actions at national and/or regional level
- developing and continuously updating global and national security strategies

In 2020, the European Union updated its cybersecurity strategy in line with the complexity of the threats posed by the increase of digitalisation and interconnectivity. The new strategy ensures an open global internet and provides safeguards to ensure not only security, but also the protection of European values and fundamental rights. Thus, the new EU cyberstrategy, in response to the complexity of the new cyberattacks, aims to implement three main instruments in three areas of EU action:[62]

"Resilience, technological sovereignty and leadership"[63] – critical infrastructures and services are increasingly interdependent and digitalised, only that infrastructures and services must be secure by design and resilient to cyber incidents, and any vulnerabilities detected must be eliminated. The focus is to build a European Cyber Shield. To this end, Computer Security Incident Response Teams (CSIRTs) and Security Operations Centres (SOCs) constantly monitor and analyse traffic to detect intrusions and anomalies in real time, and SOCs isolate suspicious events using AI and machine learning techniques. The EU proposes to build a network of Security Operations Centres across

[61] Bejtlich 2015: 159–170; Irwin 2021.
[62] European Commission 2020.
[63] European Commission 2020: 12.

the EU and support the improvement of the existing SOC centres. In other words, through collaboration and cooperation, a real cybersecurity shield for the EU can be created. These are just a few ongoing initiatives, but there are also initiatives to attract cybersecurity talent, a reinforced presence on the technology supply chain, an Internet of Secure Things, or an ultra secure communication infrastructure.

"Operational capacity to prevent, deter and respond"[64] – the EU's strategic initiatives aim to establish a Joint Cyber Unit; encourage a Member States' cyber intelligence working group within EU INTCEN; prevent and discourage malicious cyber activities; review the Cyber Defence Policy Framework; offer support for the development of an EU Military Vision and Strategy on Cyberspace as a domain of operations; reinforce cybersecurity of critical space infrastructure under the Space Program.

Cooperation to advance a global and open cyberspace – the "EU should continue to work to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values".[65] Thus, the EU Strategic Survey is about defining a set of objectives in the international standardisation process; promoting international security and stability; providing guidance on the application of human rights and fundamental freedoms in cyberspace; strengthening and promoting the Budapest Convention on Cybercrime; expanding the EU cyber dialogue with other countries and regional organisations; strengthening structured exchanges with private sectors, academia and the civil society.

In order to reduce or minimise the risk of a cyberattack, whether the attackers are individuals, groups or nation states, organisations need to develop their own cybersecurity strategies. A good defence strategy is based on the "defence-in-depth" concept, which involves the application of different techniques, technologies and strategies to protect data and resources.[66]

64 European Commission 2020.
65 European Commission 2020.
66 Krause et al. 2021.

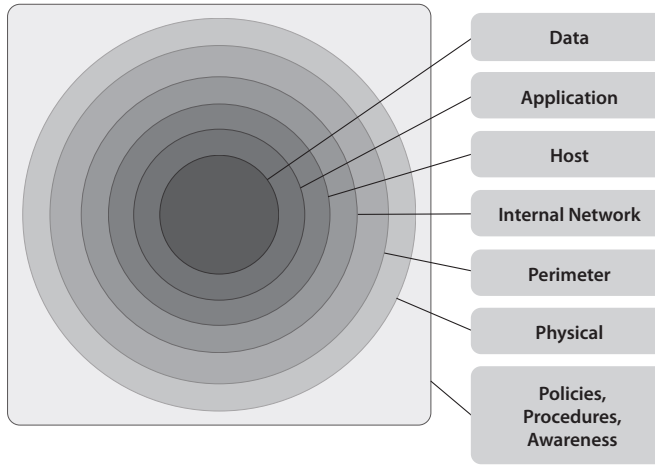

Figure 7: Defence-in-depth strategy
Source: Omoyiola 2019

The defence-in-depth approach, presupposes the existence of a number of defensive mechanisms aimed to protect data and information, especially since there is no single method to protect against any type of attack. Each method and mechanism contributes to reducing the risk of attacks arising from hardware, software and human resource vulnerabilities. Of the three types of vulnerabilities, the most exposed link is people, so developing policies, procedures, and awareness sessions for this factor is an extremely essential measure.[67]

Conclusion

Hybrid warfare is defined as a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare. This chapter pivots on the concept of cyber warfare, perceived as the first stage in hybrid warfare and one of the many unconventional ways in which an asymmetrical

[67] Oancea et al. 2019: 46–50.

fight can be carried out. The chapter starts by defining the fundamentals of cybersecurity, in the framework of the CIA triad, which encapsulates three main concepts such as confidentiality, integrity and availability, and the tools that facilitate their implementation. This section is dedicated to different types of cyberattacks and the stages any cyberattack presupposes – reconnaissance, scanning, weaponisation, infiltration and privilege escalation, exfiltration, access extension, assault, obfuscation. This section also discusses tactics used in cyber warfare and their potential consequences. By way of extended example, the case studies discussed in this chapter offer a comprehensive view to how various types of cyberattacks were conducted and how their tools were utilised so as to produce disruptive effects on organisations, institutions, governments and states. The last part of the chapter focuses on various modalities to counter cybersecurity threats and discusses international organisations' such as the European Union, as well as individual efforts aimed to increase resilience and mitigate the devastating effects of attacks in cyberspace.

Questions

1. Which are the elements of the CIA Triad and what does each of them refer to?
2. What are the generic stages of instrumenting a cyberattack?
3. What are the most common tactics utilised by one nation against another?
4. What are the goals of cyber propaganda attacks and of cyber espionage attacks?
5. What is the objective of a DoS attack?

References

2007 Cyber Attacks on Estonia. Online: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

ATT & CK Matrix for Enterprise (s. a.). Online: https://attack.mitre.org/

Baezner, Marie – Robin, Patrice (2017): *Hotspot Analysis. Stuxnet, Version 1.* Zürich: Center for Security Studies.

Bayer, Judit – Bitiukova, Natalija – Bárd, Petra – Szakács, Judit – Alemanno, Alberto – Uszkiewicz, Erik – Carrera, Sergio – Vosyliute, Lina – Guérin, Julia (2019): *Disinformation and propaganda. Impact on the Functioning of the Rule of Law in the EU and its Member States.* Brussels: Centre for European Policy Studies. Online: www.ceps.eu/ceps-publications/disinformation-and-propaganda-impact-functioning-rule-law-eu-and-its-member-states/

Bejtlich, Richard (2015): Strategic Defence in Cyberspace: Beyond Tools and Tactics. In Geers, Kenneth (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine. Tallin: NATO CCD COE Publications. 159–170.*

Chai, Wesley (2021): *Confidentiality, Integrity and Availability (CIA Triad).* Online: www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

CISA (2019): *Understanding Denial-of-Service Attacks.* Cybersecurity and Infrastructure Security Agency. Online: www.cisa.gov/uscert/ncas/tips/ST04-015

Council on Foreign Relations (2010): *Operation Aurora.* Online: www.cfr.org/cyber-operations/operation-aurora

CSIS (2020): *Countering Russian Disinformation.* Washington, D.C.: Center of Strategic and International Studies. Online: www.csis.org/blogs/post-soviet-post/countering-russian-disinformation

CSIS (2022): *Significant Cyber Incidents Since 2006.* Washington, D.C.: Center of Strategic and International Studies. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/221006_Significant_Cyber_Incidents.pdf?LnVEOhJ.dvbm2FkfowopP0XkTL7Crysq

Cunningham, Chase (2020): *Cyber Warfare. Truth, Tactics, and Strategies.* Birmingham: Packt Publisher.

Cyber One (2019): *What Is the CIA Triad?* Online: https://comtact.co.uk/what-is-the-cia-triad/

Diogenes, Yury – Ozkaya, Erdal (2018): *Cybersecurity – Attack and Defense Strategies.* Birmingham: Packt Publisher.

Enigma Soft (2010): *Hydraq Description.* Online: www.enigmasoftware.com/hydraq-removal/

ENISA (2020): *ENISA Threat Landscape 2020 – Cyber Espionage.* Annual report, 2020. Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Eset (2010): *Why Steal Digital Certificates?* Eset research. Online: www.welivesecurity.com/2010/07/22/why-steal-digital-certificates/

European Commission (2020): *The EU's Cybersecurity Strategy for the Digital Decade.* Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Parliament (2022): *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* Online: eur-lex.europa.eu/eli/dir/2022/2555/oj

Falliere, Nicolas – Murchu, Liam O. – Chien, Eric (2011): *W32.Stuxnet Dossier.* Symantec Security Response. Online: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

Fortinet (2022): *What Is Cyber Warfare?* Online: www.fortinet.com/resources/cyberglossary/cyber-warfare

Fruhlinger, Josh (2022): *Stuxnet Explained: The First Known Cyberweapon.* Online: www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Geers, Kenneth (2008): *Cyberspace and the Changing Nature of Warfare.* Online: https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

Giles, Keir (2015): *Russia's Hybrid Warfare. A Success in Propaganda.* Berlin: Federal Academy for Security Policy. Online: http://www.jstor.org/stable/resrep22215

Graham, James – Howard, Richard – Olson, Ryan eds. (2011): *Cyber Security Essential.* London: CRC Press.

Herzog, Stephen (2011): Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security,* 4(2), 49–60.

Hughes, Rex B. (2009): NATO and Cyber Defence. Mission Accomplished? *Atlantisch Perspectief,* 8. Online: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf

Imperva (2017): *How to Identify a Mirai-Style DDoS Attack.* Online: www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Imperva (s. a.): *Denial-of-service (DoS) Attacks.* Online: www.imperva.com/learn/application-security/cyber-warfare/#examples-of-cyber-warfare-operations

Irwin, Luke (2021): 5 Ways to Improve Your Information Security. *IT Governance,* 11 February 2021. Online: www.itgovernance.co.uk/blog/5-ways-to-improve-your-information-security

Kaspersky, Eugene (2012): *The Flame That Changed the World.* Online: https://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-the-world/

Kaspersky Lab (2013): *Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide.* Online: www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation—red-october—an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide

Klimburg, Alexander ed. (2012): *National Cyber Security Framework Manual.* Tallin: NATO CCD COE Publication.

Kozlowski, Andrzej (2013): Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal,* Special edition (3), 237–245. Online: https://doi.org/10.19044/esj.2014.v10n7p%25p

Krause, Tim – Ernst, Raphael – Klaer, Benedikt – Hacker, Immanuel – Henze, Martin (2021): Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors,* 21(18). Online: https://doi.org/10.3390/s21186225

Kushner, David (2013): The Real Story of Stuxnet. *IEEE Spectrum,* 50(3), 48–53. Online: https://doi.org/10.1109/MSPEC.2013.6471059

Max, Eddy (2013): How the 'Red October' Cyber-Attack Campaign Succeeded Beneath the Radar. *PC Magazine,* 14 January 2013. Online: www.pcmag.com/news/how-the-red-october-cyber-attack-campaignsucceeded-beneath-the-radar

Molina, Jesus (2022): *Real Time Flames: Welcome to the Age of Cyber-sabotage.* Online: https://waterfall-security.com/welcome-to-the-age-of-cyber-sabotage/

Naraine, Ryan (2010): *Stuxnet Attackers Used 4 Windows Zero-Day Exploits.* Online: www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

Nicholson, Paul (2022): *Five Most Famous DDoS Attacks and Then Some.* Online: www.a10networks.com/blog/5-most-famous-ddos-attacks/

Oancea, Romana – Bârsan, Ghiță – Giurgiu, Luminița (2019): Approach on Increasing User Security Awareness. *International Conference: The Knowledge-Based Organization,* 25(3), 46–50. Online: https://doi.org/10.2478/kbo-2019-0116

Omoyiola, Bayo O. (2019): The Hard Reality of Information Security. *IOSR Journal of Computer Engineering,* 21(6), 16–18. Online: https://doi.org/10.9790/0661-2106011618

Oriyano, Sean-Philip – Solomon, Michael G. (2020): *Hacker Techniques, Tools, and Incident Handling.* Burlington: Jones & Bartlett Learning.

Ottis, Rain (2008): *Analysis of the 2007 Cyberattacks against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Polyakova, Alina – Boulègue, Mathieu – Zarembo, Kateryna – Solodkyy, Sergiy – Stoicescu, Kalev – Chatterje-Doody, Precious N. – Jonsson, Oscar (2021): *The Evolution of Russian Hybrid Warfare.* Washington, D.C.: Center for European Policy Analysis (CEPA). Online: https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf

Radware (s. a.): *Botnet Definition: What Is a Botnet and How Does It Work?* Online: www.radware.com/security/ddos-knowledge-center/ddospedia/botnet/

Satariano, Adam (2019): Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds. *The New York Times,* 14 June 2019. Online: www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html

Shakarian, Paolo (2011): The 2008 Russian Cyber Campaign against Georgia. *Military Review,* 91(6), 63–68.

Shakarian, Paolo – Shakarian, Jana – Ruef, Andrew (2015): *Introduction to Cyberwarfare. A Multidisciplinary Approach.* Amsterdam: Elsevier.

Singer, Peter W. – Friedman, Allan (2014): *Cybersecurity and Cyberwar. What Everyone Needs to Know.* Oxford: Oxford University Press.

Stubbs, Jack (2020): Facebook Says Russian Influence Campaign Targeted Left-Wing Voters in U.S. *Reuters,* 02 September 2020. Online: www.reuters.com/article/usa-election-facebook-russia-idUSKBN25S5UC

SUNY (2022): *International Cyber Conflicts.* The State University of New York. Coursera online course. Online: www.coursera.org/learn/cyber-conflicts

SWD (2020): Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation. SWD(2020) 115 final. Online: https://ec.europa.eu/info/sites/default/files/1_en_swd_part1_v6.pdf

Teixeira, André – Kupzog, Friederich – Sandberg, Henrik – Johansson, Karl H. (2015): Cyber-Secure and Resilient Architectures for Industrial Control Systems. In Skopik, Florian – Smith, Paul (eds.): *Smart Grid Security. Innovative Solutions for a Modernized Grid.* Amsterdam: Elsevier. 149–183. Online: https://doi.org/10.1016/B978-0-12-802122-4.00006-7

The White House (2008): The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Online: https://irp.fas.org/offdocs/nspd/nspd-54.pdf

Trend Micro (2017): *Cyber Propaganda 101.* Online: www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cyber-propaganda-101

Tzu, Sun (1910): *The Art of War.* Online: www.gutenberg.org/files/132/132-h/132-h.htm

Woolley, Samuel C. (2020): Bots and Computational Propaganda: Automation for Communication and Control. In Persily, Nathaniel – Tucker, Joshua A. (eds.): *Social Media and Democracy. The State of the Field, Prospects for Reform*. Cambridge: Cambridge University Press. 89–110. Online: https://doi.org/10.1017/9781108890960.006

This page intentionally left blank.

Paul Tudorache – Ghiță Bârsan[1]

Strategies to Counter Hybrid Threats

Hybrid warfare has been defined in many ways from different perspectives, but for the purpose of this chapter a quite useful definition consists in "synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects".[2] Thus, from the beginning it can be estimated that hybrid warfare is a very complex phenomenon and therefore the action to combat is just as complex, hence very difficult. Without a holistic approach that must cover all essential aspects of hybrid warfare, it will be very difficult for actionable structures and dedicated capabilities to ensure a tailored response. On these coordinates, the fundamental issues that coagulate a generic picture of the reaction needed for countering hybrid warfare or countering hybrid threats comprise highlighting specific strategies used to understand what should be done in such challengeable contexts. These strategies, regardless of their national, regional or international nature, are supported by dedicated instruments, measures and capabilities which can be used based on the principle of joint, interagency, intergovernmental and multinational cooperation. On the other hand, a coherent understanding of the countering hybrid warfare or countering hybrid threats framework requires identifying some key implications at strategic level, as well as giving some planning guidance for the operational and tactical planners.

Conceptual models

To raise awareness and understand the actionable possibilities within the manifestation of hybrid threats or hybrid warfare, the authors highlight some of the models of fighting strategies used by different states and the international security community to ensure a tailored response. Consequently, in the framework of hybrid warfare, both attackers and defenders use a wide range of strategies so that they can achieve desired goals. From a defender's view, specialised sources approach countering hybrid threats (CHT) or countering hybrid warfare strategies

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] MCDC 2017: 3.

(CHW) from three different perspectives such as national, regional and international. In this regard, at the international level, one of the most representative models is the one portrayed in Figure 1 which is also adopted by NATO.

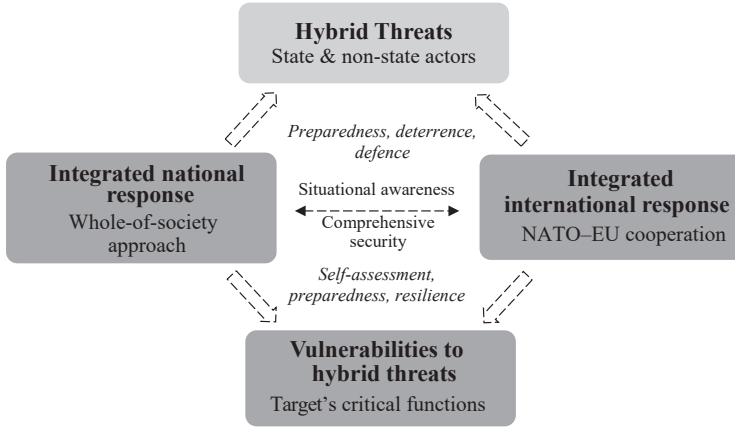

Figure 1: NATO's conceptual model
Source: Hagelstam 2018

To understand the model above it is necessary to think comprehensively which assumes integrating all necessary capabilities involving both national and international commitments. Specifically, the model indicates that a coherent and timely response requires not only strategies developed against aggressors such as preparedness, deterrence and defence, but also strategies for identifying and diminishing national vulnerabilities such as self-assessment, preparation and resilience. Also, if the national response is shaped by the positive involvement of different national authorities and agencies, the international one is tailored by the smooth cooperation between NATO members on the one hand, and between NATO and other national and regional partners such as the EU, on the other hand. Consequently, taking into consideration the conceptual model highlighted, the key strategies used by NATO for CHT/CHW are:[3]

[3] NATO 2022.

- Preparedness – is triggered by the situational awareness using joint intelligence analysis in order to identify the hybrid threat's imprint. It is achieved by developing operational early warning systems, building tailored resilience for national vulnerabilities, educating and training of specialised personnel and structures.
- Deterrence – is focused on determining the adversary to give up his hybrid threat's and hybrid warfare's actions based on the potential consequences such as political isolation, economic sanctions, and so forth; requires not only proper mechanisms for political and military decision-making, but also deployability of tailored capabilities, anywhere and anytime.
- Defence – is manifested by the ability to act/react in a timely and effective manner for CHT/CHW actions. Here decisional flexibility and capabilities' versatility are required.

As has been previously emphasised, currently NATO is working closely with regional institutions such as the EU to improve the synergistic response of CHT/CHW. In order to be able to stress the correlations between these two organisations, Figure 2 highlights the EU's conceptual model which is currently used.

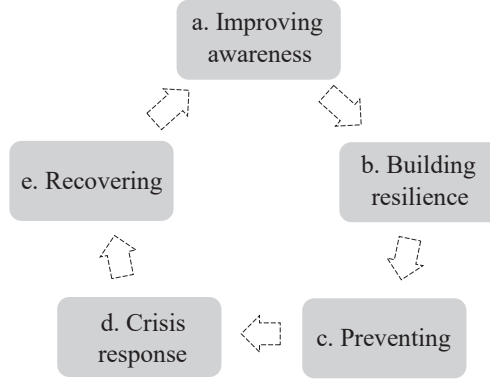

Figure 2: EU strategies
Source: European Commission 2016: 3

As it can be seen in Figure 2, the EU response is based on correlating five dedicated strategies, as follow:[4]

- Improving awareness – is performed by timely exchange of intelligence products between member states in order to recognise the potential hybrid warfare or hybrid threat activities. This strategy is performed by the activity of hybrid Fusion Cell from the Intelligence and Situation Centre, which facilitates the multi-source analyse on the one hand, and on the other hand by the EU Centre of Excellence for Countering Hybrid Threats that conducts specific researches and organises different level exercises.
- Building resilience – is understood as the capacity to resist and recover from hybrid threats or hybrid warfare actions. It is shaped by protecting critical vulnerabilities of energy networks, transport and supply security, space infrastructure, defence capabilities, public health and food security, cybersecurity; moreover, targeting hybrid threat financing, countering radicalisation and extremism or increasing cooperation with partnered countries are other measures taken by the EU to boost its societal resilience.
- Preventing – is done through the capacity of response institutions to pre-empt hybrid threats or hybrid warfare imprints. It ensures early warning of defensive capabilities to be prepared in the event of hybrid attacks.
- Crisis response – is the actual reaction to hybrid aggression provided by the integrated use of national and European capabilities coordinated by the European Emergency Response Coordination Centre.
- Recovering – is comprised of a set of post-incident measures taken to restore the optimal operating parameters of the attacked infrastructure.

Facing the same hybrid challenges, the EU and NATO cooperate closely in different areas such as situational awareness, crisis prevention and crisis response. From this reason it can be said that the strategies belonging to these two organisations are somewhat correlated. Another model of CHT/CHW, that is somewhat similar in terms of specific phases, is the one designed by the Multinational Capability Development Campaign (MCDC) whose framework is highlighted in Figure 3.

[4] European Commission 2016: 4–16.

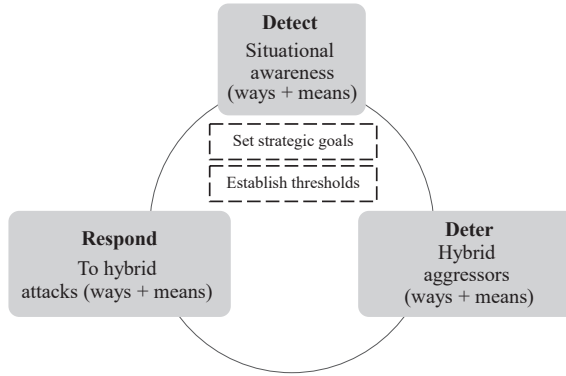

Figure 3: MCDC framework
Source: MCDC 2019: 22

Broadly speaking, the MCDC principles for CHT/CHW to establish the ends called the desired end state in the form of strategic goals based on setting thresholds on the one hand, and on the other hand, to apply specific ways and means within each strategy (detect, deter, respond). More specifically, the constituent elements of the MCDC framework refer to:

- Strategic goals – what is intended to be achieved through countering hybrid threats or hybrid warfare actions (defender's level of ambition). It is settled at the beginning of the hybrid campaign, these are pointed at: independent action capacity, dissuade/deter hybrid attacks and disrupt/prevent hybrid attacks.[5]
- Thresholds – is the hostility level to which countering hybrid threats or hybrid warfare actions must be applied; are correlated with national vulnerabilities and cover political, military, economic, social, infrastructure and information domains as outlined in the previous chapter.[6]
- Detect – is the strategy that focuses on identifying the hybrid threats or attacks through warning intelligence and situational awareness. It can be acquired by monitoring represented by known unknowns or discovery represented by unknown unknowns.[7]

[5] MCDC 2019: 19–20.
[6] MCDC 2019: 90.
[7] MCDC 2019: 26.

- Deter – core strategy for countering hybrid threats or hybrid warfare framework, due to the fact that it is directed at preventing hybrid aggressions; can be achieved through denial deterrence or punishment deterrence.[8] If denial deterrence consists in "[showing] the hostile actor that one can easily absorb the attack with minimal costs to the state that is the target of the hybrid activity",[9] punishment deterrence refers "to threaten to impose costs that are higher than the perceived benefits of aggression, so the hostile actor decides not to pursue the intended action".[10]
- Respond – strategy aiming to calibrate and direct actions using the model of 'ends', 'ways' and 'means' in which coerce/induce, overt/covert, engage/disengage, inward/outward are included.[11]

A more practical perspective regarding the use of the above elements is highlighted in Figure 4 and, as can be seen, the CHT/CHW model is based on 'being in the attacker's mind' principle (in Figure 4, red arrow).

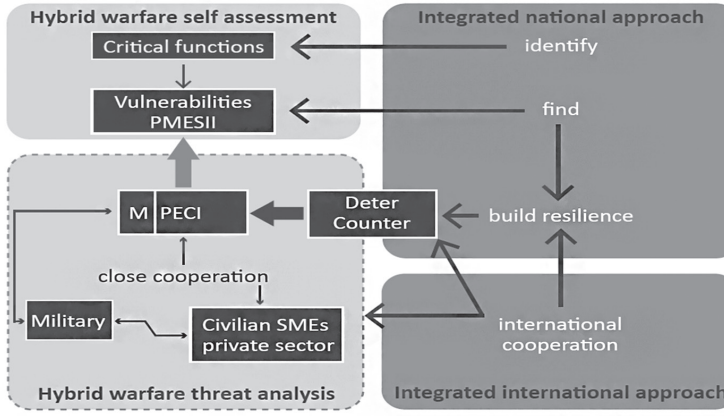

Figure 4: MCDC conceptual model for CHT/CHW
Source: MCDC 2017: 23

[8] MCDC 2019: 35.
[9] Kersanskas 2020: 11.
[10] Kersanskas 2020: 12.
[11] MCDC 2019: 53.

Moreover, the logical algorithm of the MCDC model's applicability starts with conducting a hybrid warfare threat analysis, covering military, political, economic, civilian and informational (MPECI) fields, and continues with hybrid warfare self-assessment for identifying political, military, economic, social, infrastructure (PMESII) vulnerabilities as well as critical functions, these being used to obtain the desired degree of resilience (involves national and international approach). The algorithm is completed by deterring and responding to the aggressor's MPECI using suitable strategies and capabilities.

Concluding at the end of this subchapter, we can appreciate the fact that the strategies described within CHT/CHW models share similarities as well as some differences. Also, the presented strategies are not the only ones, and others can be added, such as cooperation, persuasion, protection, coercion, control (CPPCC), each of these having specific forms as follow:[12]

- Cooperation – entanglement, conciliation, accommodation
- Persuasion – inducement, assurance
- Protection – defence, resilience
- Coercion – compellance, deterrence
- Control – prevention, pre-emption

Instruments and measures

The applicability of the existing CHT/CHW strategies is achieved by coordinating and directing specific instruments, measures and capabilities. Regardless of the hybrid threat or hybrid warfare nature, there is a common sense regarding the principles of using CHT/CHW instruments and capabilities that are equally transposed on the strategic, operational and tactical framework. These principles, also called joint, interagency, intergovernmental, multinational (JIIM), refer to the following:[13]

- Joint – entities belonging to the same agency/ministry
- Interagency – entities belonging to different agencies/ministries
- Intergovernmental – entities belonging to different governments
- Multinational – entities within different nations

[12] Sweijs et al. 2021: 6.
[13] Wide et al. 2011: 4.

In relation to the intensity of hybrid threats or hybrid warfare, these principles can be fully manifested, situation in which the approach becomes JIIM. On the other hand, any other combinations of these principles are quite possible. Also, analysing the applicability of JIIM to each CHT/CHW level such as the tactical, the operational and the strategic, it can be seen that all principles can be used, either independently or in a correlated manner. However, if at the tactical level the 'joint' principle is more widely used, at the operational and strategic levels, the 'interagency' and 'intergovernmental' principles are more suitable. Instead, the 'multinational' imprint can be recognised regardless of the level in question. As for the instruments used for CHT/CHW, they must be correlated with the domains from which the operational capabilities originate. Thus, the literature review identifies the MPECI and diplomatic, information, military, economic, legal (DIMEL) as specific tools or power instruments. The last one, DIMEL can be used in an extended formula, including other domains such as finance and intelligence (DIMEFIL). Within any hybrid operational environment, "when these elements are 'weaponized' the instruments of power can become tools of [response]".[14] For the MCDC model of CHT/CHW as displayed in Figure 4, the MPECI instruments are used to engage vertically and horizontally the aggressor's PMESII vulnerabilities. Thus, the MPECI can be used not only by the attacker, but also by the defender as a response to hybrid threat and hybrid warfare. If vertical escalation is defined by the intensity of the means employed to deter and repel the hybrid aggression, the horizontal one covers the MPECI domains from which the response capabilities will be ensured.[15] In this regard, the defender may correlate both forms of escalations such as vertical and horizontal, which materialises in a synchronised use of the MPECI capabilities whose direction will generate a tailored intensity. As the authors pointed out at the beginning of this subchapter, another effective tool for CHT/CHW identified in the international literature, is DIMEL/DIMEFIL. The principle of its use is somewhat similar to the MPECI tool, because the DIMEL/DIMEFIL instruments are also used for horizontal escalation as seen in Figure 5. Comparing with MPECI, the aspect of differentiation that appears in Figure 4 5 is based on the detailed description of the response intensity in terms of vertical escalation in

[14] MCDC 2019: 90.
[15] MCDC 2017: 9.

the form of different strategies used as displayed by CPPCC. Considering the volatile, uncertain, complex and ambiguous (VUCA) character of the hybrid threat or hybrid warfare, a correlated use of vertical and horizontal escalation is required to ensure the most comprehensive response.[16]

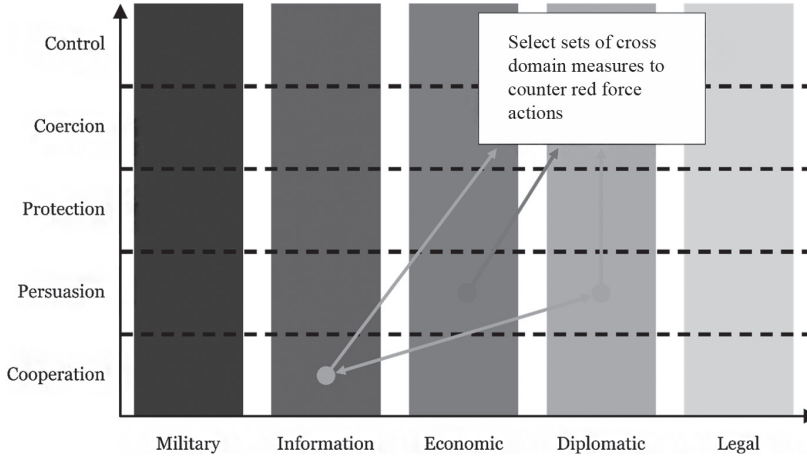

Figure 5: Vertical and horizontal escalation within CHW–DIMEL–CPPCC tool
Source: Sweijs et al. 2021: 7

Another important aspect that needs to be clarified refers to the measures taken for CHT/CHW in relation to power instruments and strategies identified. In this regard, keeping an eye on Figure 5 the authors will focus on identifying specific measures for CPPCC strategies at the level of each domain of DIMEL. Therefore, some measures that can be applied in the CHT/CHW framework are stressed in Table 1 as below. These could be obtained by correlating empirical research based on observation mostly in the form of personal experience with the analysis of specialised sources.

[16] Sweijs et al. 2021: 23–24.

Table 1: CHT/CHW measures – DIMEL and CPPCC tool

Diplomatic		
Cooperation		
Entanglement – building common norms, partnerships, diplomatic channels between public and private sector	*Conciliation* – using neutral parties for mediation	*Accommodation* – empathising with diplomatic issues from different sides
Persuasion		
Inducement – using economic stimulants for diplomatic purposes	*Assurance* – pledging or building peacetime conditions or dissolving wartime organisations	
Protection		
Defence – building or boosting defensive organisations	*Resilience* – using means of public diplomacy to develop national and international diplomatic resilience	
Coercion		
Compellance – threatening with diplomatic isolation to change the subject actor's behaviour	*Deterrence* – threatening with diplomatic isolation to maintain the subject actor's behaviour	
Control		
Pre-emption – expulsion of subject actor's diplomats as well as limiting or prohibiting his access to different international diplomatic organisations	*Prevention* – obtaining the support of various states from the subject actor's neighbourhood and using them to discourage his intention to launch hostile actions	
Information		
Cooperation		
Entanglement – stimulating media activity and identifying journalists from the subject actor's media institutions		
Persuasion		
Inducement – accommodation of the subject actor's propaganda on own territory, provided they will not promote overt misinformation	*Assurance* – ensuring the destruction of sensitive information that discredits the subject actor	
Protection		
Defence – countering various forms of information warfare using media infra-structure and strategic communication	*Resilience* – improving digital literacy and critical thinking to manage the information warfare and implicitly fake news	

Coercion		
Compellance – threatening the subject actor with the use of information warfare's forms to change his strategy; propaganda, misinformation and disclosure of sensitive information may be included	*Deterrence* – threatening the subject actor with information warfare retaliation to discourage changes in his strategy	
Control		
Pre-emption – using information warfare's means to disrupt the subject actor prior to his aggression/attack	*Prevention* – using large scale information operations (fake news, trolls) to discourage the subject actor before direct confrontation	
Military		
Cooperation		
Entanglement – risk sharing regarding the employment of military capabilities	*Conciliation* – promoting arms control activities in order to limit or prohibit the possession and use of dangerous weapons such as Weapons of Mass Destruction (WMD)	*Accommodation* – removing military capabilities from the subject actor's sphere of influence
Persuasion		
Inducement – carrying out arms trade activities to generate behavioural changes of the subject actor	*Assurance* – planning and conducting different military exercises including the subject actor in order to make him aware of own peaceful intent	
Protection		
Defence – developing and revolutionising military defensive capabilities in order to ensure countering the subject actor's attack	*Resilience* – ensuring the operation of military systems and capabilities even when some components are affected or do not function properly	
Coercion		
Compellance – threatening the subject actor with military invasion by prepositioning military forces	*Deterrence* – threatening the subject actor with the use of overwhelming military response capability	
Control		
Pre-emption – launching pre-emptive kinetic or non-kinetic strikes against the subject actor	*Prevention* – launching surgical strikes against the subject actor's high value targets (HVT) in order to diminish his combat power capacity	

Economic		
Cooperation		
Entanglement – increasing mutual economic dependencies	*Conciliation* – facilitating foreign economic competition in the respective markets by reducing or removing various taxes	*Accommodation* – recognising the subject actor as an economic competitor and accepting his presence in one's own economy
Persuasion		
Inducement – accepting the reduction or elimination of debts with the condition of changing current policy	*Assurance* – providing financial and other types of donations to adjust the behaviour of the subject actor	
Protection		
Defence – strengthening energy and supply infrastructure to limit the effects generated by the subject actor's actions	*Resilience* – building various economic connections so that the dependence on singular sources is considerably diminished	
Coercion		
Compellance – threatening the subject actor with the use of economic sanctions to shape his current behaviour	*Deterrence* – threatening the subject actor with the use of economic sanctions to maintain his current behaviour	
Control		
Pre-emption – blocking the subject actor's access to necessary resources for planning and conducting desired attacks	*Prevention* – using large scale economic sanctions to limit/prohibit the development of high-technology weapons systems	
Legal		
Cooperation		
Entanglement – active legal involvement in the various multilateral treaties	*Conciliation* – admitting different perspectives on interpreting the same law to encourage multilateral acceptance	*Accommodation* – expressing agreement related to some deviations from legal provisions
Persuasion		
Inducement – promising to consider the subject actor's opinion when drafting new laws, rules or taking legal decisions	*Assurance* – manifesting leniency towards the subject actor who violates the law to encourage his integration from a legal perspective	
Protection		
Defence – developing legal framework and identifying punitive measures applicable to those who violate the law	*Resilience* – supporting legal framework with new norms to consolidate legal defence	

Coercion	
Compellance – threatening the subject actor with using legal sanctions to determine him to respect the law	*Deterrence* – threatening the subject actor with using legal sanctions to discourage him to break the law
Control	
Pre-emption – withdrawing from different treaties to facilitate national control and autonomy	*Prevention* – prohibiting the manufacture of certain weapons systems

Source: Sweijs et al. 2021: 27–41

These measures are only a few and, as can be seen, they are generic in fashion with applicability, particularly, at the strategic level of CHT/CHW. Regardless of the level, the measures will be applied in a correlated manner, assuming the active participation of different structures, entities and capabilities within each DIMEL domain. If at the strategic level, the degree of capabilities' correlation is greatly amplified, at lower levels such as operational and tactical it decreases significantly, but it is still present.

Strategic level implications

Certainly, a comprehensive understanding of the CHT/CHW also requires deciphering the strategic picture as well as its implications for the operational and tactical levels. In this regard, from the beginning, it is necessary to emphasise the connection between these levels, which can be summarised in the fact that the strategic level should answer the question of How. This level is the one that establishes the methods of response to hybrid threats or hybrid warfare by integrating different strategies and instruments, while the operational and tactical levels are the ones that ensure the application of strategic decisions by accomplishing different missions and tasks using organic capabilities. Therefore, the implications of the strategic level can be reflected on setting the specific goals and thresholds, as well as on selecting the strategies to be used in the CHT/CHW actions. According to the MCDC framework as depicted in Figure 3, all measures and actions should be carried out in such a way as to contribute to the achievement of the following strategic goals:[17]

[17] MCDC 2019: 19–20.

- Preserving the capacity for independent action – refers to maintaining the actionable capacity of all state entities involved in the CHT/CHW effort; being a prerequisite of other additional goals, it largely depends on building and developing resilience in all spheres of society.
- Dissuading/deterring the opponent's aggression – can be reflected in the form of a response with a significantly amplified level of countering, because it means more than denial deterrence, seeking to obtain punishment deterrence if the situation calls for it.
- Disrupting/preventing the opponent from a follow up aggression – is the most complex and demanding due to the fact that it aims to degrade/disrupt the opponent's combat capabilities.

Depending on the footprint and evolution of the hybrid aggression's dynamics, one or more of the highlighted strategic goals can be pursued even within the same operational context. Selecting the appropriate thresholds is another aspect which must be analysed in order to understand the strategic picture of the CHT/CHW. This operation calls for reporting to established strategic goals because "thresholds must be set according to what level of hostility can be reasonably tolerated and what level requires countering"[18] on the one hand, and "hybrid aggressors purposefully target their adversaries by operating below known or perceived response thresholds to avoid decisive retaliation"[19] on the other hand. Consequently, thresholds are indispensable for determining the amplitude of the hybrid aggression and for directing decision-makers when they need to take specific measures in the hybrid warfare framework. Regarding the last aspect of this subchapter, the strategies that can be used for CHT/CHW have been highlighted in the presentation of the conceptual models in the first subchapter. However, some additional information can be related to the selection of the strategies and in this regard, respecting the progressive principle, as appropriate strategies are selected in relation to the identified strategic goals and established thresholds. On the other hand, returning to the influence of the strategic level on the other levels that bring their input to the CHT/CHW, as we have seen, the strategic level is the one at which the desired end state is defined in the form of strategic goals, responsive thresholds and selection/correlation of the strategies necessary for counteraction. Instead, the operational level of CHT/CHW, based on the strategic inputs, is responsible for planning,

[18] MCDC 2019: 21.
[19] MCDC 2019: 22.

coordinating and conducting the actual operations so that multi-domain combat power is directed to the decisive place and time. At the same time, it provides the bridge between the strategic and tactical level of CHT/CHW. The lowest level, such as the tactical level, ensures the implementation of organic capabilities relative to the intent of the operational level, so that, regardless of the hybrid aggression nature, it is combated.

Guidance for operational and tactical planners

At the operational and tactical level, one of the most important activities in managing hybrid threat or hybrid warfare challenges consists in performing tailored planning whose applicability ensures timely and effective countermeasures. For multi-echelon commanders, such as operational and tactical, the operational art and operations design are the most demanding challenges, including the performing of the military decision-making process (MDMP) in all its steps, which constitutes a real obstacle for tactical staff, which can only be overcome by means of detailed adaptive planning. The latter, properly correlated with the commander's conceptual planning, can ensure the achievement of desired end state. Understood as the "cognitive approach by commanders and staff – supported by their skill, knowledge, experience, creativity, and judgment – to develop strategies, campaigns, and operations to organize and employ [capabilities] by integrating ends, ways, and means",[20] the operational art has specific elements including "end state and conditions, [COG], decisive points, lines of operations and lines of effort, tempo, phasing, culmination, operational reach, basing and risk".[21] Also, its applicability is supported by the operations design that focuses on "understanding the situation and the problem".[22] Interpolating their elements, it is found that the centre of gravity (COG) represents an essential ingredient of both, which, addressed in the context of hybrid warfare offers the most significant mutations, of course, by comparing with its determination in the framework of traditional warfare. Considering critical vulnerabilities, requirements and capabilities, the comparative analysis of determining the COG for hybrid warfare and traditional warfare highlights that in the context of traditional warfare the

[20] Department of the Army 2019a: xii.
[21] Department of the Army 2019b: 2–6.
[22] Department of the Army 2019a: xii.

COG bears the imprint of a single source, usually correlated with elements of military combat power, unlike the hybrid warfare framework, where a multitude of power's sources can be identified, which, generally, are not related only to the elements of military power as seen in Figure 6.

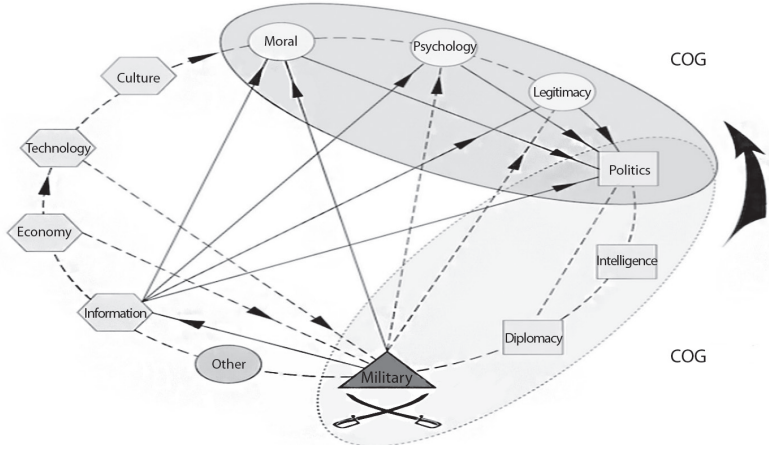

Figure 6: COG in the framework of hybrid warfare
Source: Schmid 2020: 570–579

Moreover, in the hybrid warfare framework, both attacker and defender may use multiple, correlated and shifting COGs that will be flexible, adaptable and dynamic in fashion during a multi-domain confrontation. Besides these, other aspects which commanders and their staff should take into account when planning the operations design may consist in:[23]

- Establishing the ends, ways and means in such a way that they do not follow the overwhelming of the opponent but rather generate a series of interconnected effects, even of the second and third order, which are primarily intended to control the aggressor's behaviour through lethal and nonlethal actions.
- Developing a common operational picture (COP) based on a multi-domain understanding of all significant aspects covering not only the actual subject audiences (sensitivities, perceptions, etc.), but also the different types

[23] MCDC 2020: 42–47.

of interconnections that can be established between them; determining the COGs for all interest audiences should be required.
- Defining the conditions of desired end state so that to be accepted by all interest audiences regardless of their initial perceptions; restoring the critical infrastructure and living facilities should be included.
- Engaging targeted COGs using an indirect approach built on correlating, synchronising and directing the power instruments (MPECI) against targets vulnerabilities (PMESII); the indirect approach should be used to deter and undermine the attacker's hybrid aggression.
- Synchronising the power instruments for each line of operation of CHT/CHW framework; in turn, the lines of operations must be synchronised with each other.

As the authors pointed out earlier, the challenges of countering the various forms of hybrid threat and hybrid warfare can also be encountered at the tactical level, stemming largely from detailed planning. In this sense, during the MDMP, which is a planning methodology used "to understand the situation and mission; develop, analyse, and compare courses of action [COA]; decide on the [COA] that best accomplishes the mission; and produce an order for execution",[24] planners have to adjust each dedicated step according to the hybrid threat or hybrid warfare characteristics and demands. Within each step, these adjustments are given by the following aspects:[25]

- Step 1 (receipt of mission) – by using the two forms of tactical planning, the mission can be received from higher level directly through an operations order (OPORD) in which the planning is subsequent, or through a warning order (WARNO), in which the planning becomes parallel in fashion. Regardless of the planning form, hierarchical documents must provide critical information about the hybrid adversary, including the power instruments such as MPECI, potential strategies, dynamics of relationships with other audiences which are present in the designated area of operations (AO). Also, the higher joint intelligence preparation of the operational environment (JIPOE) should include information on adversary's vulnerabilities, key enablers and different ways/means used within the estimated strategies that can be employed; moreover, to generate an

[24] Department of the Army 2019b: 2–6.
[25] MCDC 2020: 48–61.

effective COP, which is an essential requirement of understanding the hybrid situation, the establishment and use of liaison officers or liaison teams is recommended to facilitate JIIM cooperation.

- Step 2 (mission analysis) – if the first step was to focus on understanding the generic picture of the hybrid operation, this step allows for a more detailed understanding of the situation, as well as the identification of the tactical problem to be solved. In this regard, using JIPOE products and performing the intelligence preparation of the battlefield (IPB), the S2 staff evaluates the adversary and other target audiences, determines their COGs and COAs, and identifies the priority information requirements (PIR). Speaking about the audiences' assessment, including the adversary, determining their motivations, estimating their strength and will to fight, as well as the modalities regarding the use of MPECI instruments, will contribute to visualising the strengths and weaknesses of the hybrid adversary. At the same time, S3 staff must define the key factors of the hybrid operation, determine the friendly forces' COG, develop assumptions, determine the key operational requirements, identify the constraints of the operational freedom of action, develop the initial operations design and so forth. Although each of these requirements has specific features, the S3 staff should pay special attention to the operations design, as it must include multi-domain non-military means.
- Step 3 (COA development) – COA development for friendly forces must start from the premise of being aware of the possibility of continuous change in the COAs of the adversary and of other target audiences, considering the accentuated VUCA characteristics of the hybrid AO. Therefore, friendly forces' COAs must be developed in such a way as to provide a high degree of flexibility necessary to counter any changes that may occur in the hybrid AO, in general, and with regard to adversary's COAs, in particular. Also, this can be supported by a quite flexible operations design and commander's intent, as well as by a high adjustable decisive, shaping and sustaining operations.
- Step 4 (COA analysis) – using the principle of action–reaction–counteraction, this step is performed to examine each friendly forces' COA in order to identify specific advantages and disadvantages. As the authors highlighted, the hybrid footprint of the operation calls for developing the

COAs for all interest audiences that are present in the designated AO and, on these considerations, during war-gaming, not only the friendly forces and adversary's COAs, but also those of the other interest audiences should be simulated. Even if the operational picture increases significantly in its complexity, the advantage of simulating all COAs provide the possibility of estimating the likely effects of other operational audiences on friendly and adversary's COAs.

- Step 5 (COA comparison) – with the aim of identifying the COA with the highest probability of success, this step does not make many adjustments from the perspective of the hybrid operation. Even so, planners must use, in addition to the established comparison criteria (combat functions), and others such as those related to the influence of the indigenous population or the contribution of various civilian agencies, etc. Also, even COAs that have achieved lower probability of success may represent solutions in adjusting the execution to the requirements of the hybrid adversary.
- Step 6 (COA approval) – given the hybrid nature of the operation, the commander's decision should be based on the approval of that COA which enjoys the most conclusive support of friendly forces by multi-domain means, which is due to the fact that combating the hybrid adversary requires the employment of the most diversified capabilities.
- Step 7 (orders production) – once the COA was selected and the concept of operations (CONOPS) approved, planners move on with OPORD's production. It must comprise all critical information that will guide organic and subordinate capabilities to perform CHT/CHW tasks without constraining their freedom of action. On the other hand, the OPORD must give necessary information for all actionable capabilities to protect their critical vulnerabilities.

These are just a few of the many recommendations that planners should consider when dealing with planning operations for countering hybrid adversaries. At the same time, they not only imprint the methodologies specific to operational planning or characteristic of tactical structures with organic headquarters, but are also perpetuated at the level of troop leading procedures (TLP), constituting the planning methodology of the smallest tactical structures such as platoon and company.

Conclusion

Countering hybrid threat or hybrid warfare is the reaction of defenders to hybrid aggression or hybrid attack using multiple strategies, supported by tailored instruments, measures and capabilities, correlated and directed based on the applicability of JIIM principles. The purpose of this chapter is to provide a generic picture that is suitable for national, regional and international defenders. Subchapter *Conceptual models* provides, comparatively, the main conceptual models of countering hybrid threat or hybrid warfare, as well as the strategies underlying them. The main conceptual models analysed in the subchapter are those developed by NATO, EU and MCDC. The NATO model promotes key strategies such as preparedness, deterrence and defence, the EU model strategies consisting in improving awareness, building resilience, preventing, crisis response and recovering, while the MCDC boils down to strategies as detect, deter, respond. Other strategies that may be used in countering hybrid threat or hybrid warfare framework are CPPCC. Subchapter *Instruments and measures* highlights the main instruments and measures that underlie the applicability of countering hybrid threat or hybrid warfare strategies. Within it are explained not only the principles of using MPECI and DIMEL/DIMEFIL instruments in the hybrid framework, but also the main measures specific to DIMEL and CPPCC tool. Subchapter *Strategic level implications* portrays the key implications at the strategic level by setting strategic goals and specific thresholds, as well as selecting/correlating the strategies necessary for counteraction. Moreover, this subchapter defines the relationship between strategic, operational and tactical levels of countering hybrid threat or hybrid warfare. Subchapter *Guidance for operational and tactical planners* provides useful guidance for operational and tactical planners from the perspective of planning a countering hybrid operation. During it, aspects that reflect on the operational art and operations design (COG), as well as on the MDMP are highlighted.

Questions

1. Explain the conceptual models of CHT/CHW used by NATO and MCDC, highlighting the role of constituent strategies and specific elements!

2. What are the main instruments used in CHT/CHW framework to support specific strategies? Identify some CHT/CHW measures using DIMEL and CPPCC tool!
3. What are the main strategic implications in the CHT/CHW framework?
4. Exemplify some measures to facilitate the adaptation of planners to the requirements of the hybrid operation from the perspective of operations design and MDMP!

References

Department of the Army (2019a): *Joint Publication 3-0. Joint Operations.* Online: https://irp.fas.org/doddir/dod/jp3_0.pdf

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

European Commission (2016): *Joint Framework on Countering Hybrid Threats. A European Union Response.* Joint Communication to the European Parliament and the Council. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Hagelstam, Axel (2018): *Cooperating to Counter Hybrid Threats.* Online: www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Kersanskas, Vytautas (2020): *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats.* Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

MCDC (2017): *Understanding Hybrid Warfare.* Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

MCDC (2019): *Countering Hybrid Warfare Project: Countering Hybrid Warfare.* 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

MCDC (2020): *Countering Hybrid Warfare 3: Guidance for Planners.* Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1037061/MCDC_Countereing_Hybrid_Warfare.pdf

NATO (2022): *NATO's Response to Hybrid Threats.* Online: www.nato.int/cps/en/natohq/topics_156338.htm

Schmid, Johann (2020): The Archetype of Hybrid Warfare. Hybrid Warfare vs. Military-Centric Warfare. *Österreichische Militärische Zeitschrift,* 212(5), 570–579.

Sweijs, Tim – Zilincik, Samuel – Bekkers, Frank – Meessen, Rick (2021): *A Framework for Cross-Domain Strategies Against Hybrid Threats.* The Hague: HCSS Security. Online: https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

Wide, Markel M. – Leonard, Henry A. – Lynch, Charlotte – Panis, Christina – Schirmer, Peter – Sims, Carra S. (2011): *Developing U.S. Army Officers' Capabilities for Joint, Interagency, Intergovernmental and Multinational Environments.* Santa Monica: Rand. Online: www.rand.org/pubs/monographs/MG990.html

Vojtech Jurčák – Ján Mišik[1]

Risk Analysis

After the end of the bipolar world, the security environment is increasingly complicated, characterised by instability and uneven development, as well as high dynamics. The instability and uneven development of the security environment is caused by insufficient solutions to the world's global problems. The complexity of the security environment creates problems in characterising the current security actors, which are not only traditional states as the main security actors but also non-state actors, possessing weapons that in the past were owned only by superpowers. During the Cold War we knew the intentions of individual actors but did not know their potential or secret facts, but currently the opposite is true. We know the available capacities, but we do not know the intentions of the actors acting in a given security environment with unconventional means for unconventional goals and using asymmetric strategies to achieve their goals. The possibilities of destabilising the state, affecting the population, or destroying an element of critical infrastructure are no longer a matter of using strategic nuclear carriers, large-scale operations, but include laptops, computer networks, smuggled chemical, biological, radioactive substances, targeted propaganda, organised crime, etc.

Different definitions

There are several different definitions of a hybrid threat. An important sign when a threat becomes a hybrid is its use in combination with another type of threat to achieve a synergistic effect together and achieve one common goal. If a state or non-state actor wants to act on another actor and achieve its goals, it chooses the means and forms of hybrid warfare from its available resources and deploys them against its adversary. This adversary perceives deployed resources or resources that may be deployed in the future as threats to its security. If these resources are a combination of conventional forces, non-conventional forces, terrorist activities, criminal activities and various combinations of political, economic, social

[1] Armed Forces Academy of General Milan Rastislav Štefánik.

and informational activities and tools, then they become a hybrid threat. In this sense, the deployment of regular conventional military force is also a hybrid threat. It is enough if it cooperates, for example, with the means of information warfare. It follows that any security threat in the classical sense can become a hybrid threat.[2] The terms threat and risk are used interchangeably in practice. In general, we use the terms security threats and risks to express undesirable phenomena of a natural and social nature that can potentially damage protected values. These words are very similar and their content is the subject of debate in professional circles. For the purposes of this topic, the relationship between them can be expressed by the term complementary approach. The essence of this approach is the use of risk to express the acuteness of the threat.[3] This approach emphasises the relationship between risk and uncertainty. The European Union (EU), which considers the issue of hybrid threats a challenge for the current security in Europe, in its document "Common Framework for Combating Hybrid Threats" provides one of the most comprehensive definitions of hybrid threats. The EU defines the objective of the hybrid threat as follows: "The aim is not only to cause direct losses and exploit weak points, but also to destabilize society and provoke uncertainty that is intended to paralyze decision-making processes."[4] Security actors encounter various external and internal factors and influences that create uncertainty as to whether and when they will achieve their goals. The negative effect that this uncertainty has on the intentions (goals) of the actor – reference object represents a security risk.[5] The risk arises because these intentions will be monitored in the light of uncertainties. Uncertainty or lack of it is a state of, even if partial, lack of information that relates to understanding or knowledge about an event, its consequences or possibilities. This condition leads to inadequate or incomplete knowledge or understanding of the event, its consequences or probability. Therefore, it is necessary to reduce uncertainty as much as possible. Actors can set their intentions or goals, but to achieve them they often have to struggle with internal and external factors that they may not influence and that create uncertainty and thus risk. These factors can prevent or delay their achievement. Security risks, whose assessment process

2 Jurčák et al. 2017.
3 Laml 2008.
4 European Commission 2016: 14.
5 ISO 31000.

(identification, analysis and evaluation) is the subject of this topic, result from a certain danger called a hybrid threat. Risk management represents coordinated activities to manage and control the actor with regard to risk. It contributes to the understanding of the possible disadvantages of all factors that affect the actor and helps in decision-making by taking into account the uncertainty and possibilities of future events or circumstances (planned or unplanned) and their consequences for the chosen goals. A well-executed identification, analysis and assessment of security risks will make it possible to find appropriate ways to deal with permissible and unacceptable risks, which need to be modified and monitored in a certain way so that they do not cause serious negative consequences. Considering the nature of the sources of security risk consisting in a hybrid threat, it is necessary to assess each risk first individually and then in mutual contexts to determine priorities and consider a possible domino effect.[6] Sources of risk in individual areas of the security sector can be derived from the means used to conduct hybrid warfare as follows:[7]

- military
- political
- economic
- financial
- cybernetic
- propaganda
- diplomatic
- media
- symmetric
- terrorist
- etc.

The first part of the chapter focuses on the characteristics of the stages of risk assessment, including the methods that can be used. The second part is dedicated to the possibility of using modern computer technologies in the process of risk management.

6 ISO 31000.
7 ISO 31000.

Risk assessment

Risk assessment is a part of risk management that provides a structured process for identifying how the security actor's objectives may be affected and for analysing risks in terms of consequences and likelihood before deciding whether further risk management is necessary. When assessing risks, the following fundamental questions must be answered:[8]

- What can happen and why (using risk identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequences of the risk or that reduce the likelihood of the risk?
- Is the level of risk permissible or acceptable and does not require further treatment?

There are several different risk assessment methodologies that can be used for individual risks arising from hybrid threats, e.g.:[9]

- RAM (Risk Assessment Methodology)
- RVA (Risk and Vulnerability Analysis)
- RAMCAP (Risk Analysis and Management for Critical Asset Protection)
- VAM (Vulnerability Assessment Methodology)
- Risk Assessment FEMA (Federal Emergency Management Agency)
- etc.

Management systems built on the basis of Annex SL (e.g. ISO 27000, ISO 14000, ISO 9000) refer to the ISO 31000 standard at the planning stage, which provides universal principles, structure and guidance for risk management. If, for example, we will deal with information security risks – the attack vector, so the ISO 31000 standard – will allow us to work with risks in other areas as well. The risk assessment according to this standard is given as follows. According to ISO 31000 risk assessment is an aggregate process:[10]

- Risk identification – a process used to find, examine and describe risks that could affect the achievement of goals (objectives).

[8] ISO 31000.
[9] ISO 31000.
[10] ISO 31000.

- Risk analysis – a process that is used to understand the nature, sources and causes of risks to determine and assess the level of risk, it is also used to investigate their impacts and consequences and survey the established risk management measures.
- Risk assessment – a process used to compare the results of risk analysis with risk criteria and decide on risks that require treatment.

The process of risk management must begin by defining what we want to achieve – the required level of security (protection), and to understand the external and internal factors that can affect success in achieving the goals. This step, called "contextualisation", necessarily precedes risk identification. In addition to the analysis of the external and internal security environment, the contextualisation stage also includes the definition of risk criteria.[11]

Risk identification

Risk identification means the process of finding, recognising and describing the risk. Risk identification includes finding out:[12]

- Sources of risk – elements that by themselves or in combination have the internal potential to cause risk and the areas of their consequences. This includes events that risk sources can cause and circumstances that could have potential consequences for security.
- Causes of risk – answer the questions of what can happen, when and where, why and how it can happen.
- Potential consequences – include measures introduced to modify the risk.

The aim of risk identification is to create a comprehensive list of risks, based on events that could prevent, invalidate or delay the achievement of objectives to achieve, ensure, support and build security at the required level. The purpose of risk identification is to find out what could happen or what situations could occur that could affect the achievement of security objectives. As soon as the risk is identified, the actor should identify possible suitable measures for its modification, such as mechanical restraints, closed-circuit televisions (CCTV),

[11] ISO 31000.
[12] ISO 31000.

regime measures, physical protection and others. These measures are listed in the risk list. Exhaustive identification must be critical because risks not identified at this stage will not be included in further analysis. Subsequently, these risks cannot and will not be modified or otherwise influenced. The actor should use risk identification tools and techniques that correspond to his capabilities as well as the occurring risks. People with appropriate knowledge and experience should be involved in the identification of risks. Current and relevant information is important in risk identification, and if possible, should include appropriate feedback information. Risk identification can use:[13]

- historical data
- theoretical analyses
- opinions of informed persons and experts
- needs of interested participants

The identification of sources of risk or source identification means the process of finding, recording and describing the elements that alone or in combination have the intrinsic potential to cause risk and the areas of their consequences. If the source or problem is known, the events that may be raised by the source or events can be resolved. Methods (techniques) of risk identification. The following groups of techniques (methods) can be used to identify risks:[14]

- Deductive methods (ex-post methods) or evidence-based methods – are based on the analysis of events that have already occurred, the search for and clarification of their causes and connections between them. The last event is considered and the circumstances that could have caused it are sought. They can be used to create scenarios for the emergence and manifestation of various risks, they are a source of innovation in safety management processes.
- Inductive methods (ex-ante methods) – they allow predicting possible risks for protected assets, while analysing sources that could cause negative events. Using these methods, it is possible to evaluate the expected (expected, probable) number of events, estimate their possible consequences and take appropriate preventive measures. Inductive methods generally use:

[13] STN EN 31010.
[14] STN EN 31010.

- Systematic team approaches or expert assessments – where a team of experts follows a systematic process to identify risks using a structured set of challenges or questions.
- Inductive reasoning techniques – possible future expected events that can negatively affect the actor's intentions are analysed. They help to evaluate the probability of occurrence of events and their consequences, probability models are usually used that work with risk as a purely probabilistic quantity. This approach is based on the fact that the given phenomenon occurs with a certain probability, which can be determined on the basis of certain statistical variables (e.g. the number of occurrences of a given group of phenomena, the length of the monitored period, etc.). Since there can be a significant number of factors to be monitored, the process is often complicated and is only possible with the use of computer technology.

The output of the risk identification process is a verbal description of the risks in the list of risks that the actor undertakes. This is sometimes called the Risk Register, the Risk Catalogue, or the Checklist Risks. The risk description is an organised notation of the risk, which usually contains the elements shown in Figure 1.

List of risks			
Sources	**Events**	**Causes**	**Consequences**

Figure 1: The elements of the List of Risks
Source: Compiled by the authors

Risk analysis

Risk analysis refers to the development and understanding of risk. It is a process that involves understanding the nature of the risk and determining its level. It provides input into risk assessment and decisions about whether risks need to be modified and which modification strategies and methods are most appropriate. It can also provide input into decision-making where choices have to be made and the options contain different types and levels of risk. The risk analysis includes considerations of:[15]

[15] STN EN 31010.

- causes and sources of risk
- negative consequences of the event such as harm or damage
- the probability that these consequences may occur
- factors that affect the consequences and their probability, which can be an event that has multiple consequences and can affect different goals, or existing risk modification measures (risk management elements) that should be taken into account

The risk is analysed by determining:[16]

- consequences of the event
- probability of occurrence of the event
- other risk characteristics

The consequences and their probabilities are then combined to determine the level of risk. Risk analysis can be carried out with different levels of detail and depending on the risk itself, the purpose of the analysis, information, data and available resources. Analysis can be:[17]

- qualitative
- semi-quantitative
- quantitative, or
- depending on the circumstances, their combination

Qualitative methods use expert estimates, which are a direct expression of the occurrence of a risk event, determination of its size or significance, usually not directly supported by a formalised calculation. An expert estimate can be based on an intuitive assessment of the risk as a whole, i.e. without analysis of its individual quantities and assumptions, or a careful consideration of the qualitative importance of these quantities (risk parameters) and risk estimation as a quantity derived from these parameters. Expert estimates are mainly used in cases where numerical values (data) for quantitative risk assessment are missing or difficult to express, they are simpler and faster, but more subjective. Qualitative analysis is mainly used as an initial overview leading to the identification of risks that require more detailed investigation, where this type of analysis is sufficient for decision-making, or where numerical data or resources are insufficient to

[16] STN EN 31010.
[17] STN EN 31010.

perform a quantitative analysis.[18] It is advantageous to use qualitative inductive expert methods especially when solving risk analysis tasks in the field of physical security and facility security, because the conditions and prerequisites for the emergence of risks are very variable, the quantitative expression of risk parameters is very difficult due to the diversity of conditions and the significant influence of the human factor, qualitative methods do not require a lot of statistical data, but use logical links between factors influencing the emergence of risk, qualitative methods provide a clear and comprehensible description of risks and their parameters. Qualitative methods for risk analysis mainly use expert techniques: matrix of consequences and probabilities and the structure "What happens if?".[19] A verbal description is used to establish the level of importance, e.g. high, medium and low levels, but multiple levels can be used. A verbal description is more understandable and intuitively acceptable for most users. This procedure is relatively clear and simple, but there is a considerable degree of subjectivity in it, which uses subjective probability to describe individual events, expressing the degree of personal belief about the occurrence of the phenomenon (event) under consideration depending on the defined factors. Some authors assume that information obtained from qualitative analysis is almost always more valuable than from quantitative analysis, and then quantitative analysis is not always necessary. They recommend a qualitative analysis especially for the development of the initial risk assessment, which can later be refined with a quantitative analysis.[20] In semi-quantitative methods, numerical classification scales are used for consequence and probability and are combined to determine the level of risk using a formula. Scales can be:

- Linear – uniform division of the measurement range into a selected number of equal intervals with an abstract numerical value (0–X), or with a percentage value (0–100%).
- Logarithmic – the scale is the logarithm of a certain quantity, the increase of any value on the logarithmic scale by a fixed constant corresponds to the multiplication of the relevant quantity by a certain factor.
- Or they can express another relationship – the formulas used to determine the level of risk may also vary.

[18] STN EN 31010.
[19] STN EN 31010.
[20] STN EN 31010.

The goal is to create scales that are more detailed than qualitative analysis can usually provide. Numerical values replace the verbal expression of the size. In the numerical classification scale, it is possible to create more intervals or degrees than in the qualitative assessment. However, the goal is not to suggest realistic values for describing risks, as quantitative analysis attempts to do. Because of the numerical value assigned to each property may not represent an exact ratio to the actual magnitude of consequences or probability, these values should only appear in formulas that respect the constraints of established scales.[21] The semi-quantitative risk assessment procedure mainly uses the point method, in which numerical point values are assigned in the scales of probability and consequences, which are evaluated by a matrix. There are various formulas for determining the level of magnitude of a risk, but the most widely accepted formula for quantifying risk is:

$$R = P \times C$$

where R stands for the size of risk, P for the probability of event occurrence and C for the consequence of the event.[22] Special attention must be paid to the use of semi-quantitative analysis, because the numbers chosen may not correctly describe the reality, which may lead to inconsistencies or to unusual or incorrect results. Semi-quantitative analysis may not properly distinguish between risks, especially when the consequences or probabilities of events are extraordinary. In quantitative analyses, practical values for consequences and their probabilities are estimated and risk level values are determined in specific units, determined in the course of creating contexts. Full quantitative analysis may not always be possible or desirable due to lack of information about the system or activity being analysed, lack of data, influence of human factors, etc., or when quantitative analysis efforts are not warranted or required. Under these circumstances, a comparative semi-quantitative or qualitative risk classification, performed by experienced professionals in the relevant field, can still be effective. Even if a full quantitative analysis is performed, it can only be recognised that the calculated risk levels are also only estimates. It should be ensured that the level of accuracy and precision attributed to them is incompatible with the accuracy of the data and methods used. Quantitative methods use the numerical assessment

[21] STN EN 31010.

[22] Belan–Mišík 2016.

of risks by expressing their probability, frequency, credibility, potential, consequences, etc. These methods can be used primarily in cases where there is enough relevant data that can be evaluated statistically. They are mainly used in the field of information systems (they also include the vulnerability of the object). They mainly use statistical analysis (statistical characteristics of the degree of variability – variance, standard deviation, coefficient of variation), or simulation procedures (e.g. Monte Carlo, Markov analysis, Bayesian analysis). In some cases, a single numerical value is not enough to determine the consequences in different times, places or situations. The analysis should also consider and describe the uncertainty and variability of the consequences and their probability. These methods are more exact than qualitative, their implementation requires more time and effort, in some cases they can also be less clear, but they also provide a financial expression of risks, which is more advantageous for their management. To support the performance of quantitative risk analysis, special tools can be used in the form of software programs in which the methodology and system of risk analysis are already incorporated, especially CRAMM (CCTA Risk Analysis and Management Method), in the versions CRAMM expert, CRAMM express and BS 7799 (ISO 27001) Review. Also known are Decision Tools, Callio Secura 17799, COBRA, Counter Measures, EAR/PILAR, Ebios, Proteus and others.[23] The following methods are mainly used for risk analysis: HAZOP, Scenario Analysis, Root Cause Analysis, Event Tree Analysis, Cause–Effect Relationship Analysis, LOPA, Bow Tie Type Analysis, FN Curves, Risk Indices, Matrix of Consequences and Probabilities, CBA, MCDA, etc.[24]

Risk evaluation

The purpose of risk evaluation is to help in making decisions about risks requiring treatment and the priority of risks for the introduction of treatment. The risk evaluation includes:[25]

- comparison of the size of the risk detected in the analysis process, with the risk criteria determined during the creation of contexts
- consideration of the need for risk management

[23] Belan–Mišík 2016.
[24] STN EN 31010.
[25] ISO 31000.

- issuing a decision on risks that require treatment
- determining the priorities of these risks for the implementation of treatment

Decisions about risks that require treatment are based on the outputs of the risk analysis. The evaluation of risks is therefore intended to decide on the seriousness of risks for the actor, whether to accept a particular risk or to modify it with one of the ways of dealing with the risk. Risks are sorted according to their level of magnitude in categories such as acceptable, permissible or unacceptable, to determine whether it is worthwhile to modify the risk. Decisions should take into account the wider framework of risk and in some cases the risk assessment may lead to a decision to perform further analysis, or maintain the existing measures for managing it and not deal with the risk in any other way. Ethical, legal, financial and other issues, including risk perception, are used as inputs for decisions. Decisions should be taken in accordance with the requirements of laws, regulations and other requirements. The following aspects can lead to decisions:[26]

- whether the risk needs treatment
- priorities for treatment
- whether any activity is to be undertaken
- which of the many paths to take

The nature of the decisions that need to be made and the criteria that will be used to make those decisions have been decided during contextualisation, but at this stage, when more is known about the specific risks, more detail needs to be reassessed. Initial assumptions and results should be documented. The easiest way to define risk is a single level that divides risks into risks that:

- Require treatment – these include unacceptable risks and tolerable risks for which costs and benefits are assessed.
- Do not need it – acceptable level of risk.

This division gives temptingly simple results, but neither reflect the uncertainties included in risk assessment, nor define the boundary between risks that need treatment and those that do not. The decision about whether and how to deal with a risk can depend on costs and benefits, especially for tolerable risks when

[26] Belan–Mišík 2016.

taking a risk, or on the introduction of improved risk modification measures. A common way is to divide risks into three groups:[27]

- the upper group, where the level of risk is considered unacceptable, regardless of whether the activity can mean any benefit, and handling the risk is necessary at any cost
- middle group (or grey area), where both costs and benefits are taken into account, and opportunities are weighed against potential consequences
- the lower group, where the level of risk is considered negligible or so small that no measures to deal with the risk are necessary

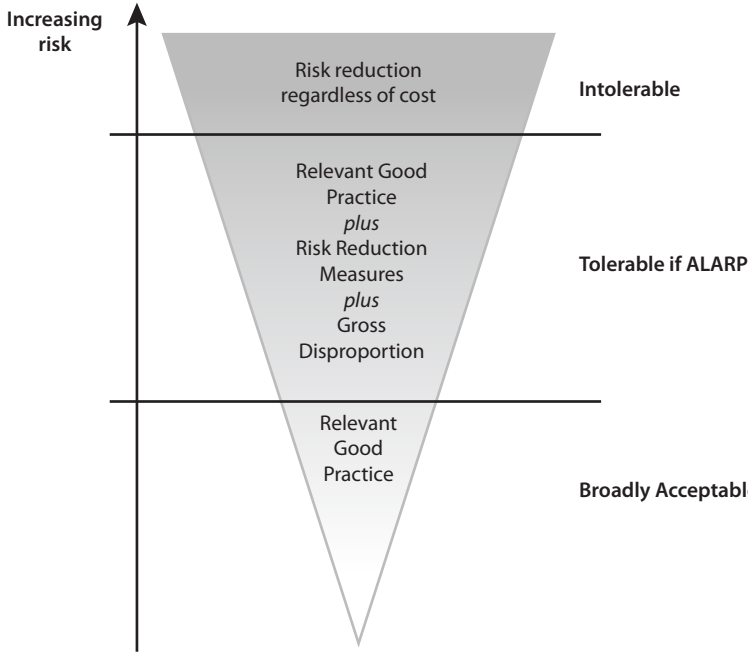

Figure 2: The ALARP principle
Source: www.shorturl.at/noPY6

[27] Belan–Mišík 2016.

To assess the costs and benefits of selected ways of dealing with unacceptable and tolerable risks, the ALARP principle ("as low as reasonably practicable") is used, which shows that appropriate attention should be paid to risk, risk management and risk modification. The principle involves weighing and comparing the level of risk with the difficulty, time and financial costs required to manage it. The ALARP principle is shown in Figure 2.

ALARP mainly addresses the middle group, where there is a sliding scale for tolerable low risks, for which costs and benefits can be directly compared, while for undesirable high risks, the possibility of damage must be reduced, unless the expenditure for further reduction is significantly disproportionate to the safety benefit obtained.[28] The result of the risk assessment should also be the compilation of the order of priority of the risks that require treatment. The ranking assigns a rating to each risk and thus sets priorities for dealing with risks. Risks requiring treatment will not always be able to be adjusted immediately, for a number of reasons, e.g.:

- time requirement
- material – technical difficulty
- financial difficulty
- high demands on human resources
- strategic intentions of the actor, etc.

The stated reasons also influence the priorities of the risks for the implementation of the chosen methods of dealing with them. The goal is to sort the assessed risks according to their significance or priority by using the selected criteria and procedures. It is the decision-making process that uses selected criteria to prioritise risks that require some treatment. The output of the risk assessment is a list of risks that require treatment according to treatment priorities. Based on the determined priorities, the order of risks is determined for the choice of method/methods of dealing with them.[29]

[28] Belan–Mišík 2016.
[29] Belan–Mišík 2016.

Table 1: The risk assessment content

Risk assessment		
Risk identification	**Risk analysis**	**Risk evaluation**
The process of finding, recognising and describing the risk	A process for understanding the nature, sources and causes of risks to assess the level of risk	The process of comparing the results of the risk analysis with the risk criteria
It includes an identification	It includes an assessment	It includes an evaluation
– **sources** of risk – elements that by themselves or in combination have the internal potential to cause risk and the areas of their consequences – **events** that risk sources can cause – **circumstances** that could have potential consequences for achieving goals – **causes of risk** – *what* can happen, *when* and *where, why* and *how* it can happen – potential **consequences** – **measures** introduced to modify the risk	– **causes and sources** of risk – danger (threat) – **negative consequences** of the event – loss – the **probability** that these consequences may occur – **other characteristics** of the risk – factors that influence consequences and probability	– **comparison** of the level of risk from the analysis process, with the risk criteria determined during the search for connections – **consideration of the need for risk treatment** – issuing a **decision on risks that require treatment** and determining their priorities for treatment
List of risks	List of **hazardous events** – documented sources of risk and factors that affect consequences and probability **Level of risks**	**Deciding on risks that require treatment and prioritising them for modification**

Source: Compiled by the authors

Conclusion

Hybrid threats have their own characteristics, therefore assessing the risks, the source of which is at the heart of a hybrid threat is a difficult process. These are relatively new, serious risks that significantly affect the safety of people, property and the environment. A security actor existing in an uncertain, ever-changing

environment must have the ability to adapt or change in order to achieve a certain consistency of his own activity, his own goals with environmental conditions that change and which can be a source of instability with all its effects on individual factors broader and immediate external environment. Risk management is therefore one of the most important issues facing actors today. It is an important part of any strategic management. There are several procedures, in this work we focused on the ISO 31000 process.

Questions

1. Define risk and security risk, and list possible sources of risk.
2. State the content of the risk assessment, and describe the principles of risk identification.
3. Characterise risk identification methods, and risk analysis methods.

References

Belan, Ľubomír – Mišík, Ján (2016): *Manažérstvo bezpečnostného rizika* [Security Risk Management]. Žilina: Žilinská univerzita.

European Commission (2016): *Common Framework for Combating Hybrid Threats.* Joint Communication to the European Parliament and the Council. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

Hofreiter, Ladislav (2015): *Manažment ochrany objektov.* Žilina: Žilinská univerzita.

IEC 31010:2019: Risk Management – Risk Assessment Techniques.

ISO 31000:2018: Risk Management – Guidelines.

ISO/TR 31004:2013: Risk Management – Guidance for the Implementation of ISO 31000.

IWA 31:2020: Risk Management – Guidelines on Using ISO 31000 in Management Systems.

Jurčák, Vojtech – Kredatus, Ondrej – Ivančík, Radoslav – Ganoczy, Štefan – Pikner, Ivo – Jurčák, Ján – Sasarák, Jakub (2017): *Identifikácia príznakov vedenia hybridnej vojny* [Identifying the Signs of Hybrid Warfare]. Záverečná správa oriešení vedeckého projektu VV-A1 [Final Report of Research Project VV-A1]. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

Laml, Roman (2008): *Vzťah pojmov hrozba a riziko (II).* Online: http://mepoforum.sk/bezpecnost/terminologia/vztah-pojmov-hrozba-a-riziko-ii-roman-laml/

About the Authors

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. is 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.

Nicola Cristadoro – is an officer in the Italian Army. He holds a degree in Political Science from the University of Milan, a degree in Strategic Sciences from the University of Turin and a degree in International and Diplomatic Sciences from the University of Trieste. For many years he worked in the field of Military Intelligence and Security, deepening his studies on the doctrine and organisation of the Russian Armed Forces. He is also an expert on Information Operations and PsyOps. He has published numerous articles in "Rivista Militare", "Rivista Italiana Difesa" (RID), "Analisi Difesa", "Difesa Online", "Nuova Antologia Militare", "Limes".

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 a Director of the Centre for the Study of New Security Challenges.

Isabela Dragomir – is an Assistant Professor at the "Nicolae Bălcescu" Land Forces Academy of Sibiu, she teaches general and military English at graduate and post-graduate level. She obtained a PhD in Philology (with focus on Linguistics) in 2019. Her fields of research include, but are not limited to Linguistics, EFL, ESP, adult learning, E-learning, gender mainstreaming. She also acts as a language expert in several international and national projects and grants, and has coordinated public diplomacy and educational projects under the aegis of NATO PDD.

Ilie Gligorea – is a System Engineer and Assistant Professor at the Department of Technical Sciences of the Faculty of Military Management of the "Nicolae Bălcescu" Land Forces Academy of Sibiu. He is a graduate engineer with a degree in Computer Science. He is currently doing his PhD in Systems Engineering. He has been involved in various national and international projects and as an IT specialist has developed/implemented e-learning platforms, web applications and other software applications in programming languages such as Python, Java, PHP.

Eado Hecht – is a Military Analyst focusing mainly on the relationship between military theories, military doctrines and actual practice. He is Senior Researcher at the Begin-Sadat Center for Strategic Studies and teaches courses on military theory and military history at Bar-Ilan University, Haifa University and Reichman University and in a variety of courses in the Israel Defense Forces. He has published more than ten books and text books and more than 50 articles and has been the scientific editor of six books.

Vojtech Jurčák – is a retired Colonel of the Slovakian Air Force who works at the Armed Forces Academy (AFA) of general Milan Rastislav Štefánik in Liptovský Mikuláš, 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 text books. 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.

Boglárka Koller – is Jean Monnet Chair, Full Professor, Head of the Department of European Studies and Vice-Rector for International Affairs at the Ludovika University of Public Service, Budapest. She graduated at the Corvinus University, Budapest as an economist in 1998; she also holds an MA in Nationalism Studies from the Central European University (CEU), Budapest and an MSc in European Studies from the London School of Economics and Political Science (LSE). Her main research areas are history and theories of European integration, differentiated integration and multi-speed Europe, Europeanisation in Central and Eastern Europe. She has numerous publications on European integration.

Jaroslav Kompan – is recently assigned as Assistant Professor at the Department of Military tactics and operational art of the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš. His field of research is mainly focused on military engineering, operational art, operational employment of land forces, national and international security. NATO DEEP SME on tactical and operational level planning and officer's education enhancement for Ukraine, Iraq and Georgia.

Attila Marján – is an Associate Professor with habilitation at LUPS with a research area covering the changes of the geopolitical situation of the EU and the underlying political dynamics. He has written extensively on European integration with critical analyses on megatrends, crisis management and various sorts of reforms. He has gathered professional experience in the Ministry of Finance, the Ministry of Foreign Affairs, was a Member of the Cabinet of the European Commission in Brussels and the European Research Director of the Hungarian Institute of International Affairs.

Ján Mišik – received a PhD in personal and property protection and EUR ING in security engineering. He held the position of Assistant Professor at the Department of Security and Defence of the Armed Forces Academy. In his professional activity, he focuses on security management, risk management and international security issues. He currently works as a General State Counsellor of the Ministry of Justice of the Slovak Republic.

Romana Oancea – is an Associate Professor at LFA she holds a PhD in Electronic Engineering since 2011. Her research area covers cybersecurity, image processing, e-learning. She participated in several international and national projects and grants, both as coordinator and member and has published valuable scientific papers on topics like: critical infrastructure protection, face detection and localisation in different contexts, computer and network security.

Aurelian Rațiu – is an infantry officer of the Romanian Land Forces, currently is Associate Professor, Dean of the Faculty of Military Sciences, "Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania. He has a PhD in Military Sciences and Intelligence, master's degree in International Affairs and postgraduate study certificates for: Defense Resources Management for Senior Officials and Crisis management. His expertise area covers military sciences, and comprehensive integrated approach in military conflicts and in complex operational environments. He has contributed to over 15 books, has served on roughly 40 international conference and he has participated in over 10 research projects.

Péter Tálas – is a historian, politologist, expert in security policy, candidate in political sciences. He graduated from ELTE (Eötvös Loránd University) in 1985. Until 1994 he worked as an Assistant Professor at ELTE Faculty of Arts. After that he joined the Centre for Strategic and Defence Studies, since 2003 he has been working as the Director of the Centre. Between 1994 and 2000 he worked at the Hungarian Public Television as freelance editor and reporter. He published as author or co-author 13 books, more than 180 studies and nearly 250 articles. He is editor of 17 books, and editor-in-chief of the journal called Nation and Security. His main research fields are strategic and security policy processes in the East Central European region and new type security challenges.

Paul Tudorache – is a field artillery officer of the Romanian Land Forces, currently working as a Professor at "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.

Milan Turaj – is Assistant Professor at the Department of Military tactics and operational art of the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš. His fields of research are mainly focused on joint fire support, Joint Terminal Attack Controllers, integration of joint fire support into the manoeuvre of land forces, national and international security. He is designated for acting as a Chief of STANEVAL and Programme Manager of NATO accredited National JTAC Training Programme.

Michal Vajda – is Assistant Professor at the Department of Military tactics and operational art of the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš. Artillery officer, his field of research is joint fire support and its integration into operations with focus on artillery gunnery.

In the contemporary conflict environment, hybrid actors and proxy groups often wage war in an asymmetric, low intensity and irregular way. This conflict environment is called VUCA for it is volatile, uncertain, complex and ambiguous. Educational and research institutions should disseminate knowledge to help perform complex tasks and duties in such an environment in an efficient and effective manner. Curriculum development within higher education helps both lecturers and students to gain cutting-edge knowledge to obtain the expected level of performance to counter hybrid threats. European societies require a proper understanding and adequate policy responses. Supporting improved awareness, strengthening resilience and building the required capacity are all part of this effort. The Russo–Ukrainian war just underlies the need for such capacities and capabilities as security challenges and threats do have the potential to undermine the security of the EU and the very values that underpin and inspire its societies. The EU must be committed to address these challenges with all available means for which this first volume of the reference curriculum on hybrid warfare is best suited.

9 789636 530310