# Hybrid Warfare Reference Curriculum Volume III

Edited by
Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS

# Hybrid Warfare Reference Curriculum
# Volume III

# Hybrid Warfare Reference Curriculum
# Volume III

## Elective Lectures

Edited by

Zoltán Jobbágy – Edina Zsigmond

LUDOVIKA
UNIVERSITY PRESS
Budapest, 2025

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

Co-funded by
the European Union Erasmus+

Editors
Zoltán Jobbágy – Edina Zsigmond

Peer reviewed by
András Rácz

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

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

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

Printed and bound in Hungary.

DOI: https://doi.org/10.36250/01237_00

ISBN 978-963-653-109-6 (print)
ISBN 978-963-653-110-2 (ePDF)
ISBN 978-963-653-111-9 (ePub)

# Contents

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

DOI: https://doi.org/10.36250/01237_01

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

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

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

The developed hybrid warfare reference curriculum, its supporting methodology and massive open online course will allow blended (physical and virtual) learning methods for accredited university classes, but also allows for mass online learning, thus reaching a much wider audience. The reference curriculum shall form the basis for either the partial or entire re-design and update of courses within the curriculum of military, police and civilian students of higher education institutions. The reference curriculum as a document reflects the combined knowledge of a multinational team of academics and policy experts drawn from European and Israeli universities and think tanks. The reference curriculum comes as the result of close cooperation between the project partners to motivate others interested in the subject. The reference curriculum also serves as an initial document for individuals or organisations looking to develop a curriculum dedicated to combating hybrid challenges, or to amend their existing curricula accordingly. The content of the hybrid warfare reference curriculum is not intended to be adopted in lockstep, but rather to fit particular needs and aspirations. Its function is to increase intellectual interoperability and foster in-depth and specific academic knowledge and professionalism in an interdisciplinary manner. It can also support interested partners in enhancing their capacities to develop their national skills and improve suitable strategies to counter or wage this sort of warfare. The reference curriculum also serves as a fundamental document to address educational institution requirements and provide helpful guidelines for relevant courses on security and defence. The reference curriculum, among others, provides an overview of underlying ideologies, motivations and methods, as well as contemporary practices and projections of future potential. As such it contributes to European and Transatlantic cooperation in security-related issues through education by offering students, professors, researchers, policy experts and the interested public a new international and interdisciplinary platform of study, and also a foundation for cutting-edge, practice-oriented knowledge. The curriculum also serves as a basis for those who intend to implement tailored versions of the curriculum for their distance learning or residential courses. It contributes to a student-centric environment too, as it can help train students to better understand the complex challenges posed by hybrid warfare and to respond better to it. The reference curriculum promotes critical thinking and a thorough understanding of European core values and interests. This important pedagogical objective is fostered through participatory structures and transformative education. To reach the goals set above and to exploit the synergies created by the participating institutions, the reference curriculum may be regarded as the basis of a modular system resulting in various single or joint degree courses at a later stage. The reference curriculum contributes to a series of online and blended modules with a focus on selected security and defence issues, involving a participative and extensive simulation exercise/wargame moderated by a trained staff. All recipients of the curriculum, irrespective of their previous background and knowledge, shall benefit from a range of delivery methods including:

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

Thus, global issues, especially security ones are increasingly the subject of policy-level deliberations, both nationally and internationally. Transnational cooperation in science deals with these issues. Cooperation in the form of various partnerships is of special importance, because they possess much of the expertise, data and resources that are needed to find effective solutions. The reference curriculum makes clear that hybrid warfare stands for issues and options that deserve the attention of scientists and researchers as they seek to design, initiate and manage collaborative research programmes and projects that include both scientific and development goals. Links between science policy and the mechanisms to address issues raised already exist in EU countries. Motivations and opportunities to support scientific collaboration in the form of partnerships to strengthen research capacity have assigned a higher priority to global issues, put more emphasis on collaborative research, and have moved beyond traditional knowledge transfer. The reference curriculum just reflects the fact that scientists and policy makers increasingly turn towards desirable and even crucial partners who can provide a wide range of expertise, resources and other benefits. Some are identifying ways to organise projects that encourage the full participation of researchers who are actively building and enhancing research capacity to create and utilise the new knowledge that is essential for their development to address local and regional manifestations of global-scale challenges of which hybrid warfare is but one. Recognising the importance of the global security challenges and trends and seeking to maximise the benefits of cooperation through linking science policy with science capabilities thus contemplating new cooperative ventures to improve existing efforts. Moreover, we are living in a time when different generations may see the world dramatically differently. Therefore the experience of the 20th century must reach out to the enthusiasm of the 21st century and make a strong bond. The reference curriculum can forge the bond in the mind and soul of the young generation, of whom university students play an important role as they will form the future cohort of intellectuals and decision-makers that will need to take care of various policy and military responses to hybrid threats in the near future. The reference curriculum offers a comprehensive and interdisciplinary approach in the broadest sense that encompasses definitions and descriptions, addresses the hard and soft aspects of hybrid warfare, and names disciplines and subjects to make hybrid warfare studies accessible for lecturers and students alike. The project stands for a change in the institutional portfolio of the authoring partner institutions since it produces new knowledge that they institutionalise and disseminate through various social practices over time. Thus, the reference curriculum brings something new and creative to the partners involved and to the wider EU community. The partnership powers high quality and fosters innovation by exploring and considering a new concept such as hybrid warfare, and by delivering new content and methods with much value to lecturers, researchers and students. The present book can be seen as a descriptive, reflective and explanatory study of hybrid warfare seen from many different angles. It is descriptive in a sense that it describes hybrid warfare as a complex phenomenon posing serious threats to the stability of any political unity. It is also reflective since by approaching hybrid warfare as an intrinsically complex and multi-layered phenomenon, consistency and coherence is provided by the use of the respective scientific literature and very often Clausewitz's epic volume *On War*. It is explanatory since inconsistencies are discovered, the authors identify and explain the contributory factors in detail. The reference curriculum aims at developing a coherent framework that offers a novel approach to hybrid warfare by detailing the underlying attributes from a multiple point of view. Since the curriculum exceeds the framework of a semester class in volume, the team of authors agreed to divide the chapters into compulsory lectures (Volume I), elective seminars (Volume II) and elective lectures (Volume III), from which lecturers may choose the topics most relevant for their classes. The present, third volume offers a selection of topics suggested for those who wish to further deepen their theoretic knowledge on the subject matter. In this volume historical processes of the 20th and the 21st centuries are compared considering the wide presence and relevance of non-military instruments fused together with the kinetic and operational dimension, making the boundaries between the state of war and "peace" indefinite. The phenomenon of "strategic surprise" will be analysed thoroughly, and it will be shown whether it has a particular resonance with Hybrid Warfare or does it really follow the patterns of other military activities. The defining characteristics of gray zone coercion will be tackled in light of its specific relevance to the maritime domain. For the intellectually hungry, the salami slicing and cabbage peeling tactics will be introduced. Adding to the content of the earlier volumes, the impact of modern technology on warfare and hybrid warfare will be further clarified. The advantages and disadvantages of "hybrid warfare strategy" will be contemplated in various political and military contexts. Again, regional considerations will be analysed in a more thorough way: What are the main concepts of the Chinese strategic culture and why should we be wary of over-examining them? Why does *Unrestricted Warfare* define China's approach to warfare? In which way can we describe ISIS warfare? Why is the notion of hybrid warfare contentious referred to Russian operations? How did Russia intervene in Syria and how did she operate in Africa? In more detail, some case studies will help to put the issue into context, such as the war in Chechnya, in Georgia or the second Lebanon war, and more.

At last, once again the topic of social media will be raised, it being an important instrument not only for public diplomacy but also as a weapon of psychological operations using misleading information and merging it into the online discourse without the target audience realising it. 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 Turin, Italy, the Bar-Ilan University in Ramat Gan, Israel and the Centre for the Study of New Security Challenges in Edinburgh, U.K. wishes interesting and useful readings for all students, lecturers and independent learners.

*Zoltán Jobbágy – Edina Zsigmond*
*editors*

Eitan Shamir[1]

# Hybrid Warfare and Special Operations Forces

This paper explores the role of Special Operations Forces (SOF) within the realm of hybrid warfare. It posits that the distinct characteristics and expertise of SOF render them an exceptionally valuable asset in the context of hybrid warfare. The growth of SOF units over the past two decades and their increasing involvement in various conflicts can be attributed to this unique utility. It is foreseeable that this trend will persist, with the SOF increasingly assuming a central role in the domain of hybrid warfare. On the official NATO website, hybrid threat is defined thus: “Hybrid threats combine military and nonmilitary as well as covert and overt means, including disinformation, cyberattacks, 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 destabilize 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.”[2] 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. […] 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 interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use

[1] Bar-Ilan University.

[2] NATO 2021.

DOI: https://doi.org/10.36250/01237_02

of military means and warfare".[3] As noted above, the term hybrid warfare as it is most commonly used today refers to two separate phenomena:[4]

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.

Considering the two aforementioned aspects of hybrid warfare, SOF offer a compelling value proposition for decision-makers. They are well-equipped to confront the array of challenges presented by hybrid warfare. SOF can effectively participate in or counter information campaigns and psychological warfare. While they are part of the regular army, they excel in the realm of irregular warfare. Despite continuous downsizing over the past two decades, which only reversed with the Russian invasion of Ukraine in February 2022, the armed forces of industrial democracies have experienced a remarkable expansion in terms of SOF. There have been increases in personnel, units, commands and supporting forces, as well as increased budgets and expanded roles. The rapid growth of SOF in the last two decades has been truly exceptional. The growth of SOF should be understood as part of a range of broader military innovations and adoptions including the use of drone units, cyber forces, judicial experts, media specialists and human terrain officers (to mention only a few). SOF have become so effective because they develop in conjunction with other military innovations that enable them to meet the challenges of the changed environments armed forces are facing today. In contrast to other military units that specialise in at most one or two specific sets of expertise, SOF are specialised generalists as they possess extremely varied abilities for action in a variety of fields straddling high and low intensity engagements, nation-building and humanitarian missions, or training indigenous forces and liaising with other national forces.[5] In today's hybrid complex environment, the specialised generalists of SOF units

[3] Hybrid CoE s. a.

[4] Hecht 2024.

[5] Luján 2013; Harkins 2015.

are increasingly attached to a variety of other military forces, governmental and non-governmental appendages and local civilian communities.[6] They link the tactical to the operational and strategic levels in a uniquely active way.[7] They are, to build on a current metaphor, 'strategic corporals'[8] whose tactical actions can have a much bigger impact on the strategic outcome. However, a word of caution is required. SOF are not to be regarded as 'the' solution – some 'surefire' key – to all military problems. Far from it. Nevertheless, in today's world they seem to offer some adaptive advantages that, organisationally speaking, are unique. It is these perceived advantages that have been used in a number of ways. In short, the adaptive potential of SOF means are being constantly used by military and civilian leaders.

## Definition and evolution

Given the contested definitions of these units, they are variously called Commandos, Special Forces or indeed SOF.[9] Therefore, we need to present a clear definition of what we mean by SOF. When we use the term SOF here, we are referring to units trained to operate in small teams, behind enemy lines, utilising a wide range of resources, equipment and technology, which can generate special capabilities that provide innovative solutions to highly problematic circumstances.[10] In addition, all SOF units consist of very high quality personnel, selected through rigorous tests and trials, and trained intensively over long periods.[11] Finally, they often report directly to senior command. Examples of such forces are Delta Force, Navy SEALs and the Green Berets in the U.S., the Special Air Service (SAS) and the Special Boat Service (SBS) in the United Kingdom, and Sayeret Matkal, Naval Commando and Shaldag in Israel. The first special operation forces in the history of modern warfare were created during the Second World War. Realising the importance of sabotage and reconnaissance missions carried out by small specialised forces, all major participants created special units of some sort.

[6] Luján 2013; Harkins 2015.

[7] Adams 1998; Spulak 2007; Turnley 2011.

[8] Krulak 1999.

[9] Last 2004.

[10] Marquis 1997.

[11] Marquis 1997: 48–55; Luján 2013: 24.

The German Army founded the Brandenburgers regiments, which contributed to the campaigns in Poland (1939), the Netherlands and France (1940).[12] The British Army, a leader in this area, established the Special Operations Executive (SOE) in July 1940 after the fall of France,[13] followed by the Special Boat Service (SBS) and the Special Air Service (SAS).[14] The French Commandos Marine was also founded in 1940. At the end of 1942, the U.S. Navy also began forming beach reconnaissance forces, which later evolved into the Navy SEALs.[15] After the war, SOF were created in many militaries.[16] The original tasks given to SOF during WWII were relatively narrow in scope, focusing on reconnaissance, sabotage and partisan activities behind enemy lines. But as the nature of warfare changed in the second half of the 20th century, the range of SOF missions broadened and diversified. SOF were used for counterinsurgency operations and nation-building operations, most frequently in areas of Cold War conflict.[17] Along these lines, SOF were deployed for protracted periods as small units among civilian populations – operating as pacification forces or in cooperation with local military units – and a growing emphasis was given to cultural awareness, regional orientation and language proficiency. In the 1980s and especially in the 1990s, SOF were restructured in many armed forces around the globe. One important change was the creation of command headquarters to synchronise the activities of special units from different branches.[18] The United States Special Operations Command (USSOCOM) and the United Kingdom Special Forces (UKSF) headquarters were both established in 1987, and the French Special Operations Command (COS) was created in 1992. Since 9/11 there has been an ever-greater broadening of SOF activities and SOF have been spearheading the global war on terror.[19] Furthermore, the increasing reliance on SOF and Special Forces Commands has been accompanied by greater participation in civilian operations in addition to standard military missions. Accordingly, SOF commands have infiltrated the cyber warfare and digital information arena while

[12] Williamson 2009.

[13] Seaman 2006.

[14] Robinson 2004.

[15] Shimron 2007.

[16] Exum 2012; Ryan et al. 2003.

[17] Tenenbaum 2016; Jones 2001.

[18] Robinson 2013: 8–9; Turse 2014.

[19] Kiras 2007.

enhancing interagency cooperation for an ever-widening scope of activity.[20] Among the main missions with which the SOF of the United States are charged are counterterrorism, counterinsurgency, counter proliferation of WMD, special reconnaissance, direct action, unconventional warfare, information operations, military information support operations, psychological operations, civil affairs operations, security force assistance and foreign internal defence.[21] These are often broken down into two groups by the SOF community – Direct Action (comprised of Direct Action, Special Reconnaissance, Counterterrorism and Counter Proliferation) and Unconventional Warfare (Unconventional Warfare, Foreign Internal Defence, Civil Affairs, Psychological Operations and Information Operations). In the U.S., for example, the former is traditionally entrusted to the 'Black' SOF (Delta, Seal Team 6 [DEVGRU] and CIA SMUs) and the latter to the 'White' SOF units (75th Rangers, Green Berets, Navy SEALs, 160th SOAR, and the recent addition of the Marine Corps Special Operations Companies and Foreign Training Units).[22] In fact, SOF have participated in a variety of other circumstances including, for example, humanitarian missions, disaster relief,[23] peacekeeping and stability operations, nation-building, Combat Search and Rescue, security assistance, counter-drug-trafficking and hostage rescue operations.[24] Specific forces may, however, be responsible for any combination of all or (more commonly) some of these missions. In addition, within the repertoire of any one unit, there is usually some kind of specialisation. And finally, on a global scope, a division of labour between the SOF of different nations with those of smaller countries can be identified, with the latter filling roles that differ from those carried out by the U.S. SOF. The American SOF community experienced an all-time low in the decade following the Vietnam War. Special Operations Forces had a very limited use in NATO's main war scenario of a massive conventional armoured confrontation in Central Europe. The disastrous outcome of Operation Eagle Claw[25] (also known as Operation Rice Bowl) made it clear to both the American public and policymakers that SOF capabilities were

[20] McLeary 2013.

[21] Horn 2004.

[22] Jackson–Long 2009: 136–137, 139.

[23] Shultz et al. 1995: 161, 203, 210.

[24] Horn 2004.

[25] On 24 April 1980, an ill-fated military operation to rescue the 66 American hostages held in Tehran ended with eight U.S. servicemen dead and no hostages rescued.

in desperate need of an overhaul.[26] The Holloway Commission report established a joint SOF directive that led to the birth of JSOC (Joint Special Operations Command). The growing acknowledgment that low-intensity conflicts (such as liberation wars, often supported by the Soviet Union) and terrorism pose widespread threats to U.S. security led to legislative action culminating in the Goldwater–Nichols Defense Reorganization Act of 1986. This led in turn to the birth of the United States Special Operations Command (USSOCOM) in 1987, in which JSOC was integrated as a Direct Action directive. In 1989, under Major Force Program 11,[27] the SOF dependence on parent services was finally overridden, allowing SOCOM, led by a four-star general, to enjoy an autonomous acquisition. During the past decade and a half, SOCOM has gained significant status through the efforts of SOF against terrorist organisations and especially since it was chosen to spearhead the Global War on Terror (GWOT). The budget and personnel of USSOCOM have risen accordingly.[28] In recent decades USSOCOM's total manpower has also grown dramatically – especially since 2005, when it was established as a mainstay of the War on Terror.[29] From about 33,000 personnel in 2001, numbers steadily rose to about 72,000 troops by the end of 2013.[30] Since 9/11 demand for special operations capabilities in the United Kingdom has also increased dramatically.[31] Accordingly, two additional units were formed, the Special Reconnaissance Regiment (SRR) in 2005 and the Special Forces Support Group (SFSG) in 2006. These were added to the already existing SAS and SBS regiments, thus doubling the number of active units in United Kingdom Special Forces (UKSF). In recent years, while British military forces have undergone financial cuts as a result of the 2010 Strategic Defence and Security Review,[32] the role of Special Forces in future British military strategy has been highly emphasised and appropriately compensated. The 2010 Review stated that the reputation of the country's SOF is widely acknowledged and therefore the size of the units is to be sustained and their support capabilities enhanced.[33] France also increased its interest in special operations over the past

[26] Marquis 1997: 69–73.

[27] Jackson–Long 2009: 142–143.

[28] USSOCOM 2014.

[29] USSOCOM 2008: 8–22; Robinson 2013: 17–18.

[30] McLeary 2013.

[31] USSOCOM 2002: 17.

[32] SIPRI 2013: 187.

[33] U.K. Ministry of Defence 2010: 27, 60.

decade and a half. In 2002, the French Army Special Forces Brigade was established, creating a framework for older SF units. They include the 1st Marine Infantry Parachute Regiment (the French SAS, established as the commando unit of the Free France army during World War II), the 13th Parachute Dragoon Regiment (whose history dates back to the 17th century), and the relatively new 4th Helicopter Regiment, which supplements the Army Special Forces Brigade as well as the other Special Operations Command units *(Commandement des Opérations Spéciales),* such as the French Navy Commandos and the Air Force's Parachute Commandos. More recently, special operations, along with cyber and information services, received further attention because of the growing awareness of low-intensity conflicts.[34] The French White Paper (Livre Blanc) published in 2013 stated: "The Special Forces have proven to be an element of utmost importance in all recent operations. Their personnel and command resources will be reinforced, along with their capacity for coordination with the intelligence services."[35] Israeli awareness of commando operations dates back to pre-independence days with Orde Wingate's Special Night Squads. The establishment of Unit 101 in 1953 was a benchmark event in Israel.[36] Specialising in small-scale guerrilla warfare, Unit 101 was created to carry out the retaliatory policy of Prime Minister David Ben-Gurion and Chief of Staff Moshe Dayan against paramilitary Arab insurgents. In 1957, a new Israeli unit was formed in the spirit of the British SAS, later known as Sayeret Matkal. While originally formulated for special reconnaissance missions, the unit mastered other capabilities and expanded its roles, as exhibited in Operation Bulmus 6 (the raid on Green Island), the Sabena Flight 571 hostage rescue, Operation Aviv-Ne'urim and Operation Entebbe. Over time, senior decision-makers reached the conclusion that a military-wide framework for special operations was needed. Hence, especially with the rising threat of Jihadist terrorist organisations, the Depth Corps was established in 2011 with the responsibility of carrying out operations deep within hostile territory and maximising the efficiency of the IDF's various SOF units.[37] More recently, the IDF established a new commando brigade (the 89th Brigade) that brings together four elite special purpose units.[38]

[34] U.K. Ministry of Defence 2010: 66–68.

[35] Ministère de la Défense 2013.

[36] Hendel 2007: 32.

[37] Oren 2011.

[38] Zitun 2015.

## The changing environments of armed conflicts

How can we explain the growing popularity of SOF? The main explanation emanates from the contemporary characteristics of armed conflict and the hybrid wars of our era. These hybrid wars include opponents organised in a variety of forms (regular armies, terror networks, criminal gangs, or local warlords) in regional conflicts. Moreover, these conflicts pose a very broad set of concrete challenges and missions such as anti-terror, anti-insurgency, policing, working with indigenous forces, humanitarian tasks, civil administration, or rebuilding infrastructure (to mention just a few). Accordingly, the argument goes, SOF are uniquely suited to participating in such conflicts because of their diverse capabilities and ability to quickly adapt to local conditions.[39] The second explanation focuses on domestic developments. The advent of what Luttwak[40] calls post-heroic warfare and Shaw[41] names the 'New Western Way of War' in the industrial democracies refers to new expectations about how armed struggles are to be pursued. These expectations derive from risk aversion, implying lower acceptance of casualties primarily on 'our' side and to a lesser degree on 'their' side[42] and buttressed by a global network of human rights and humanitarian movements calling for much greater precision in the use of military force. This kind of explanation categorises the use of SOF along with new forms of technology (precision-guided munitions) and advanced methods for gathering intelligence (SIGINT and drones, for example) as part of the growing importance of precision warfare and the shift of the armed forces from a 'shooting' to a 'sensing' organisation.[43] Thus SOF represents the potential for covert missions that lower risks to governments and precision warfare that lowers casualty rates for all sides in armed conflict. Another advantage of SOF in today's conflicts has to do with what Shaw[44] calls Global Surveillance – that is, the monitoring of armed actions by new judicial regimes, local, national and global media, politicians, NGOs, humanitarian movements, or any camera-wielding civilian. The point here

[39] Spulak 2007; Turnley 2011: 48; Leslau 2010.

[40] Luttwak 1995.

[41] Shaw 2005.

[42] The literature shows that sensitivity is contingent by various conditions but it continues to be a factor in democratic decision-making, see Smith 2005: 487–512; Coker 2002; Levy 2009: 69–82; Shaw 2005: 97–98.

[43] Arquilla 2010.

[44] Shaw 2005.

is that the armed forces have become much more transparent than they were in the past and hence are constantly struggling over their professional autonomy.[45] In other words, Global Surveillance implies a constant encroachment on the armed forces in terms of their (relative) freedom or discretion to decide not only about personnel issues and procurement but, much more importantly, operational matters. As a result, the new circumstances in the theatres of conflict around the globe have led to an even greater emphasis on discretion and deniability. Here, SOF, with their high level of professionalism, ability to work covertly, and small size offer a distinct advantage to the militaries of the industrial democracies.[46] The strength of external surveillance over the armed forces is unparalleled in history. It is in this light that the advantage of SOF should be seen.[47] Each of these explanations contends that SOF are a form of organisational adaptation to the new international and domestic environments within which the armed forces operate. The establishment and expansion of SOF thus seems a reasonable move in terms of organisational adaptation to the accumulated influence of all these global and domestic processes.

## Adaptive advantage

Despite cutbacks in forces since the end of the Cold War, during the past two or so decades, militaries have actually seen a significant enlargement, augmentation, or invention of a host of units and organisations. Alongside SOF we find a flowering of assorted functions that include drone units,[48] cyber forces,[49] intelligence apparatuses,[50] judicial arms,[51] spokespersons and media relations functionaries[52] and various kinds of experts, including organisational

[45] Shamir – Ben-Ari 2018: 335–354; Forster 2012: 273–290; Rubin 2002: 36–57; Verhoest et al. 2004: 101–118.

[46] Horn 2004: 5–6.

[47] Gelpi et al. 2006: 7–46; Gelpi et al. 2009.

[48] Parsons 2013; Springer 2013.

[49] Rid 2012: 5–32; Even – Siman-Tov 2011: 15–32.

[50] Forrester 2014; Pecht–Tishler 2015.

[51] Cohen – Ben-Ari 2014; Dickinson 2010: 1–28; Luban 2012.

[52] Bet-El 2009: 65–80.

consultants,[53] translators,[54] Human Terrain Systems teams[55] or CIMIC officers.[56] What appears to be happening is that the long historical processes of internal military differentiation and specialisation have intensified and broadened since the 1990s[57] to include the development of various organisational capabilities in specific departments, units, or roles. All these new or renewed organisational capabilities seek to address the wider political, economic, social, technological and legal changes charted out in the previous section and can be seen as adaptive innovations to demands placed on the armed forces that expand their ability to meet a plethora of external threats and risks.[58] SOF are part of this trend, but they are also different from other specialisations that have emerged or expanded in recent decades. SOF not only embody various specialties in and of themselves but also possess an ability to put together specialists in unique ways that link them, in a very different way from other specialisations, to the top levels of the military and political hierarchy. The following section explores the adaptive features of SOF that render them exceptionally valuable in the context of hybrid warfare. First, on the most basic level, SOF have a very wide variety of conventional and non-conventional capacities providing a range of responses to a broad spectrum of challenges posed by today's conflicts. [59] Even a small SOF unit can offer as large a range of capabilities as a much bigger conventional unit. In fact, SOF training focuses on specialising in a wide variety of missions, roles and capabilities. Their ability to master a broad range of missions stems from the high quality of their recruits, intense processes of selection, and years of service.[60] Their constant use in operations reinforces knowledge creation and self-confidence. In taking up these roles, operatives display an impressive array of skills such as communication skills, the ability to quickly join and detach from other units and civilian bodies, the ability to 'see the big picture', and the ability to master diverse areas of knowledge. Thus, they can be characterised as 'specialised generalists' who offer a multitude of adaptive solutions to militaries.[61]

[53] Johnson 2002: 233–241.
[54] Footitt 2012: 1–11.
[55] Fawcett 2009.
[56] Lloyd – Van Dyk 2007: 68–94.
[57] Shamir – Ben-Ari 2018: 314.
[58] Webb 2013.
[59] Spulak 2007.
[60] Turnley 2008; Turnley 2011.
[61] Shamir – Ben-Ari 2018: 335–371.

As specialised generalists, SOF embody in their actions the central tensions of contemporary hybrid conflicts. Thus, for instance, SOF troops or units easily exemplify many of the mixed roles[62] soldiers are tasked with today. They can be warrior-diplomats,[63] warrior-medical experts, or warrior-social workers.[64] In taking up these roles, they display a wide array of skills such as flexibility and the ability to quickly join with and detach from other units and civilian agencies such as NGOs, UN units of different nationalities, local communities, or indigenous forces – a skill that is much needed in hybrid conflicts. In other words, they take up a variety of roles as part of highly adaptable mixtures of alliances, coalitions, ad-hoc formations and temporary organisational shapes.[65] This skill set allows operatives to easily ally themselves with other specialised units that operate drones, analyse intelligence, perform logistical tasks and develop targeting packages for SOF. Thus, SOF can be described as experts at linking and integrating other specialisations. They have the knowledge to connect varied units within the military, such as, for example, identifying and attacking moving targets using real-time intelligence with a variety of assets such as drones or precision munitions.[66] Another distinct advantage of SOF is their connection to the senior command levels. They serve as a direct link connecting senior strategic command to tactical action. In this role SOF provide the senior command with effective tentacles for monitoring and understanding different environments and acting upon them. They are strategic corporals who have the potential to create strategic change.[67] It is no surprise, then, that many SOF officers rise through the ranks to become senior leaders.[68] Another significant aspect of SOF's contribution to hybrid warfare lies in the covert nature of many of their missions, which offers opportunities for plausible deniability in various forms. These include psychological operations (PSYOP), sabotage or decapitation operations. By definition, covert operations are conducted away from the public eye and many operations become public knowledge only after they have been accomplished and the political echelon decides to publicise the information (as in the raid on Osama bin Laden's hideout in 2011) or after a blunder or

[62] Ben-Ari et al. 2010; Simons 2004: 79–92.

[63] Burke 2009; Turnley 2011: 30.

[64] Robinson 2013: 12.

[65] De Waard – Kramer 2010.

[66] Leslau 2010: 520–521.

[67] Spulak 2007; Miller 1995: 38.

[68] King 2015; Barash–Amitai 2007; Zonder 2000: 10.

accident occurs (as in Operation Eagle Claw in Iran in 1980). The majority of SOF operations are planned, authorised and executed away from the public eye under conditions of secrecy. In contrast to deployments of regular units, very few individuals – including senior military leaders – know at any given moment the whereabouts of SOF units and the nature of the missions they plan and execute. Deniability refers to a situation in which political leaders can safely and believably deny knowledge of any particular truth because they are deliberately made unaware of it so as to shield them from responsibility associated with direct knowledge. Thus, SOF can, at times, carry out what would be considered illegal missions that are not officially sanctioned by governments so that they, who usually benefit from such missions, can safely disavow any knowledge of them in the event of their publicly uncovered success or failure. In other cases, governments may simply offer no public comment about the actions of SOF. Finally, an additional adaptive advantage of SOF is their role as testing grounds for experimentation and the initial implementation of new technologies, doctrines and practices. For instance, a significant portion of new weaponry, equipment and operational methods undergo their initial introduction and rigorous testing within these units. Once refined and improved, much of the equipment and many of the innovative procedures are subsequently disseminated to the broader 'conventional' formations.[69]

## A cautionary note

While SOF represent the many advantages we have outlined, they may also be at times counter-adaptive. One such danger centres on SOF falling prey to their own purported successes (buttressed and cultivated through thriving formal and informal public relations and marketing efforts).[70] The standing of many such units in the armed forces of the industrial democracies has grown to mythical proportions that may hide their limitations. This might lead politicians and senior military commanders to overestimate what they can achieve. One study found that policy-makers and opinion-leaders "ascribe exceptionally high importance to special operations compared to other military capabilities".[71] Indeed, a belief in

[69] Spulak 2007; Hendel 2007; King 2013.

[70] Leslau 2010: 526.

[71] Last–Thornburn 2004: 2.

the superior abilities of SOF *may* have led to a number of significant failures and disappointments.[72] A partial list of such cases since the end of the Cold War would include SAS teams failing to locate the Scud missile launchers in Iraq in 1991 (some SAS members were captured or killed in these missions);[73] the disastrous raid of Delta Force and the Rangers in Somalia 1993 (the incident widely known as Black Hawk Down), which led to major international embarrassment and a U.S. retreat from the country;[74] the 2005 Operation Red Wings in Afghanistan, which culminated in a severe loss of human life;[75] and the failed attempt to rescue Luke Sommers in Yemen.[76] The Afghanistan efforts in 2001 have also been criticised for their overreliance on SOF (in coalition with local warlords) at the expense of deploying regular ground units, which enabled Osama bin Laden to escape and survive another decade.[77] The Israel Defense Forces (IDF) has been emphasising the development and deployment of SOF in recent decades.[78] But despite intensive use of SOF for gathering intelligence and conducting raids, their impact on the strategic outcome of major campaigns such as the Second Lebanon War (2006) or Protective Edge in Gaza (2014) has been all but negligible.[79] Their role in repelling the attack by Hamas on Israel on 7 October 2023, was indeed significant – but the subsequent Israeli counteroffensive into Gaza was primarily led by heavy armour and engineering units. Overemphasis on SOF can also lead to the neglect of regular forces in the competition for material and human resources.[80] Accordingly, in some European militaries a few SOF or Commando units are kept in good operational condition while the rest of the force is incapable of mounting serious combat missions.[81] Examples include the British, German and French dependence on logistics, airlifting and intelligence provided by the U.S. during the 2011 NATO campaign in Libya[82] and the French campaign in

[72] Horn 2004: 8.

[73] McNab 1993: 110–238.

[74] Allard 1995.

[75] Luttrell–Robinson 2007: 307.

[76] Thompson 2014.

[77] Barzilai 2013; Bergen 2009.

[78] Shamir–Hecht 2013.

[79] Leslau 2010: 513, 526; Hendel 2007: 36; Petrelli 2012: 56–73.

[80] Horn 2004: 6–7.

[81] BBC 2014.

[82] Mölling 2011.

Mali.[83] Many of the units fielded by European armed forces in Iraq and Afghanistan were very capable conventional forces, but they were usually small in number and frequently comprised elite infantry units. Indeed, this trend may reinforce the mediocrity of regular forces that might be desperately needed in some scenarios of armed conflict. Because they are small in scale, the SOF lack mass, one of the great advantages of conventional units in terms of friction.[84] More widely, militaries are based on discipline that inculcates conformity and results in the certainty of command – the assurance that an order will be followed in a prescribed fashion every time.[85] In simple terms, conventional forces are often considered "reliable, disciplined, and predictable".[86] Special Forces, on the other hand, do not always adhere to the same strict discipline as conventional units, which can make them more challenging to control from the perspective of many senior commanders. This, coupled with the culture of covert operations and plausible deniability, can give rise to what is known as "rogue units".[87] One such case would be former SAS officer General David Richards' campaign against the rebels in Sierra Leone, which secured the official regime that Richards felt was more favourable to the British national interest – despite his formal orders, which only required him to conduct limited evacuation operations.[88] This (relative) disregard may be exacerbated by the close connections between SOF and senior decision-makers. Given that SOF commanders have the attention of policymakers, they may wield disproportionate influence in shaping military priorities, not only with respect to budget allocation but also in the authorisation, selection and prioritisation of SOF missions. As a result, proximity and access to senior military and civilian leaders can have both adaptive and potentially maladaptive consequences.

[83] Earlanger 2013.
[84] Spulak 2007: 31.
[85] Turnley 2011: 54.
[86] Last 2004: 37.
[87] Axe 2014.
[88] King 2015.

## Conclusion

This chapter has emphasised that Special Operations Forces (SOF) units are exceptionally well-equipped and effective in addressing the diverse challenges posed by contemporary hybrid warfare. The notable growth of SOF reflects how military organisations have had to adapt to ever-evolving hybrid environments. In contrast to other recent military organisational innovations, the significant value of SOF lies in their adaptability and role as specialised generalists. They provide the armed forces with the capability to link external and internal components to establish flexible formations. SOF not only excel in these roles but also represent compact units that, at times, can have a substantial impact through various forms of coordinated action. Within the context of broader organisational changes, SOF distinguish themselves by serving as field integrators who bridge the tactical, operational and strategic levels of action, thereby facilitating a combined effect of diverse systems and technologies. Consequently, SOF contributes by managing connections between the armed forces and external environments and integrating specialised functions. Furthermore, as units, they seamlessly blend thorough planning with improvisation, establish direct connections with a wide array of both military and non-military actors, and possess the capacity to act autonomously and clandestinely. Collectively, these distinct characteristics make SOF highly suitable for hybrid warfare.

## Questions

1. What distinguishes SOF units?
2. What is the definition of SOF, and do you think alternative definitions could be applicable? Can you propose an alternative definition?
3. What factors contributed to the significant growth of SOF units and SOF organisations (such as SOF headquarters and commands) in the past two decades?
4. What are the primary key adaptive advantages of SOF?
5. What potential disadvantages or drawbacks might be associated with SOF?
6. Do you concur with the idea that SOF is the optimal tool for use in hybrid warfare? Please provide a detailed discussion.

## References

Adams, Thomas K. (1998): *US Special Operations Forces in Action. The Challenge of Unconventional Warfare.* London: Frank Cass.

Allard, Kenneth (1995): *Somalia Operations: Lessons Learned.* CCRP Publication Series.

Arquilla, John (2010): The New Rules of War. *Foreign Policy,* 11 February 2010.

Axe, David (2014): American Commando Brought His Girlfriend to Afghanistan – And Armed Her. *War Is Boring,* 26 March 2014. Online: https://medium.com/war-is-boring/american-commando-brought-his-girlfriend-to-afghanistan-and-armed-her-b25209f58e8

Barash, Tamar – Amitai, Yotam (2007): Kochot HaMivtza'im HaMeyuchadim BaTzahal – Avar VeHoveh [Special Operations Forces in the IDF – Past and Present]. *Ma'archot,* 411, 14–22.

Barzilai, Yaniv (2013): How bin Laden Escaped in 2001 – The Lessons of Tora Bora. *The Daily Beast,* 15 December 2013.

BBC (2014): NATO 'Unprepared' for Russia Threat, Say MPs. *BBC News,* 31 July 2014. Online: http://www.bbc.com/news/uk-politics-28577904

Ben-Ari, Eyal – Lerer, Zeev – Ben-Shalom, Uzi – Vainer, Ariel (2010): *Rethinking Contemporary Warfare. A Sociological View of the Al-Aqsa Intifada.* Albany: State University of New York Press.

Bergen, Peter (2009): The Battle for Tora Bora. How We Nearly Caught Osama bin Laden. *The New Republic,* 30 December 2009.

Bet-El, Ilana (2009): Media and Conflict: An Integral Part of the Modern Battlefield. In Kobi, Michael – Kellen, David – Ben-Ari, Eyal (eds.): *The Transformation of the World of War and Peace Support Operations.* Westport: Praeger Security International, 65–80.

Burke, Edward (2009): *Leaving the Civilians Behind: The 'Soldier-Diplomat' in Afghanistan and Iraq.* Madrid: FRIDE.

Cohen, Amichai – Ben-Ari, Eyal (2014): Legal Advisors in the Armed Forces: Military Lawyers in the Israel Defense Forces as Mediators, Interpreters, and Arbiters of Meaning during Operations. *Journal of Political and Military Sociology: An Annual Review,* 42, 125–148.

Coker, Christopher (2002): *Humane Warfare.* London: Routledge.

De Waard, Erik – Kramer, Eric-Hans (2010): Expeditionary Operations and Modular Organization Design. In Soeters, Joseph – Van Fenema, Paul C. – Beeres, Robert (eds.): *Managing Military Organizations. Theory and Practice.* London: Routledge, 71–83.

Dickinson, Laura A. (2010): Military Lawyers on the Battlefield: An Empirical Account of International Law Compliance. *American Journal of International Law,* 104(1), 1–28. Online: https://doi.org/10.5305/amerjintelaw.104.1.0001

Earlanger, Steven (2013): Shrinking Europe Military Spending Stirs Concern. *The New York Times,* 23 April 2013.

Even, Shmuel – Siman-Tov, David (2011): Cyber Warfare: Concepts, Trends and Implications for Israel. *INSS Memorandum,* 109.

Exum, Andrew (2012): Special Operations Forces' Expanding Global Role. *World Politics Review,* 30 May 2012.

Fawcett ,Grant S. (2009): *Cultural Understanding in Counterinsurgency: Analysis of the Human Terrain System.* Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College.

Footitt, Hilary (2012): Introduction: Languages and the Military: Alliances, Occupation and Peace Building. In Footitt, Hilary – Kelly, Michael (eds.): *Languages and the Military. Alliances, Occupation and Peace Building.* London: Palgrave Macmillan, 1–11. Online: https://doi.org/10.1057/9781137033086_1

Forrester, Anna (2014): ODNI, DoD Update Proposed Budget for FY 2015 Intelligence Programs. *ExecutiveGov,* 24 November 2014. Online: http://www.executivegov.com/2014/11/odni-dod-update-proposed-budget-for-fy-2015-intelligence-programs/

Forster, Anthony (2012): The Military Covenant and British Civil–Military Relations: Letting the Genie Out of the Bottle. *Armed Forces and Society,* 38(2), 273–290. Online: https://doi.org/10.1177/0095327X11398448

Gelpi, Christopher – Feaver, Peter D. – Reifler, Jason (2006): Success Matters: Casualty Sensitivity and the War in Iraq. *International Security,* 30(3), 7–46. Online: https://doi.org/10.1162/isec.2005.30.3.7

Gelpi, Christopher – Feaver, Peter D. – Reifler, Jason (2009): *Paying the Human Costs of War. American Public Opinion and Casualties in Military Conflicts.* Princeton: Princeton University Press. Online: https://doi.org/10.2307/j.ctt7snhn

Harkins, Homer W. (2015): What is Old is New Again: The Reemergence of Special Warfare. *Special Operations Journal,* 1(2), 112–118. Online: https://doi.org/10.1080/23296151.2015.1096687

Hecht, Eado (2024): Defining Hybrid Warfare. In Jobbágy, Zoltán – Zsigmond, Edina (eds.): *Hybrid Warfare Reference Curriculum. Volume I. Compulsory Lectures.* Budapest: Ludovika University Press, 31–49.

Hendel, Yoaz (2007): IDF Special Units: Their Purpose and Operational Concept. *Strategic Assessment (INSS),* 10(2), 31–39.

Horn, Bernd (2004): Special Men, Special Missions: The Utility of Special Operations Forces – A Summation. In Horn, Bernd – De B. Taillon, Paul J. – Last, David (eds.): *Forces of Choice. Perspectives on Special Operations.* Toronto–Montreal: McGill-Queen's University Press, 3–34.

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

IISS (2013): *The Military Balance 2013.* London: The International Institute for Strategic Studies.

Jackson, Colin – Long, Austin (2009): The Fifth Service: The Rise of Special Operations Command. In Sapolsky, Harvey M. – Friedman, Benjamin H. – Rittenhouse Green, Brendan (eds.): *US Military Innovation since the Cold War. Creation Without Destruction.* New York: Routledge, 136–154. Online: https://doi.org/10.4324/9780203878651

Johnson, Brad W. (2002): Consulting in the Military Context: Implications of the Revised Training Principles. *Consulting Psychology Journal: Practice and Research,* 54(4), 233–241. Online: https://doi.org/10.1037//1061-4087.54.4.233

Jones, Tim (2001): *Postwar Counterinsurgency and the SAS 1945–1952.* London: Frank Cass.

King, Anthony (2013): *The Combat Soldier. Infantry Tactics and Cohesion in the Twentieth and Twenty-First Centuries.* Oxford: Oxford University Press.

King, Anthony (2015): Military Command in the 21st Century through the Eye of Two Generals. *War on the Rocks,* 22 January 2015.

Kiras, James D. (2007): *Special Operations and Strategy. From World War II to the War on Terrorism.* London: Routledge.

Krulak, Charles C. (1999): The Strategic Corporal: Leadership in the Three Block War. *Marine Corps Gazette,* 83(1), 14–17.

Last, David (2004): Special Operations Forces in Conventional Armies: "Salvation Army" or "Dirty Dozen"? In Horn, Bernd – De B. Taillon, Paul J. – Last, David (eds.): *Forces of Choice. Perspectives on Special Operations.* Toronto–Montreal: McGill-Queen's University Press, 36–57.

Last, David – Thornburn, Hugh (2004): Elite Opinion about Special Operations. In Horn, Bernd – De B. Taillon, Paul J. – Last, David (eds.): *Forces of Choice. Perspectives on Special Operations.* Toronto–Montreal: McGill-Queen's University Press, 88–101.

Leslau, Ohad (2010): Worth the Bother? Israeli Experience and the Utility of Special Operation Forces. *Contemporary Security Policy,* 31(3), 509–530. Online: https://doi.org/10.1080/13523260.2010.521703

Levy, Yagil (2009): An Unbearable Price: War Casualties and Warring Democracies. *International Journal of Politics, Culture and Society,* 22(1), 69–82. Online: https://doi.org/10.1007/sl0767-009-9048-x

Lloyd, Gary – Van Dyk, Gielie (2007): The Challenges, Roles and Functions of Civil Military Coordination Officers in Peace Support Operations: A Theoretical Discussion. *Scientia Militaria,* 35(2), 68–94. Online: https://doi.org/10.5787/35-2-38

Luban, David (2012): Military Lawyers and the Two Cultures Problem. *Georgetown Law Faculty Publications and Other Works,* 937.

Luján, Fernando M. (2013): *Light Footprints. The Future of American Military Intervention.* Washington, D.C.: Center for a New American Security.

Luttrell, Marcus – Robinson, Patrick (2007): *Lone Survivor.* New York: Little, Brown & Company.

Luttwak, Edward (1995): Toward Post-Heroic Warfare. *Foreign Affairs,* 74(3), 109–122.

Marquis, Susan L. (1997): *Unconventional Warfare. Rebuilding U.S. Special Operations Forces.* Washington, D.C.: Brookings Institution Press.

McLeary, Paul (2013): Life After Wartime: SOCOM Focuses on Global Partnership, Troop Mobility. *Defense News,* 8October 2013.

McNab, Andy (1993): *Bravo Shtayim Efes* [Bravo Two Zero]. Jerusalem: Keter Publishing.

Miller, Sergio (1995): Ha'im Yesh Atid LeKochot HaMivtza'im HaMeyuchadim? [Is There a Future for Special Operations Forces?] *Ma'archot,* 341.

Ministère de la Défense (2013): *French White Paper on Defence and National Security.* Paris: Ministry of Defence.

Mölling, Christian (2011): Europe Without Defence. *German Institute for International and Security Affairs, SWP Comments,* 38.

NATO (2021): *Countering Hybrid Threats.* Online: https://www.nato.int/cps/en/natohq/topics_156338.htm

Oren, Amir (2011): Ma Omed Me'achorei HaHakama Shel Mifkedet Ma'arach Ha'Omek BaTzahal [What Is Behind the Recent Establishing of the Depth Corps Command in the IDF]. *Ha'aretz.*

Parsons, Dan (2013): Worldwide, Drones Are in High Demand. *National Defense,* 97(714).

Pecht, Eyal – Tishler, Asher (2015): The Value of Military Intelligence. *Defence and Peace Economics,* 26(2), 179–211. Online: https://doi.org/10.1080/10242694.2014.886435

Petrelli, Niccolò (2012): The Mission Dimension: IDF Special Operations Forces and Strategy in the Second Lebanon War. *Small Wars and Insurgencies,* 23(1), 56–73. Online: https://doi.org/10.1080/09592318.2012.632853

Rid, Thomas (2012): Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35(1), 5–32. Online: https://doi.org/10.1080/01402390.2011.608939

Robinson, Linda (2004): *Masters of Chaos. The Secret History of the Special Forces.* New York: PublicAffairs.

Robinson, Linda (2013): The Future of U.S. Special Operations Forces. *Council on Foreign Relations, Council Special Report,* (66).

Rubin, Gerry R. (2002): United Kingdom Military Law: Autonomy, Civilianization, Juridification. *Modern Law Review,* 65(1), 36–57.

Ryan, Mike – Stilwell, Alexander – Mann, Chris (2003): *The Encyclopedia of the World's Special Forces.* Storud: The History Press.

Seaman, Mark ed. (2006): *Special Operations Executive. A New Instrument of War.* London: Routledge.

Shamir, Eitan – Ben-Ari, Eyal (2018): The Rise of Special Operations Forces: Generalized Specialization, Boundary Spanning and Military Autonomy. *Journal of Strategic Studies,* 41(3), 335–371. Online: https://doi.org/10.1080/01402390.2016.1209656

Shamir, Eitan – Hecht, Eado (2013): Neglect of IDF Ground Forces: A Risk to Israel's Security. *BESA Center Perspectives Paper,* (225), 4 December 2013. Online: https://besacenter.org/wp-content/uploads/2013/12/perspectives225.pdf

Shaw, Martin (2005): *The New Western Way of W*ar. London: Polity.

Shimron, Gad (2007): *Yechidot Meyuchedot Tzvaot Z'arim* [Special Units in Foreign Armies]. Tel-Aviv: Ministry of Defense Press.

Shultz, Richard H. Jr. – Pfaltzgraff, Robert L. Jr. – Stock, Bradley W. eds. (1995): *Roles and Missions of SOF in the Aftermath of the Cold War.* Collingdale, PA: Diane Publishing Co.

Simons, Anna (2004): The Evolution of the SOF Soldier: An Anthropological Perspective. In Horn, Bernd – De B. Taillon, Paul J. – Last, David (eds.): *Forces of Choice. Perspectives on Special Operations.* Toronto–Montreal: McGill-Queen's University Press, 79–91.

SIPRI (2013): *Yearbook 2013. Armaments, Disarmament and International Security.* Stockholm: Stockholm International Peace Research Institute.

Smith, Hugh (2005): What Costs Will Democracies Bear? A Review of Popular Theories of Casualty Aversion. *Armed Forces and Society,* 31(4), 487–512. Online: https://doi.org/10.1177/0095327X0503100403

Springer, Paul J. (2013): *Military Robots and Drones. A Reference Handbook.* Santa Barbara: ABC-CLIO.

Spulak, Robert G. (2007): *A Theory of Special Operations: The Origin, Qualities and Use of SOF.* Hurlbert Field: Joint Special Operations University.

Tenenbaum, Élie (2016): Beyond National Styles. Towards a Connected History of Cold War Counterinsurgency. In Heuser, Beatrice – Shamir, Eitan (eds.): *Insurgencies and Counterinsurgencies. National Styles and Strategic Cultures.* Cambridge: Cambridge University Press, 313–331. Online: https://doi.org/10.1017/9781316471364.015

Thompson, Mark (2014): U.S. Hostage Killed During Failed Rescue Attempt in Yemen. *Time,* 6 December 2014.

Turnley, Glicken Jessica (2008): Retaining Precarious Value as Special Operations Go Mainstream. *Joint Special Operations University Report,* 8(2).

Turnley, Glicken Jessica (2011): Cross-Cultural Competence and Small Groups: Why SOF Are the Way SOF Are. *Joint Special Operations University Report,* 11(1).

Turse, Nick (2014): The Rise of the Military's Secret Military. *Salon,* 8 January 2014. Online: https://www.salon.com/2014/01/08/the_rise_of_the_militarys_secret_military_partner/

U.K. Ministry of Defence (2010): *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* . London: MoD.

USSOCOM (2002): *United States Special Operations Command History: 1987–2007.* Tampa: United States Special Operations Command.

USSOCOM (2008): *United States Special Operations Command History: 1987-2007.* Tampa: United States Special Operations Command.

USSOCOM (2014): *Fiscal Year 2015 Budget Estimates.* Online: https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2015/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/USSOCOM_PB15.pdf

Verhoest, Koen – Peters, Guy B. – Bouckaert, Geert – Verschuere, Bram (2004): The Study of Organisational Autonomy: A Conceptual Review. *Public Administration and Development,* 24(2), 101–118. Online: https://doi.org/10.1002/pad.316

Webb, Brandon (2013): The Conventionalization of US Special Operations. *SOFREP,* 25 September 2013.

Williamson, Gordon (2009): *German Special Forces of World War II.* Oxford: Osprey Publishing.

Zitun, Yoav (2015): ומדוקי ןתיא קוצ ידקפמ ,ודנמוק תביטח המקוה [A Commando Brigade Has Been Established]. *Ynet,* 6 July 2015. Online: http://www.ynet.co.il/articles/0,7340,L-4676843,00.html

Zonder, Moshe (2000): *Hativat HaKomando Hukma* [A Commando Brigade Has Been Established]. Jerusalem: Keter Publishing.

Eado Hecht[1]

# Implications for Military Strategy

The purpose of this chapter is to provide a theoretical background and historical examples of the employment of the concept of Hybrid Warfare in Military Strategy. Thus strategy is defined as "a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives".[2] Military strategy is therefore the portion of strategy that employs the military instrument to achieve the political objectives: "That component of national or multinational strategy, presenting the manner in which military power should be developed and applied to achieve national objectives or those of a group of nations."[3] Military strategy determines the results required from the military forces and then creates the operational plans for achieving those results, including the tactics to be employed within those operations. In this context the concept of Hybrid Warfare describes a particular set of operational and tactical methods to be employed. The choice of a military strategy depends not only on the free will of the strategists determining the military objective best suited to compelling the enemy to surrender and then choosing the best method they think will achieve that desired military objective. The strategists' options are also determined by the tools and capabilities at their disposal. These tools and capabilities are determined by the organisation and characteristics of the military force, the manpower available to it, the equipment available to it and the industrial sources of that equipment. These tools and capabilities are often not designed specifically for the particular war but were created and maintained over many years. They are determined by the culture and political organisation of the society establishing and maintaining that force.[4] The equipment depends also on that particular society's indigenous technological capabilities and its ability to acquire equipment from others. A final factor affecting the choice of military strategy are the cultural and political

[1] Bar-Ilan University.

[2] *Department of Defense Dictionary of Military and Associated Terms* 2018.

[3] *NATO Glossary of Terms and Definitions AAP-06* 2013: 2-M-6.

[4] Nemeth 2002.

DOI: https://doi.org/10.36250/01237_03

constraints on employing its military force – what is allowed and what is not, what are the opinions of allies or other possible enemies and what is the position of the military tool in the variety of tools employed by the political leadership in conducting the conflict (diplomacy, lawfare, psychological warfare, economic warfare, cyber warfare) and the preferred intensity of violence to be employed.

## Hybrid Warfare as a military strategy

As described in the second chapter of *Hybrid Warfare Reference Curriculum. Volume I,*[5] the definition of Hybrid Warfare is constantly evolving and this requires that we first define that term for the purposes of this module. Currently, at the political level the terms Regular Warfare versus Irregular Warfare are commonly used to differentiate between the conduct of war between rival states (Regular Warfare) versus the conduct of war between a state and a non-state or between two non-states (Irregular Warfare). Also currently, at the strategic level the terms Regular Warfare versus Irregular Warfare are commonly used to differentiate between state armies employing direct military confrontation to defeat each other, destroy each other's war-making capacity or seize or retain territory in order to force a change in an adversary's government or policies (Regular Warfare) from state security forces fighting a non-state organisation in a collision of insurgency–counterinsurgency, terrorism–counterterrorism, psychological and information operations, civil–military operations and transnational criminal–policing activities (Irregular Warfare).[6] From these common definitions stem many of the operational and tactical usages of the concept of Hybrid Warfare and its synonyms. However, as previously explained, these definitions and descriptions are limited by the current cultural, ideological and contextual viewpoint of the various users and drag the discussion of methods of warfare from one on military methodology to a political debate on the legitimacy of the specific rivals and their political goals. Historically, this is an incorrect view – both state and non-state groups have conducted both Regular Warfare and Irregular Warfare and have employed strategies that include all of the methods listed above. Past use of these terms referred to the manner of conducting military operations and the tactics employed, NOT to the identities, organisation, political

[5] Hecht 2024: 31–49.

[6] *Irregular Warfare (IW) Joint Operating Concept (JOC)* 2007.

goals or legitimacy of the belligerents. The use of terms such as ‘conventional’, ‘traditional’ and ‘classic’ warfare as synonyms for Regular Warfare, whereas Irregular Warfare is described as ‘unconventional’, ‘non-traditional’, or ‘new’, etc. is also problematic from a historical point of view, as these terms suggest that Regular (conventional–traditional–classic) Warfare has been the most common form of warfare throughout history whereas Irregular (unconventional–non-traditional–new) Warfare has been the exception. In fact, the opposite is true – Irregular Warfare has always been much the most common type of warfare conducted throughout history with occasional local and temporary exceptions. The regularity of Regular Warfare does not refer to it being the norm, but rather to the fairly regular (orderly) patterns of geographic deployment (formations) and temporal phases of employment, whereas Irregular Warfare refers to the forces being deployed and employed without a clearly discernible geographic and temporal pattern, i.e. irregularly (without order). Thus, the purely military terms Regular Warfare and Irregular Warfare refer not to the identity of the warring organisations, but to two distinct manners of conducting operations and tactics:

Regular warfare is most easily recognised in practice by the closely coordinated employment of large forces, concentrated in time and space, with achievements measured mostly in conquest or retention of territory and/or direct destruction of large quantities of enemy forces. Because of the temporally and spatially concentrated employment of the rival forces, the overall intensity of combat operations (the frequency of individual combat actions and strength of each of these actions) is usually medium to high.

Irregular warfare is most easily recognised in practice by the employment of autonomous small forces scattered in space, independently conducting mostly ‘hit and run’ actions scattered over time, with achievements measured mostly in the gradual collective psychological exhaustion of the enemy. Because of the temporally and spatially scattered employment of separate small forces, the overall intensity of combat operations (the frequency of individual combat actions and strength of each of these actions) is usually very low to low.

A common error in assuming the distinction between Regular Warfare and Irregular Warfare refers to two completely separate phenomena, with Hybrid Warfare being a separate third phenomenon in between. The reality is that pure Regular Warfare and pure Irregular Warfare are two ends of a continuum, along which they merge in different quantities and that Hybrid Warfare merely refers to the midpoint along this continuum – i.e. the area in which the two forms are employed in roughly equal proportions. Thus, a campaign conducted mostly by Irregular Warfare methods might include specific acts conducted according to Regular Warfare methods, and vice versa, a campaign conducted mostly by Regular Warfare methods might include specific acts conducted according to Irregular Warfare methods. The rationale behind employing the opposite method would be its assistance to the main method employed in that operation. The concept of Hybrid Warfare describes an operation in which the two methods are merged more or less equally in one operational plan to mutually benefit from each other's unique effects.

| **Regular Warfare** | **Hybrid Warfare** | **Irregular Warfare** |
|---|---|---|

The proportion may vary over time and in different sectors of the Theatre of Operations – campaigns may oscillate between more Regular Warfare methods, more Hybrid Warfare methods or more Irregular Warfare methods according to the deliberate decisions or constraints of the adversaries. At a particular phase of the War, one adversary may prefer a particular mix whereas the other might simultaneously prefer a different mix. Each might be able to employ the mix of their choice or might be compelled to adopt the adversary's choice because of various political, strategic or logistic reasons. A second common error is the assumption that Regular Warfare can be conducted only by state armies, whereas Irregular Warfare can be conducted only by non-state organisations. From this belief stems the erroneous concept that Hybrid Warfare is therefore the conduct of Regular Warfare by non-state organisations. This error is a result of focusing only on the legal definition of what is war and who is legally allowed to conduct war rather than focusing on the actual practice of war. It must be reiterated that state armies have and can employ Irregular Warfare and that non-state organisations have and can employ Regular Warfare. Not the type of political or military organisation defines the type of warfare, but the methods employed by whichever type of organisation, as one of the developers of the concept of Hybrid Warfare wrote: "Hybrid Wars can be conducted by both states and a variety of non-state actors. Hybrid Wars 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."[7] Furthermore, the weapon systems employed do not determine whether an operation is being

[7] Hoffman 2007: 29; Hoffman 2009.

conducted by Regular, Hybrid or Irregular methods, though some weapon systems are used more typically in Regular Warfare whereas others are more typical to Irregular Warfare.

## Criteria for conducting a Hybrid Warfare military strategy

The combination of methods is measured by four criteria:

1. Sector – the combination can be employed in the same sector or in different sectors that are operationally linked so that the actions in one directly affect the actions in the other.
2. Time – the combination can be employed simultaneously or sequentially.
3. Force – the combination can be employed by the same force, whether regular or irregular, or by separate forces acting in concert – both regular, both irregular, or one regular and one irregular.
4. Mission – Hybrid Warfare can be conducted in four basic combinations between Offensive and Defensive missions[8] such as Offensive Regular Warfare and Offensive Irregular Warfare; Defensive Regular Warfare and Offensive Irregular Warfare; Defensive Regular Warfare and Defensive Irregular Warfare; Offensive Regular Warfare and Defensive Irregular Warfare.

Slightly preceding the development of the concept of Hybrid Warfare in the United States Marine Corps a similar concept under a different name, Compound Warfare, was developed by academic researchers in the United States Army. Part of the debate on Hybrid Warfare in the American military was an attempt to

[8] Offensive: Forces conduct operations in territory currently physically controlled by the enemy in order to change the existing political and/or military status quo. Defensive: Forces conduct operations in territory currently physically controlled by them in order to maintain the existing status political and/or military status quo. “Physically controlled” does not mean political ownership. If a military force invades the territory of a rival political entity and conquers territory, then for military purposes that territory is now physically controlled by the invading army – its actions to retain that territory constitute defensive operations and the original political entity’s military actions to ‘liberate’ that territory constitute offensive operations. Furthermore, physical control may be absolute (there is no enemy force left in the area and the invading force is physically present in all of it), partial (there is no enemy force left in the area, but the invading force is not physically present in all of it) or in contention (enemy forces are still fighting in some of the area).

differentiate between these two concepts – were they merely different names for a similar idea or two separate phenomena? According to Hoffman, the leading proponent of the initial Hybrid Warfare concept, the two concepts differ in one central aspect: whereas Compound Warfare is defined as a combined effort by separate forces, one specialising in the conduct of Regular Warfare and the other specialising in the conduct of Irregular Warfare, Hybrid Warfare is the conduct by the same force of both Regular Warfare and Irregular Warfare.[9] However, a Finnish officer, Petri Huovinen, who compared the writing on the two concepts as well as the concept of 'Full Spectrum Operations' developed by the United States army at that time, concluded that in fact Hybrid Warfare was a subset of Compound Warfare and that both were included in the concept of Full Spectrum Warfare.[10] He further argued that Compound Warfare was more useful a concept at the operational level,[11] whereas Hybrid Warfare is better used at the tactical level. A Military Strategy based on the concept of Hybrid Warfare refers to the combining of Regular Warfare and Irregular Warfare methods in the same Operations and Battles to directly support each other in achieving the same campaign, operational or tactical objective, whether by the same unit or by different units, in the same or adjacent sectors of action, simultaneously or sequentially.

## Why Hybrid Warfare?

Each form of warfare has different characteristics and therefore the strategist must choose the form most useful to him in a given operational situation. Regular Warfare is, by its nature, more intensive than Irregular Warfare – more forces are employed simultaneously in the same geographic location. Therefore, employing offensive Regular Warfare methods can achieve a more rapid and a more decisive operational result than employing offensive Irregular Warfare methods. However, they generally require the attacker to be superior in quantity or quality or both. Regular Warfare is also usually more expensive in friendly casualties and

[9] Hoffman 2009.

[10] Huovinen 2011.

[11] Huovinen uses the term "strategic level", but from his description of what this entails he actually means what NATO terms the 'operational level': "The level at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations." *NATO Glossary of Terms and Definitions AAP-06* 2013: 2-O-3.

expenditure of resources than Irregular Warfare. Conversely, though they take longer to achieve a final operational result and that result is rarely physically decisive – enemy casualties will be few and inflicted over a long period of time, Irregular Warfare can be conducted successfully even with forces inferior in quantity and quality – whereas successfully operating against them requires at least superior quantity. Irregular Warfare does cause some physical damage to the enemy, but its main goal is a gradual psychological disruption of the enemy's will to fight and belief in his ability to win – not the number of enemy casualties is the defining issue, but the cumulative psychological effect of those casualties. Many casualties inflicted in a very short period of time are usually less detrimental to the enemy's psychological stability than a continuous stream of fewer casualties inflicted over a long period of time, because psychological pressures take time to affect people. In the first case – a heavy price has been paid, but the conflict is over – there is hope for a better future; whereas in the second case – one sees no end to the conflict and gradually loses hope. The object of Hybrid Warfare is to combine the advantages of Regular Warfare and Irregular Warfare – disrupting the enemy's psychology and organisation to facilitate his physical destruction or eviction from a particular territory. It is, however, more complicated to command and conduct efficiently and effectively. Whether fighting against a hostile force employing only Regular Warfare or against a hostile force conducting only Irregular Warfare, an adversary generally wishes to concentrate his forces in space and time to achieve a ratio of forces sufficient to defeat that hostile force. However, Regular Warfare normally occurs along the front line between the rival armies, whereas Irregular Warfare normally occurs in the rear area of an army. So, fighting against a Regular Warfare threat requires the adversary to concentrate his forces at the front, facing the hostile forces conducting those Regular Warfare operations; whereas fighting against Irregular Warfare requires him to allocate forces to his rear areas in order to protect his logistics, headquarters and operational reserve units from being raided. Thus, when fighting a hostile force simultaneously conducting both Regular Warfare and Irregular Warfare actions the adversary is compelled to divide his forces to simultaneously conduct geographically separate operations. Given that Irregular Warfare attacks are scattered spatially and temporally so that the adversary does not know in advance where and when he will be attacked, he is compelled to disperse his own forces into many small units to simultaneously and continuously defend many different sites. Thus, to successfully counter even small Irregular Warfare offensive actions requires a very large force. Therefore, focusing on protecting his rear compels the adversary to drastically reduce the forces he allocates to conduct Regular Warfare operations at the front, thus enabling his rival to achieve numerical superiority there. Conversely, to maintain a force at the front big enough to successfully defeat the hostile force's Regular Warfare operations, the adversary must reduce the forces protecting his rear and accept the consequences of enemy Irregular Warfare operations against his logistics, headquarters and operational reserves disrupting the flow of supplies, information, orders and reinforcements required to maintain his Regular Warfare operations. These will be delayed, will arrive in fragments and will be reduced in total quantity and quality. Though the concept of Hybrid Warfare assumes a rough parity between the Regular Warfare and Irregular Warfare actions, the main effort is usually one or the other, with the opposite type employed to support it. The effect of employing Hybrid Warfare against an adversary is that it increases the variety of methods threatening that adversary and thus creates for him an operational dilemma on the best methods to counteract them and in balancing the efforts of his forces between the counter methods.

## Effects of political Hybrid Warfare on military strategy

According to Clausewitz: "War is the continuation of the political intercourse with the addition of other means."[12] Thus, all conflicts can be conducted by a variety of means to achieve the desired results from negotiations (diplomacy), adversarial activities that attempt to compel and influence the adversary (lawfare, psychological Warfare) through various levels of hostile actions that do not include actual violence (economic warfare, cyber warfare – short of actually creating irreparable physical damage and human casualties) to attempt to compel the adversary through to violent military operations at various levels of intensity (very low to high) in order to defeat the enemy and dictate terms.

In this context Hybrid Warfare is the mix of non-violent methods with violent methods. The exact mix of the means chosen to be employed by the political leadership affects the objectives, resources, constraints and methods allocated to each of the means. For military strategy this determines the military objectives which the politicians and strategists estimate will compel the enemy into

[12] Clausewitz 1989: 87.

giving-in to the political demands; the extent of damage to be inflicted on the enemy (casualties, territory taken, infrastructure destroyed, etc.); restrictions on the types of damage; and the extent and intensity of the military operations employed to inflict that damage. These are calculated to assist or enhance the other non-military means employed. Thus, if the political leaders assess that they can convince the hostile population to accept their demand through a campaign focused on economic and diplomatic incentives, they are likely to reduce the emphasis on destroying enemy personnel and infrastructure – especially those the destruction of which is likely to arouse anger in the enemy population. Theoretically, the mix of non-violent and violent operations chosen can also affect the organisation of the military force. However, often that force is a given, developed over many years and the strategists must therefore either employ the existing organisation or decide many years in advance what type of military force they will need in the future and build that force from scratch or transform the existing force accordingly. However, as argued by William Nemeth – the organisation and characteristics of a military force are determined by the culture and political organisation of the society establishing and maintaining that force.[13] Therefore, often the culture and political organisation determine also the methods in which a particular society will automatically choose to conduct warfare, regardless of theoretical debates on how a war should be conducted.

## Conclusion

On the purely military level a Hybrid Warfare operation is one that combines Regular Warfare actions (essentially the employment of large forces concentrated in time and space to destroy the enemy or to capture or retain ground) with Irregular Warfare actions (essentially actions that are conducted by small separate units 'hitting and running' to harass the enemy rather than to destroy him or capture or retain ground). Past experience shows that both state and non-state armies and both regular armies (i.e. armies organised and manned permanently) and irregular armies (i.e. armies based on an improvised organisation manned by short-term volunteers) have employed Hybrid Warfare.

[13] Nemeth 2002.

The hybridity was achieved by organising separate units each specialising in either Regular Warfare or Irregular Warfare or by training the same unit to conduct both. In some cases, the Hybrid Warfare operation included Regular Warfare actions in one sector while Irregular Warfare actions were simultaneously conducted in an adjacent sector, whether side-by-side or Regular Warfare at the front and Irregular Warfare behind the enemy's front. What converted them from separate actions to a single Hybrid Warfare operation was the direct effect each had on the other. In other cases, the mix was conducted sequentially in the same sector. In some cases, the Hybrid Warfare actions were all offensive or all defensive in nature, while in others an adversary conducted Regular Warfare defensively and Irregular Warfare offensively or vice versa. In some cases, both sides conducted Hybrid Warfare operations, though not in the exact same mix, in others only one side conducted Hybrid Warfare operations and the adversary responded with only Regular Warfare or only Irregular Warfare operations. In some cases, Hybrid Warfare was conducted solely at the military level, whereas in others the political level conducted Hybrid Warfare and the military strategy was either the major or the minor effort in this political strategy. Military strategy is always a tool of the political level, but when the political level is conducting Hybrid Warfare, the impact is greater, constraining the freedom of action of the military forces.

## Questions

1. What are the advantages and disadvantages of a Hybrid Warfare strategy in various political contexts?
2. What are the advantages and disadvantages of a Hybrid Warfare strategy in various military contexts?
3. What are the requirements in force structure and organisation to conduct a Hybrid Warfare strategy?
4. What are the requirements in force training to conduct a Hybrid Warfare strategy?
5. What are the considerations for choosing a particular measure of hybridity in a specific situation?

## References

Clausewitz, Carl von (1989): *On War.* Princeton: Princeton University Press.

*Department of Defense Dictionary of Military and Associated Terms* (2018).

Hecht, Eado (2024): Defining Hybrid Warfare. In Jobbágy, Zoltán – Zsigmond, Edina (eds.): *Hybrid Warfare Reference Curriculum. Volume I. Compulsory Lectures.* Budapest, Ludovika University Press, 31–49.

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

Hoffman, Frank (2009): Hybrid vs. Compound War. The Janus Choice: Defining Today's Multifaceted Conflict. *Armed Forces Journal,* 1 October 2009. Online: http://armedforcesjournal.com/hybrid-vs-compound-war/

Huovinen, Petri (2011): *Hybrid Warfare – Just a Twist of Compound Warfare? Views on Warfare from the United States Armed Forces Perspective.* Helsinki: National Defence University. Online: https://core.ac.uk/download/39944364.pdf

*Irregular Warfare (IW) Joint Operating Concept (JOC)* (2007). Online: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf

*NATO Glossary of Terms and Definitions AAP-06* (2013). Online: https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

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

Bálint Somkuti – András Edl[1]

# China's Methods and Other Potential Hybrid Adversaries

Hybrid warfare has become a buzzword ever since it came into existence following the lightning-fast Russian occupation of the Crimean Peninsula. History shows that words getting a new meaning are usually a clear sign of a transformation. When 'asymmetry' became a similar, widely used term after the collapse of the Saddam Hussein regime and the uprising against the American dominated Coalition Provisional Authority many experts raised their voices. Because the asymmetry of forces is a natural phenomenon of military conflicts. Yet hybrid warfare has stuck and seems to remain with us, at least until a new buzzword ends its trajectory the way asymmetry has mostly vanished from military theoretical scientific publications. The authors of the chapter think that lacking any better, or to be more precise more advertised term, we are stuck with hybrid "warfare" to describe the complex interest advancement in the globalised world. Be it DIME (diplomacy, information, military, economy) as defined by General Phillip Breedlove or a war "about omnidirectionality, synchronicity and asymmetry", as Chinese senior colonels Qiao Liang and Wang Xiangsui have put it the common opinion is that this new form of total, yet restricted, very unusual warfare has already become part of the 21st century. As so aptly described by Thucydides, rising powers such as China or Russia must find a way to work around the hegemon's strengths. And as usual even the ubiquitous Clausewitz had a fitting saying about "fashions" in warfare: "Every age had its own kind of war, its own limiting conditions, and its own peculiar preconceptions."[2]

## Definition and critics

The below 2021 description summarises the phenomenon maybe in the shortest possible way: "Hybrid warfare entails an interplay or fusion of conventional as

[1] Ludovika University of Public Service.

[2] Clausewitz 1989: 593.

DOI: https://doi.org/10.36250/01237_04

well as unconventional instruments of power and tools of subversion. These instruments or tools are blended in a synchronised manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects."[3] Another way of nailing this form of interest advancement is by James K. Wither who wrote in his 2020 article: "There are many definitions of hybrid warfare and these definitions continue to evolve. Defining hybrid warfare is not just an academic exercise because these definitions may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them. Historians have used the term hybrid warfare simply to describe the concurrent use of conventional and irregular forces in the same military campaign."[4] Many experts have had issues with the above from the very moment this buzzword has begun its stellar career. One article dared to clearly formulate that we "[…] should forget about everything "hybrid" and focus on the specificity and the interconnectedness of the threats they face. Warfare, whether it be ancient or modern, hybrid or not, is always complex and can hardly be subsumed into a single adjective. Any effective strategy should take this complex environment into account and find ways to navigate it without oversimplifying".[5] Yet the gem of group thinking is the definition of hybrid threats on the homepage of the bureaucracy called European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). It says: "The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means."[6] Let me translate it to plain English. Anything not supportive some actor defined a hostile does. Period. It is like saying we paint using only basic colours. And the variations of them. So, we do nothing special but paint. Using all colours. Because any action in security policy can be either military or non-military. They are either overt or covert. There is no third way. To sum it up anything an adversary – defined as such – does, is hybrid. One could but wonder what were serious scientists thinking when DIME, hybrid warfare and other buzzwords were introduced into security policy discussions. Because all these are nothing new, not a single element of novelty is present when compared to the grand strategy concept by Sir Basil Liddell Hart. Especially when hybrid warfare in its early form

[3] Bilal 2021.

[4] Wither 2019.

[5] Van Puyvelde 2015.

[6] See Hybrid CoE s. a.

was to focus narrowly on occupying territories. In its 2014–2015 version it was nothing but a military operation supported by public administrative and clearly propaganda efforts.[7] Not to mention Mark Galeotti's flop for making up the hybrid warfare's supporting and non-existing "Gerasimov Doctrine". Modern power struggle, or interest advancement encompasses all aspects of life blurring the lines of conflict. It suffices to compare the above very loose definitions with the Foreign Broadcast Information Service translation of the foreword of *Unrestricted Warfare:* "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden." Not to mention that one of the authors of this paper had a very similar definition of modified 4th generation warfare theory: "Fourth generation warfare is an activity aimed at achieving clearly defined political goals. In most cases this activity is carried out through non-military means, by one or more organisations sharing a common ideology. Generally accepted rules about military activities do not confine their methods, which are applied in one or more areas simultaneously in a way that their effects strengthen or enable each other. […] Its subareas are:

- global guerrillas
- information warfare, including cyber warfare
- economic manipulation, financial manoeuvres supported by media
- ideological, human rights and other perception-based operations
- or a combination of the above by state and non-state actors alike"[8]

The usual opinion about Russian hybrid warfare among western experts is that it is practised against the influence of the USA without having to face NATO militaries in a conventional conflict. Its aims to reconquer lost territories, or new ones in addition to sawing discord among NATO countries. "Russian analysts assert that a conflict only rises to the threshold of a hybrid war if the aggressor state explicitly sets reshaping the strategic orientation and "worldview" (ruling ideology) of a target state as its goal."[9] What is more the falsely claimed Gerasimov Doctrine, is in reality a way of defensive thinking a call to arms to raise the policymakers attention to the threat they are facing.[10] In Russian terminology hybrid warfare is not about the means, but a different type of armed

[7] De Benedictis 2022.

[8] Somkuti 2012.

[9] Clark 2020: 16.

[10] Klijn–Yüksel 2019.

conflict category, waged for influence. Deterrence also seems to be one of the most effective tools for Chinese strategists to avoid conflict. However, while in the Western concept the two main pillars for deterrence are "deterrence by denial" and "deterrence by punishment", in the Chinese perception – similar to the Russian one – there is also an active component of coercion. This is also reflected in the Chinese term *weishe* (威慑). It is not just trying to stop an opponent, but actively making him change his behaviour. Furthermore, the Chinese concept of deterrence can involve all the capabilities and full strength of the state, such as economic power, scientific development, or even the country's geographical characteristics.[11] The development of the Chinese military and the change in the means of deterrence has meant that other states have also adapted and tried to develop their own deterrence tools. Taiwan and Japan, for example, are in a similar situation. Both have relied on the United States, and now both are at a quantitative disadvantage vis-à-vis Chinese forces and are therefore forced to seek qualitative superiority. As a consequence, they have gradually developed a limited deterrence strategy designed to prevent China from quickly winning a war. A practically lost war would put the international community in a difficult situation, and make it much harder to gather support for an intervention.[12] The main objective of the Chinese Communist Party is to maintain internal stability.[13] This is even reflected in China's defence policy. The first objective is to deter aggression. But the second batch of objectives are national political security, the security of the people and social stability. This means that the Communist Party of China wants to maintain its leading role and must stand in the way of internal unrest. The third and fourth places are occupied by preventing the separatist aspirations of Taiwan, Tibet and the Uighur-inhabited areas. Then comes maritime navigation and trade, space, electromagnetic and cyberspace defence. In the light of current crises, some objectives may be given greater emphasis, but the overriding objective remains the same: to preserve the CCP's leadership and guarantee the unity of the country.[14] Documents analysing Chinese strategic culture, whether by Western or Eastern authors, often mention the difference between chess and the Chinese game of *weiqi* (围棋), commonly known as *go* after its Japanese name. One possible translation of the term *weiqi*

[11] Cheng 2021.

[12] Bartók 2020.

[13] Scobell et al. 2020.

[14] Ministry of National Defense – The People's Republic of China 2022.

is "encircling chess". This may shed light on the different concept that permeates the game. The main objective is to isolate and encircle the opponent's pieces, or to put him in a position where he has only one possible way out. The ideal outcome is when the opponent is defeated without a real confrontation or battle having taken place. The same idea appears in Sun Tzu's famous book, *The Art of War* (孙子兵法). The biggest flaws in this game are short-term thinking, a petty give-and-take approach and impatience. As the two games are different, Chinese and Western geopolitical thinking have different characteristics, goals and roots. According to some analyses, the Western approach is expansionist and hostile, while the Chinese is more peaceful and based on the principle of border protection.[15] As with *weiqi,* also *shi* (势) is an important element of Chinese strategic thinking. It is extremely difficult to translate, a malleable concept with many shades of meaning. There are up to 14 possible translations, such as force, momentum, energy, advantage, position, opportunity, control, formation. These meanings are not mutually exclusive but form a large cluster of meanings. The term "strategic advantage" is not an incorrect translation, but it still misses a lot. The grasp of *shi* is the ability to recognise a state of affairs influenced by many factors, and to understand the quality of a given situation. Consideration must be given to the weather, geography, the state of allies and adversaries, the political and economic situation, all of which influence the favourable situation from which appropriate action can unfold. Not the action itself, but a state of tension and possibility from which, if necessary, a range of actions can be launched. If only one possible action remains it is considered a defeat, just as in *weiqi.* From a Chinese point of view, one of the rules of engagement with other countries would be to build this favourable *shi.* A third term that often comes up in the analysis of Chinese strategic thinking is *shashoujian* (杀手锏), most often translated as "assassin's mace". These would be the weapons that would take down a much stronger opponent unexpectedly and in one fell swoop, rather than the established rules of conflict, presumably in a prolonged struggle. This does not necessarily mean a particular set of weapons, but rather anything that effectively enhances A2/AD capabilities and can be deployed quickly, with almost no telltale signs, and has deterrent power. A good example is the DF-21D anti-ship missile, which could pose a serious threat to aircraft carriers. However, analysing these concepts is not the right way for everyone and culture should not be given too much weight. For example, even if someone plays a lot of *weiqi,* its moves may not

[15] Horváth 2022.

be converted easily into real-world action. Furthermore, deception, coercion or long-term planning are culture-independent parts of the strategy, and all depend to a large extent on the reactions of the opponent. Whether they are Chinese or Western strategists, everyone is looking for the ideal mix to best impose their will in a given situation. Some argue that the strategic thinking of the two cultures is more similar than different. Thus, focusing on different concepts can be misleading, as it can make the discourse too theoretical and describe not what Chinese strategy *is* in a given situation, but what it *should* be.[16]

## Two kinds of warfare

The theoretical framework for political warfare is provided by the concept of the Three Warfare (*san zhong zhanfa* 三种战法). Whether or not it falls under hybrid warfare is debated, but it can be an effective complement to it. The term itself appeared in the public domain in 2003 when the Central Committee of the Communist Party and the Central Military Commission of the People's Liberation Army designated it as the guideline for political warfare to be followed. This strategy can be broken down into three main branches: public–media warfare (*yulunzhan* 舆论战), psychological warfare (*xinlizhan* 心理战) and legal warfare (*falüzhan* 法律战). These tools serve multiple purposes, such as controlling public opinion, diminishing the enemy's resolve, transforming emotions, psychological control, collapsing the opponent's organisation, psychological protection and restraint by law. These are closely interrelated and are not used exclusively against opponents. The control of public opinion, for example, also applies to China's own population, and state control of the media is indispensable in this. The methods used can be extremely varied and are always adapted to specific circumstances. China, for example, has taken control of the Chinese language media in many places where there is a significant Chinese minority and thus has a strong influence on communication within that community. In other cases, the "borrowed boat" method is used to publish articles in influential Western newspapers such as the Washington Post or the New York Times. These are in fact paid advertisements, but the editorial principles and the prestige of the press products that host them can make it appear to the reader as if it is

[16] Dickey 2017.

an opinion piece or a news report published by the newspaper.[17] In case of legal warfare, they can legislate that disputed territories are part of China and then present the legislation as justification for their action there, either to their own population or to foreign countries. As these tools are classified under the political work of the armed forces, it can be seen that the armed forces must also reckon with these tools and fight conflicts in more than the conventional military sense. Added to this is the new Chinese definition of national security, which now also includes China's development interests so that anything that threatens the country's development can be perceived as a security threat.[18] This broad and rather vague definition is not an accident but is suitable to the competition between states in all fields, where anything can be a weapon. In any case, the strategy of the three wars seems to be effective, and it may be that the methods used have also helped China to be judged more leniently for certain of its actions, or to take the accusations associated with them less seriously. For example, according to some analyses, the reason why Chinese cyber espionage has not received as much attention, and only minimal backlash, is that China has successfully presented itself as a responsible partner in cyberspace while taking advantage of the Snowden case and tarnishing the image of the United States.[19] The notion of hybrid warfare is often associated with General Valery Gerasimov, who in his 2013 article formulated his questions and thoughts on the nature of modern war. But similar questions were raised by an earlier Chinese work, *Unrestricted Warfare* (*chaoxian zhan* 超限战), published in 1999 and written by two generals, Qiao Liang (乔良) and Wang Xiangsui (王湘穗). Since then, Western analysts have been referring to the text and trying to draw the right conclusions. The authors' thinking is mainly similar to the neorealist school, with self-interest as the only constant factor, everything else changes. They believe that war no longer necessarily involves loss of life and that practically any means can be used since conflict takes place simultaneously on all levels, whether economic, cultural, diplomatic or military. A Machiavellian combination of skills is required in each of these areas and at different levels. More importantly, they concluded that the boundary between war and peace has disappeared, there is no sharp distinction.[20] It is worth noting that their writings sparked

[17] Vuving 2019.

[18] Jash 2019.

[19] Iasiello 2016.

[20] Liang–Xiangsui 1999.

controversy within China and, in addition to the academic disputes, offended several interest groups, so the two generals were denied further promotions and their military careers soon ended.[21] Some of the instruments classified under hybrid warfare had already appeared in earlier Chinese military theories. A summary analysis of Chinese sources revealed that Chinese scholars saw the United States as the first user of hybrid warfare and that it only emerged as a problem in American sources after it had been used against them. The Russians only perfected this method. The term grey zone warfare (*huise didai* 灰色地带) is used to describe actions used in a competition that are still below the borderline of conflict. A good example of this is the deployment of Chinese coastguards or fishing fleets in waters of disputed territorial waters and islands. Cyber and information operations can also be included here. Information warfare (*xinxi zhanzheng* 信息战争) is another concept that often appears in Chinese thinking. It is closely related to cyber warfare (*wangluo zhanzheng* 网络战争) but its use encompasses a much narrower area. Information warfare focuses on the acquisition or disposal of information and uses IT tools to do so, while cyber warfare is an umbrella term for everything conducted in the cyber domain.[22] The use of most of the tools that fall under hybrid warfare is not new, but this kind of discourse, the emergence of new concepts and doctrines, and new possibilities offered by technological developments (e.g. cyberspace or social media) or combinations of these, are new. China is trying to shape the discourse, and thus to ensure that its soft power efforts and instruments are not subsumed under the notion of hybrid warfare, which is perceived by Beijing as being of Western origin anyway. Among the principles promoted by China are such classic values as learning from others, harmony and moderation, strong governance, peaceful ascendancy, and the primacy of the community over the interests of the individual. How these ideals are achieved will largely depend on how they are judged by the rest of the world.[23] An often-mentioned hybrid tool is economic pressure. One example of Chinese expansion and manipulative techniques supposed to be the debt trap, which is mainly associated with the building of the One Belt One Road initiative. Under this, loans are given to a country that is unable to repay the loan and is forced to make concessions to China because of its heavy financial dependence. It would be naive to think that the great powers do not use

[21] Behrendt 2022.

[22] Saalman 2021.

[23] Dengg 2021.

economic pressure. However, a closer examination can reveal a different picture. The development of the port of Hambantota in Sri Lanka is often cited as an example, but it can be argued that an already indebted local government, poor project management and corporate economic interests contributed more to the situation than a shadow war directed from Beijing.[24] Another often-mentioned tool is propaganda, which is an integral part of Chinese communication, partly based on the communist tradition, and is not a negative word from a Chinese point of view. The correlation between the different methods is well illustrated by the fact that the initial support for the Chinese space program was so substantial because Mao Zedong expected great propaganda results from it. Nowadays, technical and scientific achievements continue to be used to legitimise the CCP's rule and to boost national pride. This has been so successful that a significant proportion of the population is willing to actively support government efforts out of conviction, even on their own initiative. Individuals may sometimes carry out cyberattacks on their own, while in other cases Beijing may use their capabilities as a hired "irregular cyber force".[25] The term A2/AD – active defence itself is also another western shorthand for a complex Chinese, and what is more interesting, defensive concept. First coined in 2013, when China announced the establishment of an air defence identification zone over the East China Sea. In accordance with the above plan China have started to expand and build military facilities in the South China Sea, within disputed waters, turning reefs, and submerged land features into fully fledged airbases and other military installations. Quite surprisingly the West sees these capabilities as irregular, or hybrid threat. The fact that the installations are built on disputed territories is in itself a clear breach of international law, yet the installations and the Anti-Access–Area Denial means are characterised by the offensive manoeuvre, defensive tactical stance. Given the peculiarities of modern combat operations, the concept relies heavily on information gathering means, and at the same time blocking the adversary from obtaining it. Therefore, the first pillar of the concept consists of information, surveillance, recon and target acquisition methods, as well as ways of actively countering the opponents' similar efforts. In other words, space technology, and Electronic Warfare. Little is known about Chinese anti-satellite or ASAT programme, apart from the occasional official press releases, which may or may not tell the truth about the actual equipment tested.

[24] Eszterhai 2021.

[25] Edl 2022.

Allegedly the vehicle launched SC-19, itself based on an intercontinental ballistic missile is carried ICBM capable Chinese submarines.[26] Directed energy (laser) weapons offer another possibility, and allegedly have been tested on U.S. satellites. Third possible element of such a concept are interceptor, or killer satellites either in the form of kinetic micro satellites or dual use–military satellites made for this purpose. Classic electronic warfare methods, such as jamming, and other electronic countermeasures also enhance this capability. Recent Chinese military doctrines have outlined the importance of balanced and comprehensive capabilities, so based on the development of the native electronic industry one can safely assume that a strong ECM/EW supports the A2/Ad effort. One thing is for sure. In the age of space-based information, communication and navigation making the potential enemy blind and deaf makes U.S. satellites a juicy target, even though President Trump has threatened with serious consequences. Using the gained information, the second pillar focuses at physically preventing the opponent from entering defended area, meaning this area contains mostly rocket weapons. Foremost of these, and at the same time the symbol of A2/AD without a doubt, is Dong Feng DF-21D, ship killer ballistic missile. While precise targeting against 30 knots moving targets at Mach 10 re-entry speeds remains a question, the 600–1,000 kg warhead has enough potential to achieve a mission kill on any warship, including the mighty aircraft carriers, rendering them unable to carry on. Another threatening aspect of A2/AD are shore, ship, or submarine launched supersonic antis-shipping YJ-12 and YJ-18 missiles. Based on the capabilities of the DF-21D, it is difficult to imagine how is the YJ-21 hypersonic anti-ship ballistic missile different, which China have allegedly tested from a Type 055 large destroyer. To counter airborne threats an air defence missile HQ-19 is under development with a never seen before 2,000 km (!) planned range.[27] The primary area of these measures is the South China Sea, especially the so-called "First Island Chain", which consists mostly reefs, and shoals, such as the Spratly and Paracel Islands, and the Scarborough Shoal.[28] But what is more important, Taiwan lays in the centre of this imaginary line overlooking one of the busiest naval trade routes of the world. It is a typical chicken or egg question whether the need to control led to the formulation of A2/AD and other hybrid solutions, or a ready concept was applied to the existing problem.

[26] SC-19 ASAT s. a.

[27] China's Anti-Access Area Denial 2018.

[28] Gady 2019.

Judging from the first appearance of this concept in 2013, the former is more likely. The doctrines and theories have been translated into concrete steps in China's military reform. These include the creation of the Strategic Support Force (*Zhanlue Zhiyuan Budui* 战略支援部队) in 2015. The aim was to bring together the capabilities of the People's Liberation Army to conduct space, cyber, electronic, information, communications and psychological operations. In the same year, the Chinese military was ordered to reach a level of winning an informationised local war (*xinxihua zhanzheng* 信息化战). Gaining the necessary information superiority is impossible without the effective support of the Strategic Support Forces, especially cyber and space capabilities.[29] China's already demonstrated ability to destroy U.S. satellites could act as a deterrent to the U.S. precisely because of the extent of its reliance on space capabilities. The organisation is structured along two main lines. The first is the Space Systems Department (*Hangtian Xitong Bu* 航天系统部) and the second is the Network Systems Department (*Wangluo Xitong Bu* 网络系统), under which all non-space capabilities are ordained. The Space Systems Department is responsible for virtually all space-related activities of the Chinese armed forces, including rocket launches, space observation, all support functions and space warfare.[30] The development of Chinese cyber and space capabilities has been quite spectacular in recent years. The first wake-up call was the anti-satellite (ASAT) test carried out in 2007, and ever since multiple other tests were conducted. The current space capabilities include not only kinetic ASAT weapons but also orbital manoeuvrable interceptor satellites, advanced jamming capabilities or directed energy weapons. The SSF will also play an important role in any pre-emptive strikes that may be required against a technologically more advanced and powerful adversary. One of the main functions of space capabilities will be to identify targets and to assist in the navigation and communication of own forces. Meanwhile, the forces under the Network Systems Division will seek to disrupt the information structures of the adversary based on the principle of network-electronic warfare (*wangdian yitizhan* 网电一 体战).[31] Based on China's assumed capabilities, a space war game conducted in 2021 was built around the Taiwan conflict. The U.S. and its allies won, but the outcome was close. This raised alarms in the Pentagon yet again and gave considerable support for

[29] Office of the Secretary of Defense 2018.

[30] Weeden–Samson 2022.

[31] Kania–Costello 2021.

budgetary requests. The means employed by the two sides during the wargame exercise did not generate another cloud of space junk, but they did make ample use of their cyber capabilities, used lasers to temporarily blind their opponents' satellites and deployed manoeuvring satellites capable of forcing targets out of their orbits. The lessons learned suggest that the United States needs to cooperate much more closely with its allies.[32]

## Reactions to Chinese hybrid methods

The Taiwan issue has long been a challenge for Beijing. After the civil war of 1946–1949, the defeated *Guomindang* (国民党) forces fled to Taiwan and the government still considers itself the successor to the republic proclaimed in 1912, while the People's Republic of China considers the island its province. Beijing envisages reunification by essentially peaceful means. It has been suggested that Taiwan could retain a degree of autonomy on the basis of the "one country, two systems" principle, as Hong Kong and Macao have done. However, the idea of independence, which has periodically gained strength in Taiwanese politics, led to the adoption of a law in 2005 that would give Beijing the right to use military force in the event of a declaration of Taiwanese independence. There is also a strong U.S.–China rivalry in the background. An important element of this is the deliberately vague wording of the Taiwan Relations Act (TRA) of 1979, which allows the sale of defence equipment to Taiwan.[33] Beijing's clear aim is to guarantee its own security and promote its interests, while Washington has the same objective, but interests may clash in certain areas. While the United States is currently seen as the strongest power, China is seen as an emerging power with the potential to become a new hegemon. Politicians and strategists in both countries are raising the question of how to deal with the other. Some call for cooperation, others for confrontation or a mixture of the two. Analysts try to draw on patterns of past events to help them find a solution. One well-known concept is that of the Thucydides trap, proposed by Graham Allison, whereby an emerging, revisionist power clashes with a hegemon, who is interested in maintaining the status quo. Another potential threat is the Kindleberger trap. The essence of this is that while the hegemon can no longer (or only partially) maintain

[32] Sokolski 2021.

[33] Salát 2019.

the world order, the emerging power does not want to participate in maintaining it, but simply uses it for free, like other smaller states do. However, a greater responsibility would presumably mean a greater say, so it is questionable how much the hegemon would support this. Bergsten considers these two potential pitfalls and believes that China cannot be isolated because it is too powerful and dynamic. In addition, isolation is not necessary, because Beijing does not want to subvert the world order, but to revise it, and the right approach would be a "conditional competitive cooperation".[34] Friedberg and others argue that this is simply naive. The reality is quite different, China is led by a ruthless party that wants to retain power and whose leadership believes a confrontation with the United States is inevitable and will do whatever it takes to win. Friedberg believes that the United States needs to close ranks with its allies against China, step up the decoupling of the economy and supply chains, and prepare the military for conflict.[35] This is in line with Pillsbury's view that China is only waiting for the right moment to make its move. It is hiding its forces and real intentions until it is too late for the U.S. to take effective countermeasures.[36] But looking at the phenomena in this way, it is easy to take a paranoid view in which even well-intentioned steps can be seen as a cunning disguise. Current trends suggest that more pessimistic, confrontational voices may predominate. The Chinese official position is that Washington is responsible for the deterioration in relations and that this is largely due to their perception of China's rise and their relative decline in power. However, there have been Chinese voices willing to acknowledge that the U.S. reaction is also largely dependent on China's actions. It is noteworthy that Chinese leaders and scholars in 2021 predicted in unison that the Biden Administration's China policy would not be fundamentally different from the Trump Administration's and would be fundamentally confrontational. This has so far proved to be correct. And although China is becoming increasingly assertive globally, its main interests are strengthening its regional power and influence, reducing its dependence on the United States, strengthening the world's dependence on China and ensuring a peaceful environment for its further development.[37] It is of course a valid question how this Chinese approach differs from the methods that have been used in the past. It can be observed that in the

[34] Bergsten 2022.

[35] Friedberg 2022.

[36] Pillsbury 2016.

[37] Hass 2021.

discourse in the West, the concept of the Chinese hybrid threat is well applied and used to draw attention to the Chinese gains, but also to attribute insidious intentionality. The proposed responses are numerous: supplying arms to Taiwan, diplomatic action, restructuring goals and developing new strategies. The lack of unified leadership and administration is cited by several authors as one of the major obstacles to a successful U.S. response. Somewhat idealistic authors argue that the needs of allies and potential partners should be addressed in a way that maintains a moral and ethical high ground compared to a dishonest China.[38] The countering of the Chinese hybrid threat is also reflected in government documents. The public version of the 2022 National Defense Strategy was not yet available at the time of the submission of this chapter. But it is already known that integrated deterrence is one of the key concepts that appear in the document. The U.S. aims to develop a full-spectrum, all-around deterrence that requires the involvement of allies. Among the various proposals in the discourse around the document, we can find the launching of offensive hybrid operations as the only way to deter China and Russia.[39] From a military point of view, the United States realised the threat posed by China's A2/AD capabilities and the new risks it posed quite early. Even in 2010, the formulating A2/Ad strategy 2010 has already made its way into the Quadrennial Defense Review (QDR). 2014 QDR restated that U.S. military forces need to be able to maintain power projection in anti-access regions, thus maintaining global reach of the U.S. Past U.S. efforts planned to counter China's A2/AD have pressed enhanced joint force cooperation and allied nations cooperation in contested regions, along with more cost-effective air defence system for long range, regional and theatre defence. It was probably not a coincidence that in 2013, the United States deployed a Theater High Altitude Air Defense (THAAD) battery to Guam. Further strengthening its air defence capabilities Patriot/PAC-3 batteries have been permanently deployed to U.S. military bases in Okinawa, further capabilities provided by sea-based assets. Although Aegis system equipped vessels (SM-2, SM-6, ESSM interceptors) provide a layered missile defence, these shipborne systems are not designed to counter large ballistic or cruise missile salvos. Thus, the old saturation attack surfaces again.[40]

[38] Fogel 2022.

[39] Starling et al. 2021.

[40] China's Anti-Access Area Denial 2018.

## Conclusion

Hybrid warfare as such is a buzzword coming to life after the events of 2014, especially the lightning quick occupation of Crimea, and the coming of the "little green men". Yet, this phenomenon so hotly embraced by western experts is nothing but the millennia old grand strategy, where every means of state, including clearly non-military ones such as culture, media and social tools are employed to achieve politico-military goals.

Not surprisingly it was two Chinese senior colonels who first wrote about a new type of warfare which conforms to contemporary international relations, and their book *Unrestricted Warfare* is still the handbook of players looking for unusual solutions. Contrary to Russian understanding of the phenomenon, Chinese see irregular solutions purely as defensive, within a geographically limited area. Economic, legal, diplomatic and other non-military means are used successfully by China to promote is interests. Yet the most famous hybrid warfare method is definitely A2/AD, which in itself is again nothing new, but a classical layered and complex defence.

## Questions

1. What are the main concepts of Chinese strategic culture and why should we be wary of over-examining them?
2. How does the Chinese concept of hybrid warfare differ from Russian ideas? (Does hybrid warfare even exist?)
3. What is the essence of the A2/AD strategy and what are its main tools?
4. What is the role of the different branches of the Strategic Support Forces?
5. How can the U.S. and China be characterised in their confrontation?

## References

Bartók, András (2020): Az „Első szigetlánc" hullámtörői – rendszerszintű hasonlóságok Japán és Tajvan korlátozott elrettentés stratégiáiban [Breakwaters of the "First Island Chain" – Structural Similarities in Japan and Taiwan's Limited Deterrence Strategies]. *Hadtudomány,* 30(4), 31–46. Online: http://doi.org/10.17047/HADTUD.2020.30.4.31

Behrendt, Paweł (2022): *San Zhong Zhanfa or Three Warfares. Chinese Hybrid Warfare.* Online: https://instytutboyma.org/en/san-zhong-zhanfa-or-three-warfares-chinese-hybrid-warfare/

Bergsten, Fred C. (2022): *The United States vs. China. The Quest for Global Economic Leadership.* Cambridge: Polity Press.

Bilal, Arsalan (2021): *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote.* Online: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Cheng, Dean (2021): An Overview of Chinese Thinking about Deterrence. In Osinga, Frans – Sweijs, Tim (eds.): *NL ARMS Netherlands Annual Review of Military Studies 2020. Deterrence in the 21st Century – Insights from Theory and Practice.* The Hague: T.M.C. Asser Press, 177–200. Online: https://doi.org/10.1007/978-94-6265-419-8_10

China's Anti-Access Area Denial (2018). Online: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/china/china-anti-access-area-denial/

Clark, Mason (2020): *Russian Hybrid Warfare.* Online: https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

Clausewitz, Carl von (1989): *On War.* Princeton: Princeton University Press.

De Benedictis, Kent (2022): *Russian 'Hybrid Warfare' and the Annexation of Crimea. The Modern Application of Soviet Political Warfare.* London: Bloomsbury Publishing.

Dengg, Anton (2021): China's Narratives in the Context of Hybrid Threats. In Frank, Johann – Vogl, Doris (eds.): *China's Footprint in Strategic Spaces of the European Union.* Vienna: Federal Ministry of Defence, 59–84.

Dickey, Lauren (2017): *Wei Qi or Won't Xi: The Siren Call of Chinese Strategic Culture.* Online: https://thestrategybridge.org/the-bridge/2017/9/26/wei-qi-or-wont-xi-the-siren-calls-of-chinese-strategic-culture

Edl, András (2022): Space Program and Propaganda in the People's Republic of China. In Doma, Petra – Takó, Ferenc (eds.): *"Near and Far" 10/1. Proceedings of the Annual Conference of ELTE Eötvös Collegium Oriental and East Asian Studies Workshop.* Budapest: Eötvös Collegium, 131–144. Online: https://eotvos.elte.hu/media/fa/e8/5823639a75240a258593bb18e75d44405149a287c5b8323bbf48d760e4c7/ec_Kozel_s_Tavol_X_06_06.pdf

Eszterhai, Viktor (2021): *Srí Lanka esete a kínai adósságcsapda-diplomáciával – mítosz és valóság* [The Case of Sri Lanka with Chinese Debt-Trap Diplomacy – Myth and Reality]. Online: http://real.mtak.hu/123686/1/10.KKIElemzesek.E-2021.10_SriLanka_Eszterhai_20210331.pdf

Fogel, David L. (2022): *I Helped Defend against China's Economic Hybrid War. Here's How the US Can Respond.* Online: https://www.atlanticcouncil.org/blogs/new-atlanticist/i-helped-defend-against-chinas-economic-hybrid-war-heres-how-the-us-can-respond/

Friedberg, Aaron L. (2022): *Getting China Wrong.* Cambridge: Polity Press.

Gady, Franz-Stefan (2019): Why China's Military Wants to Control These 2 Waterways in East Asia. *The Diplomat,* 15 September 2019. Online: https://thediplomat.com/2019/09/why-chinas-military-wants-to-control-these-2-waterways-in-east-asia/

Hass, Ryan (2021): *How China Is Responding to Escalating Strategic Competition with the US.* Online: https://www.brookings.edu/articles/how-china-is-responding-to-escalating-strategic-competition-with-the-us/

Horváth, Levente (2022): *A kínai geopolitikai gondolkodás. „Egy övezet egy út" kínai szemszögből.* Budapest: Pallas Athéné Könyvkiadó.

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

Iasiello, Emilio (2016): China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities. *Journal of Strategic Security,* 9(2), 47–71. Online: https://doi.org/10.5038/1944-0472.9.2.1489

Jash, Amrita (2019): *Fight and Win Without Waging a War: How China Fights Hybrid Warfare.* Online: https://www.claws.in/static/Amrita-Jash.pdf

Kania, Elsa B. – Costello, John K. (2021): Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies,* 44(2), 105–121.

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

Liang, Qiao – Xiangsui, Wang (1999): *Unrestricted Warfare. China's Master Plan to Destroy America.* Beijing: PLA Literature and Arts Publishing House.

Ministry of National Defense – The People's Republic of China (2022): Defense Policy. *Ministry of National Defense of the PRC,* 1 January 2022. Online: http://eng.mod.gov.cn/defense-policy/index.htm

Office of the Secretary of Defense (2018): *Military and Security Developments Involving the People's Republic of China.* Online: https://media.defense.gov/2018/aug/16/2001955282/-1/-1/1/2018-china-military-power-report.pdf

Pillsbury, Michael (2016): *The Hundred-Year Marathon. China's Secret Strategy to Replace America as the Global Superpower.* New York: St. Martin's Griffin.

Saalman, Lora (2021): China and Its Hybrid Warfare Spectrum. In Weissmann, Mikael – Nilsson, Niklas – Palmertz, Björn – Thunholm, Per (eds.): *Hybrid Warfare. Security and Asymmetric Conflict in International Relations.* London: I. B. Tauris, 95–112. Online: https://doi.org/10.5040/9781788317795

Salát, Gergely (2019): *Kína biztonsági problémái.* Online: https://www.academia.edu/39962458/K%C3%ADna_biztons%C3%A1gi_probl%C3%A9m%C3%A1i_

SC-19 ASAT (s. a.). Online: https://www.globalsecurity.org/space/world/china/sc-19-asat.htm

Scobell, Andrew – Burke, Edmund J. – Cooper, Cortez A. III – Lilly, Sale – Ohlandt, Chad J. R. – Warner, Eric – Williams, J. D. (2020): *China's Grand Strategy. Trends, Trajectories, and Long-Term Competition.* Santa Monica: RAND.

Sokolski, Henry ed. (2021): *China Waging War in Space: An After-Action Report.* Online: https://npolicy.org/wp-content/uploads/2021/08/2104-China-Space-Wargame-Report.pdf

Somkuti, Bálint (2012): *A negyedik generációs hadviselés: az érdekérvényesítés új lehetőségei* [Fourth Generation Warfare: New Possibilities for Advocacy]. Doctoral Dissertation. Budapest: National University of Public Service.

Starling, Clementine G. – Wetzel, Tyson – Trotti, Christina (2021): *Seizing the Advantage: A Vision for the Next US National Defense Strategy.* Online: https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/seizing-the-advantage-a-vision-for-the-next-us-national-defense—strategy/

Van Puyvelde, Damien (2015): *Hybrid War – Does It Even Exist?* Online: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

Vuving, Alexander (2019): China's Strategic Messaging: What It Is, How It Works, and How to Respond to It. In McDonald, Scott D. – Burgoyne, Michael C. (eds.): *China's Global Influence. Perspectives and Recommendations.* Honolulu: Asia-Pacific Center for Security Studies, 160–173.

Weeden, Brian – Samson, Victoria eds. (2022): *Global Counterspace Capabilities. An Open Source Assessment.* Online: https://swfound.org/media/207350/swf_global_counterspace_capabilities_2022_rev2.pdf

Wither, James K. (2019): Defining Hybrid Warfare. *Per Concordiam,* 10(1), 7–9. Online: https://perconcordiam.com/defining-hybrid-warfare/

Andrea Beccaro – Enrico Spinello[1]

# Different Regional Theatres

This chapter aims to contextualise the notion of hybrid warfare in three regional theatres. Different political, economic and strategic contexts offer to state and non-state actors peculiar ways to employ "hybrid warfare" tools; as a consequence, this chapter intends to take into account case studies in order to highlight: how the specific context impacts on the hybrid warfare notion; how various actors can use different approaches; how hybrid warfare changes in different strategic environments. In the academic literature, hybrid warfare is a rather nebulous term, therefore, in this chapter we will use the two most common meanings of the notion of hybrid warfare: as a way to describe modern irregular groups and their method of fighting; a concept used to describe Russian operations during and after the conquest of Crimea in 2014.

## Middle East: The Islamic State Case

In the section that follows, the case study of the Islamic State (ISIS) is presented as a good example of hybrid warfare. In this context, hybrid warfare describes a modern and technological insurgency, i.e. a modern conceptualisation of the notion of "irregular conflict", that is a conflict in which at least one actor is not a State. Consequently, hybrid warfare can be understood as a synonym of guerrilla warfare, low intensity conflict and similar concepts. In this context, the notion was first used and defined by Frank Hoffman and according to his ideas, hybrid warfare is based on four key elements. First, regular and irregular elements become blurred into the same force in the same battle space, even though the irregular component becomes operationally decisive.[2] As far as ISIS is concerned, this feature is evident looking at its operation in Iraq and Syria where it has used conventional infantry tactics in several occasions. During 2015 Spring, ISIS tried to conquer the city of Ramadi, in May it finally was able to

[1] University of Turin.

[2] Hoffman 2007.

DOI: https://doi.org/10.36250/01237_05

do it employing a coordinated attack. The first round of the attack was composed of a bulldozer followed by several large cargo and dump trucks that were crawling toward the heavily barricaded Iraqi checkpoints. Iraqi Security Forces did not have any anti-tank weapons but only machine guns and rifles that were useless against the ISIS vehicles armoured by steel plates. Therefore, the bulldozer began to remove the concrete barriers that blocked the road until it was clear. When a breach was created, the trucks began to pour through. These trucks were vehicle-borne bombs that was another ISIS speciality, a very effective weapon using a technology remarkably simple. When the trucks reached their target, its suicide bomber drivers detonated the payload producing two results: it destroyed the Iraqi defensive positions and shocked who were not killed. So, the suicide trucks were used as a Precision Guided Munition and of artillery fire in conventional Western way of war.[3] Thereafter, ISIS foot soldiers assaulted the Iraqi defence positions and conquered the city. Therefore, in this occasion ISIS developed a coordinated attack using "artillery" and "infantry" to achieve the desired results. During the battle of Mosul in 2017, ISIS was able, even though it lost the battle at the end, to fight a conventional urban battle against Iraqi forces supported by Kurdish militias and U.S. special forces and airpower. The battle of Mosul lasted as long as the battle of Verdun during the First World War and demonstrated the ability of ISIS to slow down the Iraqi advance and produce a very costly battle. Similar situations were repeated in other cities like Ramadi, Raqqa in Syria and Sirte in Libya. Moreover, ISIS in other battles used artillery fire to pound enemy defensive positions or to support infantry units, used tanks and other military equipment seized from the Iraqi Army. In this context, it is also fair to say that ISIS, and other non-state actors in the Middle East like Hezbollah, Hamas and other Shia militias in Iraq, are increasingly using modern weapons such as MANPADS.[4] The second element of hybrid warfare is that terrorism becomes the main fighting method. This is certainly true for ISIS because terrorist tactics are easier and cheaper to use than more conventional ones. ISIS has relayed on terrorist tactics in cities where it had not the control of terrain, but it also used terrorism as a tactic to terrorise the local population in order to gain its support, as it did, for instance, in Mosul during the months and weeks before the conquest of the city. However, ISIS is not a true terrorist group because 'pure' terrorist groups do not hold terrain as ISIS did in Iraq and

[3] Ollivant 2016.

[4] Vinson–Caldwell 2016.

Syria and elsewhere. This control of terrain and its ability to boast some 30,000 fighters can better define ISIS as an insurgent group. Furthermore, ISIS has a "transnational nature" that explains both its use of terrorism, because it is a perfect stand-off tactics to cross national borders and strike targets that are not in the main theatre of operations; and the way in which it controlled terrain using ideology and people who shared the same understanding of Islam. The third element of hybrid groups is their use of modern technology "to avoid predictability and seek advantage in unexpected ways and ruthless modes of attack".[5] ISIS has used technology in several different ways. First, it has used modern media and social media to broadcast its propaganda. We can divide ISIS video propaganda into two different types. Soft propaganda that targeted people who already supported the group, or were already sympathetic to the group, and aimed to show how good ISIS was in organising the life inside the Caliphate. The goal was to convince people to move to Iraq and Syria, live under the ISIS rule with their family and fight for it. Hard propaganda composed of the most violent and brutal videos of killing prisoners, beheaded westerners and so on, the goal of which was to terrorise both local and Western population and security forces in order to soften their ability to resist. Second, it uses modern weapons, or it has created–modified its own. Mainly in Syria and Iraq it has used chlorine gas, it has manufactured its own tele-operated sniper rifles and submachine guns. Moreover, during the battle of Mosul in Iraq, ISIS has widely used drones in offensive operations. Finally, the fourth element of hybrid warfare is related to the battle space because hybrid war, like every irregular war, takes place in complex terrain, most likely the burgeoning cities of the developing world. The most recent and important battles against ISIS were all fought in an urban environment. Among the most recent examples, not only related to ISIS, are: Aleppo, Syria, 19 July 2012 to 22 December 2016; Ghouta, Syria, 7 April 2013 to 14 April 2018; Deir ez-Zor, Syria, 14 July 2014 to 10 September 2017; Ilovaisk, Ukraine, 7 August 2014 to 2 September 2014; Kobani, Syria, 13 September 2014 to 26 January 2015; Debal'tseve, Ukraine, 14 January 2015 to 20 February 2015; Ramadi, Iraq, 11 August 2015 to 9 February 2016; Sirte, Libya, 12 May to 6 December 2016; Fallujah, Iraq, 22 May 2016 to 29 June 2016; Mosul, Iraq, 16 October 2016 to 20 July 2017; Raqqa, Syria, 6 November 2016 to 17 October 2017; Marawi, Philippines, 23 May 2017 to 23 October 2017; Tal Afar, Iraq, 20 August 2017 to 2 September 2017. ISIS is a "hybrid" threat because

[5] Hoffman 2007.

in Iraq, in Syria, in Libya and in Egypt it has used both modern advanced weapons, such as armoured vehicles, tanks, missiles, drones, artillery and conventional-like infantry tactics and terrorism, and guerrilla warfare. It has also used suicide attackers and suicide vehicle borne IED as a kind of cruise missile able to strike precisely the desired target. Reading the problem of suicide attacks in this light, Bunker and Sullivan underline two features of the tactics included even in the Revolution in Military Affairs (RMA) concept of stand-off weapons. First of all, the suicide fighter is invisible to the defender who reckons that they are under attack only when the explosion has occurred. In this way the suicide attack is a surprise attack and represents the most important tactics in an irregular war. Secondly, suicide bombings could be absolutely precise, enabling the attacker to hit difficult and well protected targets, and they are flexible enough to change target or attack procedure if necessary.[6] Another common feature between modern weapon systems and suicide bombing is the ability to project force. Cruise missiles, aircraft like B2 and so on were designed to penetrate in-depth into enemy territory due to their "invisibility", a suicide fighter can carry out the same deep penetration, albeit with less destructive power, allowing the militias to strike in territories which are far beyond the recognised battlefield. According to Lewis, suicide bombing is not simply a metaphor of technology, it is a kind of technology: "In this light, suicide bombing appears as a technological solution to a practical problem."[7] While the United States, in particular, have spent billions and billions on technological research and innovation, militias use what they have in a new and unexpected way. Moreover, while the United States installs in their bombs or missiles devices able to guide them precisely to the target, ISIS and other militias, who have not the same technology, money and research possibilities, have used a "human device" for the same purpose.[8]

## MENA region: The Russian operations

The notion of hybrid warfare has also been used in a completely different strategic context compared to the previous one focused on non-state actors, militias,

[6] Bunker–Sullivan 2004.

[7] Lewis 2007.

[8] For an in-depth analysis see Bertolotti–Beccaro 2015.

the role of terrorism and so on in order to describe recent Russian military operations. In this sense, the notion of hybrid warfare was "originally introduced by NATO's Allied Command Transformation as part of planning for out of area activities" and then it "gained a foothold in NATO Headquarters in mid-2014 as 'the Russian hybrid model in Ukraine' became a means of explaining operations that did not fit neatly into NATO's operational concepts".[9] However, understood in this way hybrid warfare can hardly be considered a doctrine for Russia's power projection.[10] This is evident looking at Russian operations in Syria and then in Africa. Traditionally,[11] Moscow perceived Syria and the Middle East to be part of its extended neighbourhood, and Syria has been Moscow's closest Arab ally since the Cold War.[12] It is true that Russia's influence on Syrian policy has been, and is currently, limited; however, the two countries have developed a strong political, economic and military relationship since the 1950s. Moreover, Moscow has viewed Damascus as a potential foothold in the Eastern Mediterranean, with its warm water ports at Tartus. Although the relevance of this military base can be questioned since the fleet's dismissal in 1991, it was the only Mediterranean base that Russian vessels may have used. In addition to its military base and its geopolitical role, while Syria is not the most important economic partner, it has always been an important one for Russia.[13] Moscow has always supported Assad politically and diplomatically. Russia played a key role in 2012, reaching an agreement with the United States regarding the destruction of Syria's chemical arsenal. However, Russia's goal in Syria has never been to "win the war" for Assad; instead, it has been to preserve the pro-Russian Syrian state system. Consequently, Moscow strengthened its military presence, fortifying its air base in Hmeimim and its naval base in Tartus, and intensifying cooperation with Iran-backed Shiite ground troops in an attempt to cleanse Syria's key areas of anti-Assad opposition. The Russian military presence in Syria has improved not only the fighting effectiveness of the Syrian Army and paramilitary units but also, and probably most importantly for Moscow, Assad's negotiating position with rebel groups.[14] In the MENA region, Moscow is seeking to deny NATO

[9] Giles 2016: 8.

[10] Kofman–Rojansky 2015.

[11] Beccaro 2021.

[12] Vasiliev 2018.

[13] Kozhanov 2013.

[14] Souleimanov–Dzutsati 2018.

freedom of movement and impede the United States' success in playing the role of regional hegemon. Consequently, Russia first reinforced the Black Sea Fleet to use it as a platform for denying NATO access to Ukraine and the Caucasus, and to serve as a platform for power projection into the Mediterranean and Middle East. Studying modern American military operations, Russia has inferred that one way to hinder, or even to negate American military superiority, is to create an environment where American air power cannot operate, or cannot operate freely, and thus an environment where the United States Air Force cannot use all of its arsenal in an uncontested way. In order to achieve this goal, an A2/AD strategy, i.e. Anti-Access Area Denial, has to be developed. The goal of this concept is to prevent an opponent from entering into theatre (Anti-Access) by means of long-range weapons, and deprive it of freedom of action in the theatre (Area Denial) by means of shorter-range tools. To carry out A2/AD tasks, the entire range of missiles is used, including surface-to-air missiles (SAM), anti-ship ballistic missiles (ASBM), anti-ship cruise missiles (ASCM), mines or drones. Russia has been increasingly using the A2/AD measures, and Syria is now part of Russia's defence system. The western Russian flank is now completely closed to Western air forces because Russia has altered the security balance in the Black Sea, Eastern Mediterranean and Middle East by establishing large Anti-Access Area Denial exclusion zones, while the north section of the flank had been an exclusion zone for years. Russia operates advanced air defence not only within its own territory but also from sites in Syria and Crimea, as well as cooperatively through the Joint Air Defence Network in Belarus and Armenia. This use of modern military weapons, air power, the creation of A2/AD bubbles and so on are the most clear and straightforward examples of conventional military approach. Russian military operations in Syria were mainly based on the airpower and this is a novelty in the context of Russian military approach, but it is not hybrid. Moreover, in Syria, despite various technical setbacks, Russia tested modern weapons, such as the new attack helicopter Mil Mi-28, used its only aircraft carrier, which was a novelty in Russian military operations, fired ballistic and cruise missiles from sea and Russian territory, and used its Special Operations Forces (SOFs) in their classic role of training and support forces to local allies. Russia used almost its entire conventional arsenal because Syria was a testing ground for new weapons and to advertise them for sale abroad, and because Russian capabilities had to impress Western audiences and create a sort of deterrence.[15] Furthermore, Chief of Russia's General Staff General Valery Gerasimov stated that the Russian military is acquiring priceless combat experience in Syria because Russian servicemen have been deployed on short tours, in order to maximise exposure to real operating conditions and to "training" under real conditions.[16] Nothing of what we have previously described suggests a new approach to military operations and strategy and lead to use a new label as "hybrid warfare". On the contrary, the Russian approach in Syria emulated the U.S. approach based on stand-off fire, air power, small units on the ground to support local allies. In spite of these findings about the notion of hybrid warfare and Russian operations, the African case study is more consistent with the notion of hybrid warfare. However, it is fair to say that such approach is not new since it is a classic approach of influence, economic and military support that the U.S. and Western countries have extensively used labelling as soft power. Russia's expansion of military, economic and political cooperation with Africa has grown in recent years. For example, Russia signed more than 20 bilateral defence agreements with African countries, increased its trade volume with the continent, and also expanded its media presence.[17] In doing this, Russia capitalised on frustrations with Western policies and skilfully played the anti-colonialism card on the African continent. The result of this Russian growing influence has been the first Russia–Africa summit in 2019. Another sign of Russian leverage in the continent has been the fact that 24 out of the 54 African countries did not support the UN General Assembly resolution in March condemning Russia's invasion of Ukraine. Another important sector that highlights the Russian role in Africa is the military as Russia is the largest supplier of arms to Africa, accounting for 44% of the imports to the region between 2017 and 2021.[18] Compared to the Syria case study, in Africa Moscow has used a completely different approach, far less military and much more economic and diplomatic. These engagements extend from deepening ties in North Africa (Algeria, which is an old and traditional ally since the Cold War; Libya in which Moscow has been able to take advantage of the chaos created by NATO intervention in 2011; Egypt), expanding its reach in the Central African Republic and the Sahel, and rekindling Cold War ties in southern Africa. Moscow typically relies on

[15] Blank 2019.

[16] Giles 2019: 287–288.

[17] Dreyfus 2020.

[18] Wezeman et al. 2022.

irregular and/or extra-legal means to expand its influence: deployment of mercenaries, disinformation, election interference, support for coups, and arms for resources deals. This is a low-cost strategy which can exert a significant influence to advance Russian interests. In contrast with Chinese inroads into the African continent, which have a much larger footprint and consist of visible infrastructure projects, Russia manages to accrue influence more haphazardly by playing to its strength and exploiting Western weaknesses. While the sustainability of Moscow's influence can be doubted, its efforts are proving effective and can be conducted cheaply. One important element of Russian influence in Africa is the rhetoric that support it. Moscow presents itself as a natural ally to African states, one that respects their sovereignty, in contrast to neo-imperialist Western States. Not only this approach has been used in several countries like the Central African Republic (CAR), South Africa, Sudan, Libya, the Democratic Republic of the Congo and Mali, but it also refers to the Soviet Union's legacy of supporting liberation struggles and post-colonial governments. Russia's soft power in Africa is run primarily by a vast net of politico-oligarchic individuals and their networks.[19] This approach has several advantages. First, Russian interests are tied to individuals and their networks and as a result they are resilient to political changes. Generally speaking, the Russian approach is more pragmatic and less ideological than the Western one, so it is not interested in the legal status or democratic legitimacy of its local partners. Second, it provides a veneer of deniability, since Russia's agents act independently, this also allows Moscow to establish networks without straining the administration's budget. An important element of Russian intervention in Africa is related to the use of private military companies. The Kremlin, therefore, has been able to consolidate its strategy and fully capitalise on the advantages inherent in the use of Private Military Companies. By deploying more and more contractors rather than regular troops, Russia has obtained natural resources, minerals, energy, strategic positions. According to Faulkner, the Wagner Group has operated in as many as 28 countries across the globe, but it has become most visible on the African continent, having deployed to at least 18 African states since 2016.[20] The strength of this expansionism lies in offering political leaders complete and economic solutions to stay in power: training and advice to local security forces, counterinsurgency and counterterrorism operations, protection of natural resources and strategic

[19] Orizio 2022.

[20] Faulkner 2022.

infrastructures. In exchange for their services, the Russians obtain mining, energy and other commercial contracts through specially created companies: M-Invest and Meroe Gold in Sudan, EvroPolis in Syria, M-Finans, Lobaye Invest and Sewa Security Services in the Central African Republic and others. Since May 2018, the Wagner Group has supported general Khalifa Haftar and his Libyan National Army – LNA. In addition to training militiamen and arms transfers, Wagner soldiers took part in the failed attempt to conquer Tripoli in September 2019. The Russian contractors also conquered and garrisoned oil fields and infrastructures in the so-called Libyan oil crescent. In the summer of 2020, for example, al-Sharara and Es-Sider ended up in their hands: respectively the most important oil field and the main port oil terminal in the country. In 2017, the Wagner Group was hired by Omar al-Bashir in Sudan to strengthen his regime, training the Army and subsequently participating in the repression of street protests that broke out in December 2018. The Russian military company, through M-Invest and Meroe Gold, would also be in charge of the safety and exploitation of gas, oil and gold fields, as well as prospecting projects for the extraction of uranium in the western part of the country and in the Darfur. These mining concessions by the fifth largest gold producer in Africa would have allowed Moscow to increase its gold reserves, mitigating the effects of Western sanctions. At the end of March 2018, Russian contractors arrived also in the Central African Republic to protect President Faustin-Archange Touadéra and support him in the ongoing ethnic-religious civil war. In addition to training local security forces, Wagner's men helped repel an offensive by the rebel which, after taking control of areas south and west of Bangui, threatened the capital itself. In September 2019, the Wagner Group arrived in Mozambique and at the same time Moscow forgave 95% of Mozambique's debt and proposed a whole series of industrial, commercial and military cooperation agreements. The initial Wagner's assignment was to protect President Filipe Nyusi and support his political position. Wagner's mission then extended to a counterinsurgency operation against Islamic guerrillas who since 2017 have spread death and destruction in the region of Cabo Delgado, rich in important natural gas fields. In Mali, the Wagner Group arrived in December 2021 with the task of training the local Armed Forces, the protection of some political figures and fighting local jihadist groups linked to al-Qaeda.[21] This situation angered Paris which

[21] Orizio 2022.

soon announced the official withdrawal from the country of all its troops by June 2022 along with the forces of a dozen European partners (including the Italian contingent of the Takuba Task Force).

## East Asia: China

Modern international politics has some revisionist powers whose aim is to erode and slightly change the current balance of the international system. Russia is one, but also Iran and China have revisionist goals, even though they are different in scope and possibilities. At least in terms of economy, China and Russia differ profoundly. Russia has a weak and stagnant economy that relays mainly on the energy sector, while China is one of the most important economies of the world. However, China shares with Russia a similar political position because both are revisionist powers, they try to undermine the U.S. position, they both are nuclear powers and member of the UN Security Council. During the last decade, both countries have collaborated in the military sector and done drills together. Nevertheless, the competition between the two is probably a serious obstacle for a closer collaboration in terms of military technology. China can use and has used Gray Zone Warfare tools to improve its political position on several issues. The last example is probably the use of propaganda after the spread of the Coronavirus pandemic. The use of propaganda, information and the Internet is a central tool for each country that has global or regional goals. The Chinese strategic thought is one of the most important traditions in the world, suffice it to mention Sun Tzu and Mao Tze Tung. Soon after the end of the Cold War, two colonels in the People's Liberation Army, Qiao Liang and Wang Xiangsui wrote the book *Unrestricted Warfare*[22] in which they try to explain how a nation such as China can defeat a technologically superior opponent (such as the United States) through a variety of means. Rather than focusing on direct military confrontation, the book instead examines a variety of other means, including the use of International Law and a variety of economic means to place one's opponent in a bad position and circumvent the need for direct military action. The book aims to devise a strategy to fight and win a war against a stronger opponent without using military means, and, therefore, it lists alternative methods that in contemporary world characterised by a rapid and

[22] Liang–Xiangsui 1999.

continuous technology evolution and economic interdependence can have the same destructive force than traditional military warfare. For instance, because of the international nature of the modern world and activism, it is much easier for nation states to effect policy in other nation states through a proxy. Consequently, lawfare or political action through transnational or non-governmental organisations can effect a policy change that would be impossible otherwise. This is the notion of colour revolution that Moscow used some years later and influenced the Russian understanding of 21st international politics. Owing to the interconnected nature of global economics, nations can inflict grievous harm on the economies of other nations without taking any military offensive action, suffice it to mention economic sanctions. This is another element that Russian strategic debate is using to describe current security environment. One of the better-known ideas in the book is that of attacking networks (data exchange, transportation, financial institutions and communication). Attacks that disable networks can easily hamstring large areas of life that are dependent on them for coordination. This is an example of cyberattack and the use of the Internet to harm the enemy without using military force directly. Finally, terrorism erodes a nation's sense of security, even though the direct effects of the attacks only concern a minute percentage of the population. As the Russian strategic debate that sees the Gulf War the turning point in modern warfare and technology as the most important element, the book aims to describe war and international competition in an era of increasing technology evolution. The American strategic debate of those years was focused on how technology has impacted warfare and on the notion of Revolution in Military Affairs. The 1991 Gulf War showed the American technological gap and consequently less advanced armies needed both new tools and new ideas. In this new and highly technological context, information technology plays the most important role: it has radically changed warfare. However, this radical revolution is an underway process that started during the Cold War and will continue in the next decades. According to the authors, even the most modern weapon system is old because it has been made using old conceptions of war. Consequently, in the new context a new approach is needed. As the new weapons are increasingly costly, it is necessary to find cheaper way of attacks, i.e. a new approach to weapons. This means that weapons have to be seen outside the mere military sphere, but have to be seen as a tool that transcend military force. This new way to understand weapons encompasses everything that can be used against the opponent: civil protest, economic measures, information and so on. The battlefield of such conflict is everywhere because it encompasses cyberspace and the Internet and consequently information and propaganda. The actors are not only traditional state and their armies, but also hackers and non-state actors. *Unrestricted Warfare* has several shortcomings; however, it shares interesting elements with the notion of Gray Zone Warfare. First, it describes a holistic approach to strategy that mix military, economic, political, informational elements in one single strategic plan. Second, it breaks down the dividing lines between civilian and military affairs and between peace and war.[23] Third, the adjective "unrestricted" does not refer to a kind of warfare with extreme violence (a kind of nuclear Armageddon), but to the fact that in the 21st century security environment is not limited to military tool, but it encompasses economic, financial, social, political sphere and means. Despite the fact that the book was written by two colonels of the Chinese Armed forces, it should be noted that it did not represent official military doctrine. While China, as Russia, is using GZW tools to improve its political position and developing military tools to counterbalance the U.S. military strength, i.e. A2/AD strategy in the Pacific region, one should be wary of the idea that a future confrontation between China and the U.S. will be a kind of indirect war of rapprochement or proxy war. A more likely scenario is an economic competition, with non-violent subversion, and, if that fails, high-intensity warfare. This because China's greatest strength is its economic might. It is the world's leading trading nation, and uses its global reach to export everything from consumer goods to high-tech tools. The result of this dominance is the Belt and Road Initiative, in which Chinese firms have spent more than $450 billion building infrastructure around the world since 2013. The Belt and Road Initiative highlights the Chinese approach to the international system, because when inducement fails, China does not hesitate to employ coercion and even espionage to achieve desirable trade terms. Moreover, China is willing to exploit asymmetric economic interdependence and economic leverage to force other states to take political and military actions it desires.[24] On the one hand, China is investing in a "Revolution in Military Affairs with Chinese characteristics" developing A2/AD strategy for denying the western Pacific to American forces, in part by making extensive use of guided missiles deployed in a decentralised manner. An important element of this strategy is the artificial island bases that allow China to control the sea and airspace of the South China Sea at the outbreak of hostilities. As a consequence,

[23] Mazarr 2015.

[24] Mattis–Brazil 2019.

the South China Sea is a no-man's land for most U.S. forces (submarines excepted) giving the islands considerable military value for Beijing. However, the aim of the artificial islands is not only to be an element of a conventional military strategy against the United States, but also to use civilian and paramilitary pressure to coerce neighbouring states, making it prohibitively risky for Southeast Asian players to operate in the South China Sea. The threat dissuades neighbouring states from using more forceful military responses against illegal actions and from supporting the U.S. that are not able to provide security. In these artificial islands, and in other islands in the area, China has deployed several fighting jets and this along with the distance from the nearest U.S. base has enabled Beijing to have a full dominance of air space in the region. Considering that China has deployed in these islands anti-ship missiles, anti-aircraft missiles, radar and signals intelligence capabilities, that such facilities are very vast and spread out across a considerable area, they represent an almost insurmountable defence line. They represent both an asymmetric tool since the construction of artificial island to change the geography of the battle space is something surprising and it exploits an adversary weakness; and a major element of a conventional strategy and not hybrid because such islands are part of a conventional approach and confrontation based on aircraft, vessels and missiles. On the other hand, China has proven willing to employ nonviolent subversion worldwide because it considers actions below the threshold of armed conflict (influencing public opinion, legal and psychological warfare) essential to success in future competition. Consequently, China is more likely to employ economic and informational tools to achieve its aims, while focusing on partnerships with state actors and striving to remain below the threshold of armed conflict. As far as the cyber dimension is concerned, "China has developed official military doctrine for cyberwarfare, trained large numbers of military officers to conduct offensive operations on the internet, and conducted an extensive series of exercises and simulations".[25] Moreover, Beijing has done it partially in consultation with Russia.[26] Chinese strategy uses GZW approach because it emphasises the holistic, multi-domain aspects of military confrontations, tightly integrating political, diplomatic, informational and economic elements. Moreover, China tends to favour patient, indirect approaches.

[25] Breen–Geltzer 2011: 48.

[26] Breen–Geltzer 2011: 48.

## Conclusion

In different geopolitical contexts the notion of hybrid warfare assumes different meaning and encompasses different approaches. In a more conflictual situation like the Middle East, hybrid warfare has been used to describe modern militias that leverage contemporary strategic trends such as the increasing role of terrorist tactics, the urbanisation of conflicts and the use of modern technology to improve the military capabilities of so-called irregular groups (from social media for propaganda purposes to the use of both commercial and military drones). The Russian approach in the MENA region and Africa is very different and is more related to the notion of soft power because in this context hybrid warfare is a set of economic contracts, military deals and political influence. At the same time in Syria, Russia has used a more traditional military approach based on airpower and A2/AD that can be hardly labelled as hybrid. The China approach has been described also as Grey Zone Warfare meaning that Beijing operates in the area between war and peace using both political–economic–diplomatic leverage along with some kind of conventional military tools to improve its global and regional geopolitical position.

## Questions

1. In which way can you describe ISIS warfare?
2. How did Russia intervene in Syria?
3. How did Russia operate in Africa?
4. Why does *Unrestricted Warfare* define China approach to warfare?

## References

Beccaro, Andrea (2021): Russia, Syria and Hybrid Warfare: A Critical Assessment. *Comparative Strategy,* 40(5), 482–498. Online: https://doi.org/10.1080/01495933.2021.1962199

Bertolotti, Claudio – Beccaro, Andrea (2015): Suicide Attack: Strategy, from the Afghan War to Syraq and Mediterranean Region. A Triple Way to Read the Asymmetric Threats. *Sicurezza, Terrorismo, Societá,* 283(2), 21–59.

Blank, Stephen J. ed. (2019): *The Russian Military in Contemporary Perspective.* Carlisle: The United States Army War College Press.

Breen, Michael – Geltzer, Joshua A. (2011): Asymmetric Strategies as Strategies of the Strong. *Parameters,* 41(1), 41–55. Online: https://doi.org/10.55540/0031-1723.2565

Bunker, Robert – Sullivan, John (2004): *Suicide Bombings in Operation Iraqi Freedom.* Arlington: The Institute of Land Warfare.

Dreyfus, Emmanuel (2020): Moscow's Limited Prospects in Sub-Saharan Africa. *Kennan Cable,* (47). Online: https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/KI_200224_cable%2047_v1.pdf

Faulkner, Christopher (2022): Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa. *CTC Sentinel,* 15(6), 28–37.

Giles, Keir (2016): *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power.* Online: https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

Giles, Keir (2019): Russia's "Lessons Learned" from Ukraine and Syria. In Blank, Stephen J. (ed.): *The Russian Military in Contemporary Perspective.* Carlisle: The United States Army War College Press, 287–303.

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

Kofman, Michael – Rojansky, Matthew (2015): A Closer Look at Russia's "Hybrid War". *Kennan Cable,* (7), 1–8. Online: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

Kozhanov, Nikolay (2013): Russian Support for Assad's Regime: Is There a Red Line? *The International Spectator,* 48(2), 25–31.

Lewis, Jeffrey W. (2007): Precision Terror: Suicide Bombing as Control Technology. *Terrorism and Political Violence,* 19(2), 223–245. Online: https://doi.org/10.1080/09546550701246890

Liang, Qiao – Xiangsui, Wang (1999): *Unrestricted Warfare. China's Master Plan to Destroy America.* Beijing: PLA Literature and Arts Publishing House.

Mattis, Peter – Brazil, Matthew (2019): *Chinese Communist Espionage: An Intelligence Primer.* Annapolis: Naval Institute Press.

Mazarr, Michael J. (2015): *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle: The United States Army War College Press.

Ollivant, Douglas A. (2016): The Rise of the Hybrid Warriors: From Ukraine to the Middle East. *War on the Rocks,* 9 March 2016. Online: https://warontherocks.com/2016/03/the-rise-of-the-hybrid-warriors-from-ukraine-to-the-middle-east/

Orizio, Pietro (2022): I contractors del Gruppo Wagner contro i jihadisti in Mali: l'Europa risponde con le sanzioni. *Analisi Difesa,* 5 January 2022. Online: https://www.analisidifesa.it/2022/01/i-contractors-del-gruppo-wagner-in-mali-a-combattere-i-jihadisti-leuropa-risponde-con-le-sanzioni/

Souleimanov, Emil – Dzutsati, Valery (2018): Russia's Syria War: A Strategic Trap? *Middle East Policy,* 25(2), 42–50. Online: https://doi.org/10.1111/mepo.12341

Vasiliev, Alexey (2018): *Russia's Middle East Policy. From Lenin to Putin.* New York: Routledge.

Vinson, Mark – Caldwell, John (2016): Violent Nonstate Actors with Missile Technologies. Threats Beyond the Battlefield. *Joint Force Quarterly,* 80(1), 116–123.

Wezeman, Pieter D. – Kuimova, Alexandra – Wezeman, Siemon T. (2022): *Trends in International Arms Transfers, 2021.* Sipri Fact Sheet, March 2022. Online: https://www.sipri.org/sites/default/files/2022-03/fs_2203_at_2021.pdf#xd_co_f=ZjViMGM4NmYtYWQ2NS00MWU4LWIxZWEtYjkzMTM1ZTJhYmE0~

Andrea Beccaro[1]

# The Evolution of Hybrid Warfare

Hybrid warfare has several nuances and can be referred to various tools and means. While some of them are relative new elements related to the current international system, several others represent the last evolution of a long history. This chapter aims to contextualise the notion of hybrid warfare in the broader framework of the contemporary international relations. Hence, the chapter intends to analyse two different contexts in which the notion of hybrid warfare has been used and the way in which that notion has been integrated in the EU official documents like EUGS (European Union Global Strategy) adopted in June 2016.

## Introduction

In recent years, scholars, politicians, think tanks have started to use terms, such as "hybrid–warfare–wars–conflicts–operations"; however, their definition is vague and indistinct. Moreover, the different use of such notions highlights the fact that they have evolved in the last two decades from an effective, albeit contentious, idea to describe a kind of modern and technological insurgency, to a less clear label used to describe very different military and non-military approaches related to the Russian operation in the international system. The main problem using the hybrid warfare notion is that in the literature it is used in order to describe at least two very different military situations both present in the EUGS. On the one hand, it has been used to describe the kind of military operations used by Russia since the occupation of Crimea in 2014. On the other hand, hybrid warfare could describe the warfare of non-state actors that use a mix of conventional and unconventional tactics and modern weapons. This double use of the term is clearly confusing and creates misunderstandings. For instance, if the EUGS referred to hybrid threat from Russia, then the countermeasures would be more conventional, such as an A2/AD system, counter propaganda, military units

[1] University of Turin.

DOI: https://doi.org/10.36250/01237_06

inside the European border and ready to operate. If the EUGS referred to hybrid threat as something related to irregular fighters, then the countermeasures would be more related to counterinsurgency doctrine, counterterrorism, Special Forces in war theatres outside, albeit near to, Europe. Therefore, different meanings of hybrid warfare lead to very different military and political solutions. In other words, if the notion of hybrid warfare is not correctly defined, the risk is to fight the wrong kind of war using the wrong strategy. The paper seeks to describe the different ways of using the notion of hybrid warfare, and, accordingly, is divided into three sections. The first one takes into account hybrid warfare that in the literature refers to irregular fighters and non-state groups, i.e. hybrid warfare understood as a kind of modern insurgency. The second section takes into account the Russian hybrid warfare that is more a Western label than a military doctrine elaborated by Russian military. Finally, the third section deals with the strategic debate in Europe and mainly with EUGS and EUS in order to mark the concepts used to define the EU strategic threats.

## Hybrid Warfare as modern insurgency

Since the end of Cold War, a huge debate in the strategic–security studies field has emerged related to how war and warfare have changed. This debate encompasses several different conceptualisations, ideas and scholars, and analysing it is outside the scope of this paper. However, the concept of hybrid warfare was firstly used in the context of this debate that stemmed from the idea that since 1989, but even since 1945, the most common type of war has not been state against state war but an irregular one labelled as guerrilla, insurgency, terrorism. This kind of war differs from conventional state wars because: it does not involve regular armies on both sides and most of its victims are civilians. In this context the notion of hybrid warfare is used to refer to a conflict in which at least one side is not a state in the modern and Western meaning. In this sense the notion of hybrid warfare predates the Russian version because it was used for the first time in 2005 and then in 2007, Hoffman formulated his theory that is the theory used here. It could be argued that any type of war is itself hybrid, but the term “hybrid” refers to the fact that contemporary conflicts present a mixture of regular and irregular elements, of conventional tactics, guerrilla warfare and terrorism. The theory of hybrid warfare stems from the Lebanon War of 2006 between the Israeli IDF and Hezbollah.[2] Hezbollah is interpreted as an example of the new enemy because it is structured in a network, is linked to the local population, and is irregular in its tactics. At the same time, Hezbollah employed anti-ship and anti-tank missiles along with small units and hit and run operations in a guerrilla warfare style for halting the advance of the IDF.[3] Then the notion of hybrid warfare has been used for describing the military operations of ISIS, which uses terrorism, guerrilla tactics and more conventional weaponry. Hybrid Warfare is characterised by the concept of *synergy,* that is, the simultaneous application of a multiplicity of ways of fighting to reach the goal.[4] In essence, contemporary conflicts cannot be characterised by a simple dichotomy of black and white, but they have more nuanced characteristics, losing the perception of boundaries between different forms and concepts. The war is therefore hybrid because the enemy's way of fighting combines different methods, tactics and tools, including conventional capabilities, irregular tactics, terrorism, indiscriminate violence, and criminal acts with the most modern technologies.[5] The situation is further complicated by the fact that the "hybrid warfare" battlefield is threefold: conventional; linked to the indigenous population; international. Only by prevailing in all three battlefields is it possible to win. Moreover, what distinguishes "hybrid warfare" from other types of struggles is that it must be fought on all three battlefields simultaneously and non-sequentially. The strategy to be used is defined as "counter organisation", because the aim is to destroy the irregular organisation in order to break their ties with the population and maintain the initiative. According to Frank Hoffman, hybrid warfare "incorporate[s] a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. [...] These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battle space to achieve synergistic effects in the physical and psychological dimension of conflict".[6] As a consequence, hybrid warfare represents a mix of different tactics (from terrorism to guerrilla warfare to more conventional operations) and uses

[2] Glenn 2008.

[3] Biddle–Friedman 2008.

[4] Hoffman 2006.

[5] Hoffman 2007.

[6] Hoffman 2007: 8.

different kinds of weapons (from small arms to more sophisticated missiles to propaganda and media coverage). According to Hoffman's conceptualisation, hybrid warfare is based on four key elements. The first element is that, in hybrid wars, regular and irregular elements "become blurred into the same force in the same battle space. 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."[7] As far as ISIS is concerned, this feature is evident looking at its operation in Iraq and Syria where it has used conventional infantry tactics in several occasions. For instance, in the north of Iraq it used artillery fire to pound Kurds Peshmerga or in al-Anbar it has manoeuvred units composed of several vehicles around the battlefield in order to have the element of surprise. Moreover, during the battle of Ramadi in the spring of 2015, ISIS used a very effective tactics combining suicide attacks to break the defensive lines of Iraqi Security Forces and then waves of foot soldiers. It should also be noted that ISIS used tanks and other military equipment seized from the Iraqi Army. This could represent a major difference between ISIS operations in Iraq and those in Libya because there ISIS has never had the same kind of arsenal it had in Iraq due to the fact that in Libya it was a latecomer militia and has not been able to seize considerable military equipment.[8] However, it has stolen modern weapons then used them in the Sinai Peninsula. As a consequence, the second element of hybrid warfare is that terrorism becomes the main fighting method. This is certainly true for ISIS because terrorist tactics are easier and cheaper to use than more conventional one. Furthermore, they can be used even far away from the main theatre of operation. ISIS has showed its ability to use quasi conventional tactics in theatres of operations where it is the main military force: in Iraq, Syria and to some extent Libya. However, it relays on terrorist tactics in cities where it has not the control of terrain and in those cases mass attack conducted with suicide attackers and car bombs are the norms. However, ISIS warfare is not limited to terrorist tactics and even when it attacks a market or a checkpoint using a terrorist method, it is not a 'pure' terrorist group for at least two main reasons. Firstly, 'pure' terrorist groups do not hold terrain as ISIS did in Iraq and Syria where it controlled vast areas between the two countries and ruled several cities: Raqqa, Mosul, Ramadi, Tikrit, Falluja. Its foothold in Libya has been more limited, yet it conquered and ruled for several months the

[7] Hoffman 2007: 8.

[8] Beccaro 2020.

city of Sirte. According to Cronin, "[t]errorist networks […] generally have only dozens or hundreds of members, attack civilians, do not hold territory, and cannot directly confront military forces. ISIS, on the other hand, boasts some 30,000 fighters, holds territory in both Iraq and Syria, maintains extensive military capabilities, controls lines of communication, commands infrastructure, funds itself, and engages in sophisticated military operations. If ISIS is purely and simply anything, it is a pseudo-state led by a conventional army."[9] As a consequence and this is the second reason, ISIS could be better defined as an insurgent group because insurgency includes both guerrilla tactics and terrorism. From a historical point of view, insurgent groups' tactics have always ranged from almost conventional operations to guerrilla style warfare to terrorism. The choice between those different tactics is often made based on the local military situation and on the strength of the group. This, for instance, explains why ISIS could not be considered defeated in Libya just because it has lost Sirte. It could use different fighting methods in order to achieve its goals: it could use 'hit and run' operations instead of a static defence as that of urban areas. Moreover, the role of terrorism in ISIS warfare is functional to its ideology and its transnational nature. According to Lia, "[un]like ethno-nationalist revolts or revolutionary struggles against national authorities, jihadis are not ideologically bound to fight in only one country or against one specific national regime".[10] The "transnational nature" is a key element in order to fully comprehend both the regional threat posed by ISIS and the terrorism role. Terrorism is a perfect stand-off tactics to cross national borders and strike targets that are not in the main theatre of operations. Furthermore, ignoring national border means that counterterrorism, or better counterinsurgency, has to be transnational and has to involve more states and agencies. The third element of hybrid groups is their use of modern technology "to avoid predictability and seek advantage in unexpected ways and ruthless modes of attack".[11] ISIS has been able to use modern technology in order to build new kinds of weaponry and devise different ways of attack, mainly suicide operations. ISIS has used technology in several different ways. First, it broadcasts its propaganda through numerous social media, website and blogs. Second, it uses modern weapons or it has created its own. Mainly in Syria and Iraq it has used chlorine gas, it has manufactured its own tele-operated sniper

[9] Cronin 2015: 90.

[10] Lia 2016: 83.

[11] Hoffman 2007: 16.

rifles and submachine guns. Moreover, during the battle of Mosul in Iraq ISIS has widely used drones in offensive operations. Third, the extensive use of suicide attacks could be explained looking at their tactical benefit. In fact, ISIS has often used this fighting method to soften enemy defence and open gaps where its foot soldiers could get in. In this way, suicide attack represents a kind of "smart bomb" as those used by Western Armed Forces. Finally, the fourth element of hybrid warfare is related to the battle space because hybrid war, like every irregular war, takes place in complex terrain, most likely the burgeoning cities of the developing world. As a consequence of the increasing urbanisation of the world population, today conflicts seem to be fought more often in urban areas. While the "urbanisation of conflicts" is a global trend rooted in "rapid population growth, accelerating urbanization, littoralization (the tendency for things to cluster on coastlines), and increasing connectedness",[12] the European Southern Neighbourhood is particularly affected as the urban population growth shows: it "grew by 40 million between 1970 and 2000, and three-quarters of that growth was in North Africa and the Middle East".[13] It is no coincidence that the two countries most affected by urbanisation were Tunisia and Libya. Moreover, the 2011 uprisings showed another key element related to urbanisation of conflicts, i.e. its connectedness, because they "saw the use of cell phones, social media, and text messaging as organizing tools".[14] ISIS is a "hybrid" threat because in Iraq, in Syria, in Libya and in Egypt it has used both modern advanced weapons, such as armoured vehicles, tanks, missiles, drones, artillery and conventional-like infantry tactics and terrorism and guerrilla warfare. It has also used suicide attackers and suicide vehicle borne IED as a kind of cruise missile able to strike precisely the desired target. At the same time, it used both its great mobility to evade enemy reconnaissance and strike where it wanted, as every guerrilla group had done throughout history; and terrorism attacks in cities where it had a loose presence or the security forces were better armed, such as Baghdad or Paris. Moreover, like successful guerrilla groups of the past it was able to control territory using it as a safe haven where to plan, organise, train and so on. Finally, ISIS uses modern technology to improve its fighting ability and spread its propaganda. As for propaganda, ISIS is well known for its ability to record high quality videos such as that of the burning of the Jordanian pilot or that of pure

[12] Kilcullen 2013: 25.

[13] Kilcullen 2013: 23.

[14] Kilcullen 2013: 23.

propaganda in which it is stated that ISIS will conquer Rome. However, ISIS has even produced reviews, such as *Dabiq,* that reflect the glossy magazines of the West. The combination of all of these elements is not entirely new, but it represents a different kind of threat compared to conventional ones. As for the Russian concept of hybrid warfare, it is not a novelty, but simply an evolution of modern warfare, which is neither original nor typical of Russia; this meaning of hybrid warfare has a long history. However, there is a substantial difference between the links to strategic history of these two concepts of hybrid warfare. While the Russian version does not add anything really new compared to previous conventional operations fought in the same way, the ISIS version has some new features compared to the long history of irregular warfare. It is true that throughout history insurgent groups have used terrorism, guerrilla warfare and more conventional tactics, depending on their resources, strategic and tactical situation and political context; however, the real difference between modern hybrid warfare and the older one lies in the use of technology. In the past, it was difficult for them to acquire and use modern weapons; today, it is not only simpler but these weapons can also be created by irregular groups, as ISIS has already demonstrated, with its suicide vehicles, drones, and the use of social media and the Internet.

## A Russian Hybrid Warfare?

The question mark in title of this section[15] is not accidental, because after the Russian military operations in Ukraine and Crimea in 2014, several Western scholars labelled the Russian operations as hybrid warfare. The term ‘hybrid war’ to describe Russian military operations gradually gained ascendancy in the second half of 2014; however, two problems arise from this label. First, the hybrid warfare term was used by western pundits only and it was not present in Russian official doctrine back then.[16] Consequently, hybrid warfare is a western label used to describe Russian operations, rather than a military doctrine that Russians used to achieve their goals. Secondly, the kind of operations labelled as hybrid actually resemble the same kind of operations used by the U.S. over the last few decades, that is, a combination of Special Forces, conventional forces,

[15] Beccaro 2021.

[16] Bartles 2016a; McDermott 2016.

local allies and propaganda. According to Keir Giles, the notion of hybrid warfare was "originally introduced by NATO's Allied Command Transformation as part of planning for out-of-area activities" and then it "gained a foothold in NATO Headquarters in mid-2014 as 'the Russian hybrid model in Ukraine' became a means of explaining operations that did not fit neatly into NATO's operational concepts".[17] The problem with hybrid warfare is that it misses a key point. "Hybrid war can hardly be considered a definitive doctrine for Russia's future power projection in its neighborhood, much less a model that could be easily reproduced in far flung and diverse corners of the post-Soviet space."[18] This is clear looking at Russian operations in Syria. They followed short after the operations in Ukraine, yet they fit into a completely different pattern because in Syria, Russia used its airpower, tested modern weapons, implemented an A2/AD strategy, and used its Special Operations forces in their classic role of training and support forces to local ally. The problem to label Russian operations as hybrid warfare lies in the fact that "[t]he 'hybrid' aspect of the term simply denotes a combination of previously defined types of warfare, whether conventional, irregular, political or information".[19] However, neither the combination of different types of warfare nor their uses are new in history or particularly original to justify the use of a new label to differentiate it from the old ones. At least since the 1990s, the U.S. has recognised the key role of information in modern warfare; accordingly, Russia has recognised the nature of modern warfare and has used it. Even the idea to use non-military tools to fight modern wars is hardly new. For instance, in a widely discussed book of the 1990s, two Chinese colonels described the modern warfare as *Unrestricted Warfare* because modern warfare is not limited to military tools anymore. The key idea of the book is that modern warfare erodes the traditional boundaries of war, and looking at modern operations, such as *Desert Storm* and *Deliberate Force,* it suggests a warfare that eludes traditional military borders and enters into the world of economics and finance, or employs those weapons in unexpected ways.[20] According to Michael Kofman and Matthew Rojansky, Russia describes modern warfare as "the integrated utilization of military force and forces and resources of a nonmilitary character" that is exactly the idea of unrestricted warfare aforementioned. Moreover, the Russians

[17] Giles 2016: 8.

[18] Kofman–Rojansky 2015: 1.

[19] Kofman–Rojansky 2015: 2.

[20] Liang–Xiangsui 1999.

understand modern military operations as integrated with information and propaganda: "The prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force."[21] However, they did not invent this approach, for instance a very well-known example of this approach is the famous discourse of the then Secretary of State Colin Powel to the UN showing a vial "full" of "anthrax" supposedly produced by Iraq that was later demonstrated to be a total fake news. Even the "participation of irregular armed force elements and private military companies in military operations," and "use of indirect and asymmetric methods of operations" is not new nor only Russian.[22] This is a key element of modern western operations that some scholars have even labelled as "Afghan model"[23] indicating the fact that U.S. and Western states used their SOF to support local allies. Russia seems to have learnt this lesson, since according to McDermott one of the most outstanding features "of advances in Russia's application of military power […] in Syria relate to the success of training proxy forces […] introducing new or advanced systems in these operations and supporting operations adequately through predominantly air and sea lines of communication".[24] Moreover, the use of contractors in different roles and theatres of operation is a widely known aspect of modern Western Warfare since the conflict in the Balkans. Russian operations in Crimea in 2014 began with a covert military operation, combining ambiguity, disinformation and the element of surprise; then, a more conventional military invasion and occupation of the peninsula, using Russia's airborne, naval infantry and motor rifle brigades followed completing the annexation. However, this kind of operations were possible in Crimea where the majority of the population is Russian and where Russia had already had a strategic naval base in Sevastopol where, before the beginning of the operation, it sent secretly several members of its Special Forces. However, the strategic importance of Crimea, the local population, the geographical proximity and the presence of Russian military assets are crucial elements that could not be replicated elsewhere. To conclude, according to Kofman and Rojansky Russian operations in Ukraine are not a new

[21] Kofman–Rojansky 2015: 3.

[22] Kofman–Rojansky 2015: 3.

[23] Biddle 2002.

[24] McDermott 2016: 8.

type of warfare or a hybrid one, instead they "should be understood in more flexible and basic terms – as an attempt to employ diplomatic, economic, military, and information instruments in a neighboring state where it perceives vital national interests to be at stake".[25] Furthermore, this pattern, from diplomatic actions to military operations, is very Clausewitzian rather than hybrid. In fact, according to Charap both in Crimea–Ukraine and Syria "the use of force has come after other non-kinetic means have been tried" and failed. Accordingly, from a Russian point of view the use of force represents just a last resort. "In the six months before the invasion of Crimea, Moscow threatened and then implemented economic sanctions (July–September 2013), offered a whopping $15 billion in economic assistance (December 2013), and engaged in diplomacy with the West (the February 21, 2014 agreement) prior to using the military." Equally, Russia in Syria had engaged in extensive diplomatic outreach, conducted arms transfers, and even attempted to organise the opposition before using directly its military mean.[26] In Crimea, Russia used a combination of covert operations, Special Forces and propaganda. Clearly, this is not a conventional operation but, at the same time, it is a very common way to employ military forces. Furthermore, the use of Special Forces, paratrooper units and raids against key enemy targets has always been a central element of Soviet and then Russian military doctrine. Moreover, denying the presence of regular forces where they are on the ground is an old tool to frustrate enemy response and has numerous precedents. The USSR did it during the Cold War with troops secretly deployed in Egypt, Syria and Angola. However, the United States has also used such tools several times. The "new" Russian operations in Crimea could be better understood as an evolution of the old Soviet military doctrine in which the use of partisan forces and special operations forces (SOF), intelligence services and propaganda to conduct provocations and shape the area of operations were certainly part of the military operations. However, these activities were secondary in comparison to the major actions of the conventional war fighter.[27] Consequently, today the role played by indirect tools such as SOF, propaganda, intelligence and so on, is bigger and more visible than in the past. Yet, this is not true only for Russia, but it is a strategic reality for every modern Army. Nothing in the notion of "hybrid warfare" is really new. According to Peter Mansoor: "Hybrid warfare has been

[25] Kofman–Rojansky 2015: 7.

[26] Charap 2016.

[27] Bartles 2016b.

an integral part of the historical landscape since the ancient world, but only recently have analysts – incorrectly – categorized these conflicts as unique."[28] Furthermore, looking exclusively to Russia: "Many elements of this 'new' warfare: subversion, physical and informational provocation, economic threats, posturing with regular forces, the use of special forces, and the military intelligence coordinating paramilitary groups and political front organizations, have been part of the Russian/Soviet lexicon of conflict for generations."[29] Consequently, what Western scholars have called "hybrid warfare" indicating with this notion a new Russian doctrine is, on the contrary, a classic example of covert operations that Western practitioners should know very well.

## The EUGS and the concept of Hybrid Warfare

The wide use of "hybrid warfare", and accordingly its relevance in today's security debate, is also shown by the fact that it is currently used in official EU documents, i.e. EUGS, which refers to "hybrid threats" five times. Nevertheless, every reference is very general and does not define any specific kind of threat or risk. Therefore, EUGS fails to define precisely what a hybrid threat is or is not. The publication of the EU Global Strategy (EUGS) on 28 June 2016 by the EU's High Representative for Foreign and Security Policy Federica Mogherini represented the final result of a two-year-long work that involved extensive consultations with EU member states, European experts and scholars, and third country representatives. It also represented a key step by the EU in order to improve its foreign policy, its understanding of current security threats to its neighbourhood, and a needed revise of its strategy after the publication of the European Security Strategy (ESS) in 2003. The geopolitical and security situation is dramatically changed since 2003. ESS was clearly outdated because, for example, it stated: "The violence of the first half of the 20th Century has given way to a period of peace and stability unprecedented in European history."[30] Such an *incipit* has been made obsolete by the deteriorating geopolitical situation in the Southern and Eastern neighbourhood of the EU where several different types of conflicts are taking place. The war in Ukraine underscores the complex

[28] Mansoor 2012.

[29] Jonsson–Seely 2015.

[30] Council of the European Union 2003.

relations between the EU and Russia and epitomises a state against state conflict, albeit with some differences compared to the past. Libya has become a failed state, is divided between two governments, and several militias representing a completely different threat. Besides, Islamist groups are active in Libya but even in the Sinai Peninsula and Tunisia where they risk to destabilise those countries. The war in Syria represents another type of conflict with deep and important geopolitical consequences linked to the involvement of Russia, Iran and Turkey[31] and to a broader and growing instability in the Middle East. The EU published EUGS in order to deal with the aforementioned complex political and security issues; however, with regard to conflicts in its neighbourhoods, EUGS seems to be vague at least when it seeks to clearly define and identify security problems. It does offer an in-depth analysis of current conflicts in the European Neighbourhood Policy (ENP) area, moreover the use of terms such as "terrorism" or "hybrid war" are vague using it for labelling two very different political and military contexts and EUGS is able only partially to understand the complexity of these violent phenomena. ESS and EUGS are very different documents mainly because their geopolitical background is completely different. ESS was published in 2003 when the security on the ENP seemed certain and guaranteed mainly by the United State military forces in the area. At the time, Russia was still recovering from the Soviet collapse in 1990 and Putin was nearly at the end of his first presidential term. The Mediterranean region was stable and the war in Iraq was just at its early stages, but the country was slowly descending in a violent and bloody insurgency. This chaos offered new possibilities to groups such as al-Qaeda in Iraq (AQI) that became ISIS in those times. On the contrary, the EUGS was published in a completely different and extremely more violent geopolitical situation. First, the U.S. under the Obama Administration started to withdraw from the Mediterranean region giving political space to other actors. The U.S. withdrawal from Iraq in 2011, for instance, was a major blow to the security of that country and consequently to the entire region in a historical moment deeply influenced by the so-called Arab Spring that spread instability along the entire Mediterranean region creating failed state in Libya, increasing instability in Egypt, civil war in Syria. Meanwhile, Iraq increasingly became a sort of failed state where ISIS militias, Shia militias, the Iraqi Army and Kurdish Peshmerga faught for their own political goals. Furthermore, ISIS

[31] It should be noted that when EUGS was published the trilateral agreement between Russia, Iran and Turkey has not yet been reached.

and similar jihadist militias expanded their operative range not only inside the Mediterranean region exploiting this increasing instability, but also inside the EU carrying out several terrorist attacks. Even the Eastern Neighbourhood became more unstable with a more active Russia that waged wars in Georgia in 2008 and in Ukraine in 2014 to defend its geopolitical interests and military bases. The European Security Strategy (ESS) stated that: "Large-scale aggression against any Member State is now improbable. Instead, Europe faces new threats which are more diverse, less visible and less predictable."[32] Amongst them the ESS listed: terrorism highlighting that it arises out of several causes such as "modernisation, cultural, social and political crises, and the alienation of young people living in foreign societies";[33] state failure caused by bad governance, corruption, weak institutions and civil conflict; organised crime that was labelled as internal threat but with an important external dimension with regard to "cross-border trafficking in drugs, women, illegal migrants and weapons" and to links with terrorism associated with failing states.[34] Moreover, the ESS listed more conventional threats: Proliferation of Weapons of Mass Destruction;[35] regional conflicts yet far from the EU. The aforementioned enormous geopolitical difference between 2003 and 2016 has influenced the EUGS even if it has strong links to ESS. For example, the EUGS refers often to the problem of weapons of mass destruction, simply changing the label used, that is, nonproliferation meaning in this way even arms control.[36] The EUGS does not rule out the risk of external and more conventional threats, since it states that EU members: "Must be ready and able to deter, respond to, and protect [them]selves against external threats." As a consequence, the EUGS calls Europeans to "be better equipped, trained and organized".[37] In the EUGS, the notion of failed states is not present; instead, it uses notions such as "fragile states" and stresses the idea of resilience in order to underline the need to address stability processes, peace enforcement operations, etc. Moreover, the EUGS stresses the idea to invest more in "artificial intelligence, robotics and remotely piloted systems".[38] In fact, the EUGS underlines the fact that EU members have to improve their

[32] Council of the European Union 2003: 3.
[33] Council of the European Union 2003: 3.
[34] Council of the European Union 2003: 4.
[35] Council of the European Union 2003.
[36] Council of the European Union 2016.
[37] Council of the European Union 2016: 19.
[38] Council of the European Union 2016: 43.

cooperation in intelligence and in sharing crucial information. While terrorism remains a key issue, the EUGS expands the spectrum of threats including the concept of “hybrid warfare”. Both terrorism and hybrid warfare, however, are not precisely defined in the EUGS and even in the literature they are difficult to define. With regard to terrorism, the term misleadingly describes the conflicts in the Mediterranean region. Terrorism simply does not describe the real nature of the threat posed by groups such as ISIS, al-Qaeda, al-Nusra and al-Qaeda in the Islamic Maghreb. They use often tactics that could be defined as terrorist, but on the other hand they control territories, people, and have a very well structured and deep-rooted web of relationship inside and outside Europe. Concerning, instead, the notion of hybrid warfare it should be noted that in the EUGS it refers to the Russian operations in Ukraine; however, this term is misleading because in the literature “hybrid warfare” refers to non-state actors that use some conventional capabilities in order to fight against a stronger enemy. All things considered, if the notions of terrorism and hybrid warfare used by the EUGS are misleading and incorrect to clarify the kind of conflicts that affects ENP and so the EU security, how could they be defined? It is simply impossible to answer this question, in-depth analyses remain of the academic debate that focuses on how contemporary wars are fought. This will enable a better comprehension of the conflicts that the EUGS would confront.

## Conclusion

First of all, “hybrid warfare” is challenging to define because every kind of warfare is somehow in itself “hybrid”, so the notion of “hybrid warfare” has to be understood in relation to the conventional warfare, i.e. state against state warfare. Consequently, “hybrid warfare” represents a mixture of different tactics and/or weapons that then creates a warfare that has some elements of the conventional one but which is not the same. The problem with the notion of “hybrid warfare” is that it is used to describe two very different kinds of armed conflicts, i.e. the Russia “doctrine” used in Crimea and the terrorist strategy employed by groups such as ISIS, that have nothing in common and that represent deeply different military threats and political context.

## Questions

1. Which are the main features of the notion of hybrid warfare as modern insurgency?
2. Why is the notion of hybrid warfare contentious referred to Russian operations?
3. In which way does the EUGS use the notion of hybrid warfare?
4. Why is the notion of hybrid warfare so challenging?

## References

Bartles, Charles (2016a): Getting Gerasimov Right. *Military Review,* 96(1), 30–38.

Bartles, Charles (2016b): Russia's Indirect and Asymmetric Methods as a Response to the New Western Way of War. *Special Operations Journal,* 2(1), 1–11. Online: https://doi.org/10.1080/23296151.2016.1134964

Beccaro, Andrea (2020): ISIS in Libya and Beyond, 2014–2016. *The Journal of North African Studies,* 27(1), 160–179. Online: https://doi.org/10.1080/13629387.2020.1747445

Beccaro, Andrea (2021): Russia, Syria and Hybrid Warfare: A Critical Assessment. *Comparative Strategy,* 40(5), 482–498. Online: https://doi.org/10.1080/01495933.2021.1962199

Biddle, Stephen (2002): *Afghanistan and the Future of Warfare: Implications for Army and Defense Policy.* Carlisle: The United States Army War College Press.

Biddle, Stephen – Friedman, Jeffrey (2008): *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy.* Carlisle: The United States Army War College Press.

Charap, Samuel (2016): *Russia's Use of Military Force as a Foreign Policy Tool. Is There a Logic?* Online: https://www.ponarseurasia.org/russia-s-use-of-military-force-as-a-foreign-policy-tool-is-there-a-logic/

Cronin, Audrey K. (2015): ISIS Is Not a Terrorist Group. *Foreign Affairs,* 94(2), 87–98.

Council of the European Union (2003): *A Secure Europe in a Better World. European Security Strategy. Shared Vision, Common Action: A Stronger Europe.* Online: https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf

Council of the European Union (2016): *A Global Strategy for the European Union's Foreign and Security Policy.* Online: https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en

Giles, Keir (2016): *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power.* Online: https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

Glenn, Russel (2008): *All Glory Is Fleeting: Insights from the Second Lebanon War.* Santa Monica: RAND.

Hoffman, Frank (2006): Complex Irregular Warfare: The Next Revolution in Military Affairs. *Orbis,* 50(3), 395–411.

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

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

Kilcullen, David (2013): *Out of the Mountains. The Coming Age of the Urban Guerrilla.* London: Hurst.

Kofman, Michael – Rojansky, Mathew (2015): A Closer Look at Russia's "Hybrid War". *Kennan Cable,* (7), 1–8. Online: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

Lia, Brynjar (2016): Jihadism in the Arab World after 2011: Explaining Its Expansion. *Middle East Policy,* 23(4), 74–91.

Liang, Qiao – Xiangsui, Wang (1999): *Unrestricted Warfare. China's Master Plan to Destroy America.* Beijing: PLA Literature and Arts Publishing House.

Mansoor, Peter R. (2012): Introduction: Hybrid Warfare in History. In Murray, Williamson – Mansoor, Peter R. (eds.): *Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present.* Cambridge: Cambridge University Press, 1–10.

McDermott, Roger (2016): Does Russia Have a Gerasimov Doctrine? *Parameters,* 46(1), 97–105. Online: https://doi.org/10.55540/0031-1723.2827

Marco Di Giovanni[1]

# History and Theory

In this chapter the author will compare historical processes of the Twentieth and, in perspective, of the Twenty-first century, to place within some specific frames of time the scenarios in which the multilevel dimension of the conduct of conflicts – with the wide presence and relevance of non-military instruments fused together with the kinetic and operational dimension – get a strategic significance. An historical condition that makes the boundaries between the state of war and "peace" indefinite. Historical and, structurally, socio-political phases, in which a dense gray area is created, that sometimes preludes to war, sometimes replaces the open unleashing of the military instrument, pursuing by different means the same goals of open war, which sometimes it introduces, sometimes it accompanies. Phases that solicit, even on the theoretical terrain, an attempt to specifically qualify the new ways of war. History can be the instrument that help us to fix and define this kind of scenarios in which the combination of military and non-military means organised in a system, get the strategic level. Today's unconsolidated proposal of the "hybrid warfare" category responds, in the laborious and often contradictory attempts at definition, to a transitional phase of this nature and calls political theory and history an interpretative discipline, in the definition of their objects. The scenario of the thirties of the last century, reveals precisely a full deployment of non-linear war structurally based on the perspective of ideological war and on the profound transformation of the world of information with the irruption of new penetrating media and a studied use of propaganda. Kingdom of a political and psychological action that accompanies the properly military dynamic. Nazi Germany politics and non-linear approach to war, as a key and ideologically grounded instrument of its aggressive revisionism, will be the focus in our discussion. Processes that call us to reflect on our time as an analogous age of "revolutionary" change.

[1] University of Turin.

DOI: https://doi.org/10.36250/01237_07

## International scenario and communications environment

The starting point must be the Great Transformation between the two world wars. In the heart of the Second Thirty Years' War, the myth of the homeland state and the model of the total state were mixed with the pitfalls of the internal enemy and the paths, of various matrices, of "subversion". A technological threshold of communication and mass politics had been crossed. Radio broadcasts broke boundaries and incorporated the attractive force of ideologies, the messages of the "politics of fear and identity", the charismatic force of the shouted word of dictators in the "Age of Anxiety". International politics and conflicts could absorb, in a new key, the fusion of external and internal threats and the actors could add with new intensity and depth the indirect and "covered" tools to the direct ones, to erode the reaction capacities of the opponents and acquire political or also operational advantages, even before crossing the threshold of military action. The twenties and especially the thirties are, in short, the scenario in which a full transition is condensed that feeds the war as a total and complex confrontation, the ultimate landing place of a friction managed on many different levels and in forms that associate the recognisable "conventionality" of the military dimension with other paths. Thus, even tools already tested in the past, such as deception and propaganda, incorporated elements of erosion of the enemy, of "subversion", that gained greater relevance. Above all, they integrated systematically with other elements, from the diplomatic and economic ones to those properly "kinetic" and operational, in a complex conflictual process, programmatically developed in strategic direction. The "subversive" integration of particular military instruments capable of combining deep penetration and dissolution of the political structure of the enemy's resistance belonged to the Soviet military vision of a potentially international "civil war" since the 1920s.[2] The vision of Frunze and in particular of Tukhachevskiy of a war "in depth" that would merge the strategic mobility of motorised or airborne troops and political participation of civilians (certainly starting from Soviet soil and as "resistant") was fully placed, in an operational key, in this horizon. It was assumed, on a class basis, the meeting of men in uniform and ideologically similar volunteers even in the conquered foreign territories, all operating according to the modalities proper to a civil war. Moreover, the awareness of the absolute enmity between the two worlds, the capitalist and that of the socialist revolution *in fieri,* made

[2] Raychev 2019; Fridman 2012; Sinovets 2016; Jonsson 2019.

perpetually latent, even in non-kinetic phases, the state of war. Sedition and internal revolt prepared and subsequently met with the external military impulse prepared by political action. Interior and exterior met, and the cadres of the armed revolution of each country had to be prepared in the temporary external "island", the homeland of socialism.[3] This approach was also referred to by those German officers and observers who, on the basis of the wide – and secret – cooperation of the military of the two countries in the twenties, reflected on the development of the new specialty of the paratroopers, ready to give, in fact, an interpretation that combined conventional military action with the potential of "political warfare".[4] A further point of conjunction between the Russian world, Nazi Germany and non-linear forms of war can also be found in the biographical itinerary of Evgeni Messner, a Russian officer who switched to Nazism to fight the Soviets in the Axis propaganda departments in 1941 and a theorist of the war of subversion and non-linear warfare in the age of total and ideological war.[5] Intertwined with these shared ideas, however, it was Nazi Germany that fully set in motion, in the perspective of its aggressive revisionism, an integrated political and strategic approach called to exploit all available means to march towards the objectives established, as far as possible, below the threshold of war.

## Nazi Germany: Diplomacy, non-state actors and the fifth column

The examination of the practices of Nazi Germany in accompaniment and premise of military actions[6] suggests in fact a reflection and a potential generalisation about the paths through which revisionist powers conceal their final objectives through processes of deception and manipulation of the adversary perception. A sequence of increasing complexity aimed at exploiting the weaknesses, real or ideologically hypostatised, of adversaries, fragmenting systems of alliances and collective security in the face of "ambiguous" actions and paralysing their ability to react. Actions that structurally combine total disregard for the system

[3] Only one example can be invoked with regard to the Soviet attempt to destabilise Estonia in December 1924, through the use of communist supporters destined, unsuccessfully, to attack the palace of government to pave the way for the Red Army.

[4] Basseches 1945; Bassenge 1939; Schuttel 1938.

[5] Thomas 2016; Fridman 2018.

[6] Weinberg 1995.

of norms and international law, a solid determination and a strategic approach in the use of political and non-military instruments to the brink of war (and beyond). We will find in our path a structured and increasingly defined combination of elements that, it seems to us, anticipate many aspects of the dynamics of our age. In particular, we will be able to highlight:

- covert actions and deniability (with the involvement of minorities, local actors and agencies)
- coercive diplomacy
- strategic ambiguity (and opacity of the boundaries of actions between peace and war)
- manipulation of perception and decision-making processes (with coercion at different levels)
- diplomacy of deception and *fait accompli* policy through rapid and decisive military action

A sequence destined to be renewed on the international scene starting from the German rearmament and militarisation of the Rhineland right into the war itself, from the Polish defeat to the collapse of France.[7] During the Twenties, the creation of the Abwehr and international constraints had certainly fuelled German attention to non-linear methods and unconventional instruments, shared as mentioned with the Soviet world. The Foreign Ministry's institutional tradition of commitment in these fields (through unconventional actions against the British empire during the Great War) was revived in the years of Nazism with the contribution of other agencies. We find the creation, in 1935, of an office specifically dedicated to these operations at the Abwehr and a very extensive commitment abroad of the Nazi Party, crossing every threshold of ethical and operational scruple.[8] The Nazi policy of influence abroad aimed at expanding in different directions and with aims that far exceeded the usual drive to erode the British Empire (support for Indian, Irish or Arab nationalism)[9] but aimed to integrate fully with an operational perspective. It now consciously accompanied the itinerary of a diplomatic, informative and political escalation that pursued the demolition of the resistance capacities of the target countries. The age of the "fifth column", these certainly not new as a deception tool but fully

[7] Cristadoro 2022.

[8] Mengel 2007.

[9] Perkins 1991.

reshaped in that radicalised season of total ideological conflict, opened new perspectives to actors and methods that navigated in the gray area of "state deniability".[10] Means that could anticipate but also, subsequently, accompany a military action, integrating into its operational phases.[11] A cycle that fully grew between 1938–1942, in which various German and Nazi organisations activated the collaborations of external actors and minorities, later experiencing a rapid decline linked to the negative course of the war, while an initial multiplicity of agencies was reabsorbed by a central political control service.[12] William Shirer journalist, historian and direct witness of the events, offers us the sequence of passages that mark the revisionist path of Nazi Germany. Starting from the structural construction of the Nazi rule over information, favoured by the monopoly on radio broadcasts (usual in Europe), while press and cinema were, between 1933 and 1934, fully framed in the Nazi control system. Shirer, a political commentator for Universal Service – by the end of 1937 he had switched from the newspaper's press to radio broadcasts with CBS and its information service from Europe based in Vienna – could grasp over time the ability of the radio medium and its deceptions to penetrate the beliefs of the German public.[13] At that stage, a modern information space was defined that combined different tools for political manipulation at home and abroad. Between 1933 and 1935: "preaching peace", "clandestine rearmament" and covert preparation for war avoiding the risk of a preventive intervention by the victors of Versailles constituted the guidelines of Hitler's policy, aimed at managing a functional communication towards the outside.[14] The occult action of Nazism moved from this framework but opened the ways to create the most of the divisions between democracies and inside their public opinions. The Nazi management of the erosion of the international security system shows, in an exemplary sequence, an authentic model of implementation of revisionism, with an articulation of political instruments and non-military means pushed to the threat of escalation but set to remain below the threshold of war. A dynamic built to make up for an initial military inadequacy with respect to the political objectives but shaped around the awareness and exploitation of the weaknesses of the adversaries that

[10] Orlow 1999.

[11] Godson–Wirtz 2011.

[12] Mengel 2007.

[13] Shirer 1974; Shirer 1986.

[14] Weinberg 1995.

themselves become decisive instruments of a political war. A flexible and pragmatic opportunism accompanies an outlined strategic itinerary. The crisis of July 1934 in Austria was an initial stage revealing the forms and also the dangers inherent in these proceedings. The assassination of Austrian Chancellor Dollfuss and an attempted assault on the Chancellery by the local Nazis highlighted too early the organisational work that the German Nazi Party had activated in the Austrian scenario. Alongside the direct support to sympathisers, with the formation in Bavaria of an Austrian legion ready to cross the border, it was evident in fact the active support for radio propaganda – from Munich – of the local Nazi leader in "exile" Alfred Frauenfeld. Besides, there was no lack of support for terrorist activities in Austria against state structures and members of the government. An international scenario not yet softened and divided and a rapid Italian reaction imposed a hasty withdrawal of the Reich Government, forced to dissociate itself from the political dynamic triggered, denying any involvement in the crisis. From there began an intense activity of disinformation towards the foreign press more willing to confirm the absence of bellicose projects on the German side.[15] A "brake" that corresponded, however, to the hidden start of rearmament in the autumn of 1934, with the first secret expansion of the army personnel and a plan for new shipbuilding. The next phase was openly revisionist in the erosion of the bonds of Versailles, managed by *faits accompli* (from the official announcement of the rearmament in March 1935 to the reoccupation of the Rhineland in 1936) and public statements oscillating between the demand for "good rights", victimisation for the legacy of Versailles and solicitations for new fair agreements veiled by allusions to the use of force. At that point, the incipient division between the European main actors (with the Italian attack on Ethiopia) and their substantial unwillingness to act firmly were exploited. The military coup of the reoccupation of the Rhineland, in March 1936, inaugurated a process destined to be repeated, with the construction of a *fait accompli* from which to start peace offers. These offers combined the manipulation of reality and an increasingly firm intimidation as international interlocutors proved divided and irresolute in front of the violation of international agreements. The breaches were followed by the acceptance of the new conditions in search of a possible balance that would temper feared *escalation* towards war and also confirming Hitler's strategic determination and his confidence in the means adopted. It was precisely the evident lack of determination

[15] Shirer 1974.

of the democracies, the different perception of the threat by Great Britain and France, that convinced the new Austrian Chancellor Schuschnigg to seek a policy of agreement with Hitler that would safeguard the integrity of Austria even if not full sovereignty. The treaty of 11 July 1936 was one of the diplomatic traps devised by Nazism to undermine the target countries from within. It guaranteed German non-interference in Austrian affairs and the recognition of a sovereignty tempered by the constraint of considering the general interests of the Germans in foreign policy. The document, however, contained secret clauses that, on the operational level, opened the way to a full penetration of the interests of the Reich in Austria, with the guarantee of amnesty for the arrested local Nazis and the constraint of reserving to that political party important positions within the administration. A Trojan horse destined to open in February 1938.[16] When the diplomatic framework appeared mature and relations with Italy redefined with a substantial consensus of Mussolini, the feasibility of the Anschluss became concrete. Hitler's strategy since the end of 1937 was war-oriented but with variable time horizons. The fragility of democracies, the internal political tearing in France and British uncertainties about an effective continental commitment, the unwillingness to use the military instrument as a deterrence, the support now guaranteed by Mussolini, offered the basis for still acting below the threshold of war. The absorption of the Austrian Republic into the Reich was achieved through an exemplary sequence destined to be repeated. This developed from a direct military intimidation that accompanied Hitler's ultimatum to Chancellor Schuschnigg (12 February 1938) to obtain the placement of Austrian pro-Nazis in key government posts, a similar integration of the security forces and a process of economic assimilation. News of German military movements on the borders accompanied the timing of the "negotiation" for the signing of the "agreement". Hitler reinforced the threat with shouted public statements (speech of 20 February to the Reichstag) about the rights of Germans outside the borders of the Reich while the local Nazis unleashed demonstrations and violence in Austria. Military intimidation and subversion paved the way for a "peacemaker" intervention. Arthur Seyss-Inquart and the other Nazis who had become part of the government apparatus undermined even minor attempts at opposition by favouring the internal crumbling of the state. France did not have a government in those weeks and Chamberlain's British Government had no

[16] Shirer 1974.

intention of intervening in the "internal relations between the two states".[17] International response for the protection of small states was inexistent. The coup was completed with Hitler's triumphant visit to his native country. The defence of the Germans, a "question of minorities", could be consolidated as an instrument for the next steps to achieve a "reflexive control" on democracies and legitimise the Reich's "reasonable" demands. The strategic scope of the project remained hidden. Even the planning of the crushing of Czechoslovakia, (the "Fall Grün" originally traced in the summer of 1937), included, in its definition of April 1938,[18] a complete section dedicated to "propaganda" in addition to political and military measures.[19] It was necessary to support and feed the action of the Sudeten German Party, directly financed by Berlin and capable of animating the chauvinism of a large part of the local German minority (about 3 million).[20] It was up to them to undermine, with deliberately unacceptable political petitions, the stability of the country's government and its credibility with the allies, who were annoyed by the Czechs' unwillingness to compromise. The result was to be a contrast between sovereignty and "justice" aimed at making the horizon of law opaque and international support for the attacked country friable. All the more so if in the background and with ever greater determination Hitler could wave the threat of war. A new *fait accompli* had to be made possible, that would paralyse and empty any possible will to react by the international community. Hitler had systematised this perspective, transforming it into a political paradigm, already in the meeting of 21 April 1938 with the leaders of the armed forces: "Politically speaking, the first four days of military action are decisive. Without significant military successes, a European crisis will certainly erupt. The *fait accompli* must convince foreign powers of the futility of military intervention."[21] It had to be "a lightning strike, the consequence of some serious incident which for Germany represents an intolerable provocation and which, at least in the face of a part of public opinion, offers a moral justification for military measures". In short, the necessary premises of military action were systematically built on a political and propaganda basis that condition its implementation and success. Manipulating international public opinion and dividing it by providing it with

[17] Shirer 1974.

[18] The absorption of Austria had made the defensive position of the Czechs very difficult.

[19] Shirer 1974.

[20] Koutek 1964.

[21] Shirer 1974.

formal anchors for disengagement was one of the preliminary tools of the action, which will count on the substantial isolation of the victims. Military action will have to find support, up to the operational level, from the fallout of propaganda itself and the pressures of economic warfare:

- "The propaganda war must, on the one hand, intimidate the Czechs by means of threats and wear down their resistance force; on the other hand, it must give national minorities instructions on how to support our military operations and influence the neutrals on our behalf.
- The economic war has the task of using all available economic resources to accelerate the final collapse of the Czechs [...]."[22]

## Coercion becoming "cross domain"

The intensification of the subversion activity of the Sudeten Germans and the rupture of these with the Prague Government for the management of autonomy were the background to the growing German military and diplomatic pressure "to protect the minority" and its good right on those territories. Faced with the threat of war, we were witnessing the gradual slide of diplomacy, especially British, towards openness to the demands of the Reich. While the *decalage* of Western guarantees developed rapidly in September, the diplomatic action of the Reich urged the push on all minorities, Hungarians and Poles and their countries to crumble Czechoslovakia. On the ground, units of Sudeten volunteers flanked by SS units militarily occupied cities on the border along the lines of a substantially planned "gray" sedition. The dissolving outcomes of Munich represented at that point the full success of "a new strategy and technique of political warfare that made effective war superfluous".[23] The acquiescence of the democracies would be quickly followed, at the beginning of 1939, by a further, hasty and impudent fait accompli, with the political "emptying" of what remained of the attacked country. The rapid military occupations of Bohemia and Moravia followed the disengagement of Slovakia. By similar means, a few weeks later, once again combining diplomatic intimidation and organised intemperance of local Germans, the Memel district was absorbed by Lithuania. The Bohemian case consolidated a practice that was now taking on systematic features. Political

[22] Shirer 1974: 561.

[23] Shirer 1974: 651.

dismemberment through the use of local actors was a necessary premise for the decisive effectiveness of the military occupation. This was directly requested only at the end of the path and in the form of “protection” of German minorities exposed to the “massacre” and victimised through internal unrest provoked artfully and transformed into imperative and suggestive messages in international communication. The direction was fully defined on the strategic level but assumed an “opportunistic” trend, tactically seizing all the opportunities to deepen the blows to the stability of the victim State and international support for it. Diplomatic deceptions were realised through “peace offers” that incorporated, in strategic ambiguity, both the implicit and coercive threat of a military escalation and the promise, each time repeated, of guarantees against any further claim. All this transformed the international arena of communication into a pulsating ground of tension. It was to amplify the weaknesses of democracies and the frailty of their permeable public opinions. In the Czech case, the result was an effective manipulation of the perception of danger through a renewed and extreme *bluff,* also making the scenario of a blatant aggression confusing – and ultimately acceptable. In the Polish case, immediately following, all this would have recurred with a more intense diplomatic and communication manipulation, passing from the mere sphere of propaganda to that of interference in cognitive and decision-making processes and on the determination to act of democracies in front of uncertainty. Among the tools adopted, the “fog of war” passed from the tactical level to settle also on the strategic one. Even the planning of the attack on Poland, the “Fall Weiss” that began to take shape in the aftermath of Munich, was nourished by a fundamental political approach. In those weeks, in fact, it was envisaged “a semi-revolutionary action in Danzig to take advantage of a favourable political situation, not a war against Poland”.[24] It was the last hypothesis that did not foresee an open armed conflict and was destined to fade in the light of the hardening of the line of democracies in front of the “fait accompli” against what remained of Czechoslovakia, of January 1939. At that point, however, the indications to the military still aimed to circumscribe the war scenario, on the basis of the certain political crisis of democracies and in particular of France, operating around the non-inevitability of their intervention. On the one hand, faced with the now defined line of Franco–British guarantees to Poland, democracies were accused of warmongering, trying to

[24] Shirer 1974: 706; Bergen 2008.

influence the determination of public opinion[25] (after all, the traditional congress of the Nazi Party that was to be held the following August, was to be called, almost mockingly, "Peace Congress"). On the other hand, the directives for military action incorporated a series of eminent political activities with a significant institutional interweaving between the actors, political and military, of the Nazi machine. Alongside the growing diplomatic intimidation through the exaltation of the power of German weapons,[26] an operational organisation developed in order to exhaust the Polish resistance very quickly, hypothetically in just two weeks.[27] A series of "surprise attacks" was to paralyse the mobilisation of Warsaw, while inside Danzig would have been immediately declared German territory and defended by local militias. The Nazi party, anticipating the action of the Wehrmacht, had in those months brought in arms and officers through East Prussia to train the local defence militia. A typical model of *ambiguous warfare* that mixed the action of non-state actors with the coverage and execution of properly state directives. Similarly, the Party's action became central to the organisation of an "incident" which, according to Hitler's precise and calculated directives, was supposed to justify the German September attack in the eyes of a hesitant international community. The SS-held "Operation Himmler" involved a fake Polish attack on the Gleiwitz border radio station, employing concentration camp inmates wearing Polish uniforms.[28] Actions that could hope to convince above all the internal front in Germany[29] but that certainly aimed to make confused, for the public opinion of democracies, even the scenario of a blatant aggression.[30] Mixed with a dense tissue of "last minute" negotiations aimed at nailing Poles to responsibility for a rejection of peace offers, these operations moved from the mere sphere of propaganda to that of interference in decision-making processes and the determination of democracies to act in front

[25] Shirer 1974.

[26] Shirer 1974.

[27] Shirer 1974.

[28] Shirer 1974.

[29] It was substantially isolated and invulnerable to propaganda from the outside since the materialisation of the *Gleichschaltung,* fully aligned, according to Shirer's solid testimony, with the idea of the threat of Polish criminal aggression towards the German people. In this dynamic, the typical asymmetry between authoritarian states and democratic societies, intrinsically exposed to the divisions and destabilising influences induced by the former, took fully shape.

[30] In this case too, Hitler would have peppered the last diplomatic and propaganda exchanges with the democracies with references to the martyrdom of the *Volksdeutsche* in Poland.

of uncertainty. The lightning nature of the military action could also make it possible to arrive at a new *fait accompli* by "isolating" the "Weiss Fall", while the Ribbentrop–Molotov pact helped to push France and the United Kingdom again – guided, in Hitler's vision, by "little worms" – towards the precipice of an unruly and paralysing "wisdom".[31] In the military conference of 22 August, Hitler gave as absolutely unlikely an attack from the West even in front of the now certain aggression against Poland and, around 25 August, imagined at most a possible "fake war" by Chamberlain, desperately looking for a way out of a concrete and general war. The Fuhrer postponed the attack, originally scheduled for 26 August, precisely in order to influence public opinion (the French in particular) and democratic governments, proposing a political "solution" to cling to. Possibly provoking a Polish rejection of "reasonable" proposals to anchor the abandonment, by democracies, of the commitments undertaken.[32] Moreover, right on the threshold of the war, Hitler himself confirmed that he had consciously achieved the long list of successes and annexations of previous years with the "political bluff".[33] We could say, with today's eyes, that deception and *reflexive control,* although not codified in a doctrine, dominated the scenario and accompanied the properly military action. Peace offers would arrive again from Hitler at the end of September with the last steps of the very rapid triumph in Poland to further survey and challenge the fragility of the opponents, whose operational immobility was eloquent. And reviving the exhausting factor of political action while in fact planning the military attack on the West. The season of the lightning spring offensives of 1940 would incorporate a "sensible integration between penetrating military action, diplomatic deception and[34] jamming operations built on the disguise and spread of chaos, as in the case of German soldiers disguised as Belgian and Dutch border guards in May 1940.[35] In this case there was, in coordination with military operations on the ground, an integrated form of *ambiguous warfare,* through the masked deployment of units, or even the simple looming possibility of infiltrating units or agents behind the lines. The use of airborne troops or paratroopers represented at that point one of the tools of psychological disintegration of the opposing front, even for the mere suspicion that these new

[31] Shirer 1974.

[32] Shirer 1974.

[33] Shirer 1974.

[34] Shirer 1974.

[35] Shirer 1974.

troops and tools, acted alongside elusive "accomplices" and local supporters, on a political-ideological, ethnic or corrupting basis.[36] State and non-State crossed each other, breaking solid fences and inaugurating the season of a "war without fronts".[37] Precisely this type of action became the stimulatory and coordinated ground for an intense activity of information accompaniment, of *white* or *black* propaganda, which strongly characterised the *psyops* character of many military operations. The unexpected and rapid capture by airborne units on gliders of the Belgian fort of Eben Emael, considered a modern and insurmountable defensive jewel, stood out as an enigma in the eyes of the allies and populations, both uncertain whether to attribute it to the betrayal of a fifth column or to the actual irresistibility of "new means of war" as a pounding German campaign deliberately leaked. Precisely the pounding scenario of the German advance and successes favoured a generalised collapse of the reaction capacity of the allies to which the dense tissue of propaganda and deception that accompanied them contributed. In fact, at that stage the activities of clandestine or "open" radio stations began. Sometimes mounted on trucks they were able to move along the borders or along the French and Belgian front to deceive with their propaganda populations and troops in retreat.[38] Radio broadcasts would increasingly turn into a direct terrain of war and its action would interfere with operational situations and their planning. The impact of "news" could become an immediate weapon and contribute directly to success. It was the starting point of that dense tissue of radio activities that took shape in the following weeks on the German side to prepare and accompany, with the poisonous suggestions of "English" voices, the attack on the British Isles.[39] Voices that were to amplify the sense of defeat and bewilderment as an expression of the authentic opinion of the English people, in front of the recalcitrant ruling classes who claimed to continue a war destined to become unsustainable and terrible, even when Hitler offered "generous" peace offers (in the impressive speech to the Reichstag of 19 July 1940). Not only flowed the open propaganda of William Joyce, a fugitive in Berlin and voice known as Lord Haw-Haw, but also the covert and insidious voice of the broadcaster "Concordia" after the success of similar operations in the French context. Three stations dedicated to different social segments and engaged both in the strategic

[36] Shirer 1974; Lagrou 2004; Vlaemynk 1977.

[37] Di Giovanni 1991.

[38] Salata 2020; Koestler 1989.

[39] Doherty 1994.

dissociation of the British people from their government, as well as in the tactical spread of panic and chaos. That summer thus became the scene of a campaign of rumours about widespread sabotage, actions of the fifth column and landings of paratroopers, growing up to the exhortation to revolt and escape in the psychological urgency of an impending invasion. Manipulate events to the point of paroxysm and urge listeners to disseminate their "authentic", catastrophic meaning. A dynamic that places us fully in the "revolutionary" circuit opened by the great transformation of information and that at the time prompted a series of initiatives from the British side, also on the basis of the weight attributed to German propaganda in the collapse of France. In May, the Political Committee at the Ministry of Information evaluated the information disseminated on German paratroopers and subsequently the fear spread that the broadcasts would dialogue directly with a fifth column on the territory. The result would be an "anti-rumour" campaign called "Silent Column".[40] At that stage an observation service was activated by the BBC to combat false news (the so-called "Anti-Lie Section", BBC Monitoring Service). In the growing German difficulty of preparing a complex operation like "Sea Lion", the propaganda and internal disintegration of the British could still appear to General Jodl, second at the top of the OKW, a tool to amplify the physical and moral effects of the bombings, opening the way to a possible solution without invasion of the island.[41] From then on, however, the domination of arms and the policy of occupation would define other priorities in the strategic complex of the instruments of war.

## World War II and the non-linear legacies of the Cold War

The scenario was no longer in a single direction and even the British information and military structures had begun to move, although they would have tended to characterise themselves in a decidedly different way.[42] The transformation of the war into a long-lasting total conflict placed the whole and the combination of the "new" instruments tested in a secondary and subsidiary position with respect to the dominant kinetic dimension. The Allies declined some of the instruments matured in that season according to the conduct of a war that had to rest, on

[40] Doherty 1994.

[41] Shirer 1974.

[42] Plock 2020.

the strategic level, on an overwhelming military superiority. However, that war developed the relationship with the populations of occupied Europe and collaboration with resistance movements, with an intrinsic political dimension. Therefore, the external activities of the BBC[43] and a specific declination of propaganda grew, while agencies were born aimed precisely at developing the integration between information action and kinetic operations and the development of tools specifically dedicated to *psyops.* They combined (according to a British model of "unorthodox warfare") different paths and activities that included, in addition to the acquisition of information, *Political Warfare* oriented to propaganda and deception or to the activation of subversion in local areas, sabotage and direct action, up to the organisation of close operational combinations between special forces and Resistances, as happened on the occasion of Overlord.[44] In the British context with the SOE and in the USA with the Coordinator of Information and later with the OSS, there were organisational and doctrinal developments that institutionalised the experience in progress.[45] The path would continue even after the end of the war but confirming a clear sign, especially in the American context: the strategic dimension belonged to other sectors, and the Army favoured a fully conventional vision of the military instrument.[46] It was the pressure of the Cold War (Korea) that forcefully re-proposed the political dimension of the war and led to the creation of a new agency in the USA, the Office of the Chief of Psychological Warfare in 1951. From here the 10th Special Forces Group was born to train "indigenous" personnel who acted behind the lines of territories invaded by the USSR. A position distinct from the elite units of the Army, wary of unconventional scenarios. It was an area also disputed by other "political" agencies. The consolidation came with the creation in Fort Bragg of a Psychological Warfare Center (1952) which collected under a specific doctrinal profile both *the psyops* and Unconventional Warfare, doctrinally reserved for direct action or combined with external actors of the Special Forces.[47] The Cold War scenario, therefore, included an intense recourse by military actors to specific tools more or less "covered" and operating in a gray area. For the USSR, military intimidation, covert operations and incitement to political dissent, the general information war

[43] Pronay–Taylor 1984; Taylor 2007; Graham 2019.

[44] Kilcullen 2019.

[45] Paddock 1980.

[46] Paddock 1980.

[47] Paddock 1980.

of subversion that was part of the "active measures"[48] represented some of the areas of the "gray zone" destined to remain doctrinal heritage until today's Russian Federation.[49] Both actors also defined a strong propaganda action, with dedicated radio broadcasts behind the "curtain" and other diversified forms of influence, but in the framework of a confrontation that, despite the many peripheral declinations, gravitated around other strategic priorities and did not make the gray area the systemic pivot of its perspective.

## Conclusion

The arrival of our path is placed in front of the effects of the new and extraordinary transition of the communication and information environment inaugurated in the new millennium. A complex scenario of which we only seek to indicating some aspects connected to the strategic opportunities that open up in the confrontation between different political systems. A picture that brings us back to the great strategic transformation we have been dealing with. The appearance, in the second decade of our Century, of aggressive revisionist actors, Russia and China in particular, can be linked to many factors, but certainly among these must be counted the growing vulnerability of open societies with a democratic character, what, in a general sense, we call "the West". New technologies make non-linear instruments in the Gray Zone more effective and place them strategically at the forefront of the military dimension. That is, it opens up a field of action that lies below and alongside the technological and military superiority of the West. The technological environment in transformation multiplies the friction surfaces and seems to welcome in its widest folds spaces for actions not easily attributable, areas of plausible deniability. A situation that fully favours the deployment of aggressive operations in the gray area and their strategic importance. A transformation that enables the democratisation of operational capacities up to very reduced organisational levels, through the potential weaponisation of ordinarily civilian instruments. Nevertheless, it also feeds the combination from above, and on the platform of the State, of a set of activities potentially integrated, opaque and not recognisable in the actors and intentions. Tools and methods so effective in their joint action that they can produce the erosion at various levels of the

[48] Cristadoro 2022.

[49] Morris et al. 2019.

compactness and resilience of the target country, finalising to the maximum the opportunities offered by this renewed and deep Gray Zone, configuring it as a new area of war.[50] The revisionist powers seem in fact particularly structured to make use of it, slipping under the constraints apparently imposed by the superiority of the West and emphasising the substantial asymmetry in the penetrability of "information", in the control of internal political dynamics, in the internal and external relevance of legal *pivots.* Not only explicit propaganda, but the structured practice of intoxicating information, delegitimising institutions and the authority of the State, simply creating uncertainty and chaos. These are elements that converge strategically in shaping a socio-political environment incapable of responding when concrete challenges arise. Specific political processes active in modern post-ideological and social-media oriented democracies, such as institutional disintermediation and accreditation of populist policies, have exalted the destructive permeability to these threats. "Reflexive control" and the sequential violations of rules *(slicing salami)*[51] therefore articulate revisionist itineraries that feed on ideological conviction and concrete and continually solicited manifestation of the fragility and vulnerability of the West.[52] Not simply War but War. The action of the Russian Federation is extremely eloquent and disturbing. The threshold crossed on 24 February 2022 calls us to recognise the cognitive biases that had conditioned our perception of the ideological determination of the Russian actor, and the actual maturation, in his perspective, of the decadence of the West. Confusing once again for "pragmatism" an opportunism nourished by a precise ideological and strategic vision that was able to feed, failed yet another *fait accompli,* a war of the "colonial" type that brings the hands of history back to where all this began. Hitler operated according to a project in which pragmatism had a place in a purely tactical perspective. Planning on an ideological basis determined the direction of the march consciously destined to lead to war as the political-military annihilation of the adversary. The ideological approach and political determination made it possible to identify and exploit a set of tools – typical of that age in transformation – capable of plunging into the systemic fragility of opponents, strategically building the foundations of the final military deployment. A threshold used in a coercive perspective and crossed, in Hitler's expectations, to complete the work of erosion of the enemy long started

[50] Matisek 2017; Jonsson 2019.

[51] Adamsky 2015.

[52] Adamsky 2018.

by operating at various levels on its vulnerabilities. The great transformation of information, networks, and of what is integrated with them, which increasingly characterises the new millennium, opens the space for a wide and deep Gray Zone in which non-state and, in particular, state actors, can act in the midst of plausible deniability and/or with predominantly non-military instruments to erode the stability of target countries. Democracies appear particularly vulnerable to this type of disruption. The new revisionist and autocratic powers, guided by an approach ideologically based on the conviction of the irreversible decline of the West and the weakness of democracies, exert on this sphere an articulated and multilevel erosive action, organic on the strategic level. This erosive action today appears not only substitutive, but potentially preparatory and preliminary to the full deployment of military actions.

## Questions

1. Which are the main features of the Non-Linear Warfare in the nineteen-thirties?
2. How do revisionism and NLW connect? Think about it.
3. What are the fragilities, yesterday and today, of democracies in the face of non-linear threats?
4. What are past and present examples of the abuse of the claims of national minorities in internal subversion?

## References

Adamsky, Dmitry (2015): *Cross-Domain Coercion: The Current Russian Art of Strategy.* Paris: IFRI Security Studies Centre.

Adamsky, Dmitry (2018): From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture. *Journal of Strategic Studies,* 41(1–2), 33–60. Online: https://doi.org/10.1080/01402390.2017.1347872

Basseches, Nikolaus (1945): *L'esercito russo.* Milano: Bompiani.

Bassenge, Emilio (1939): Le fanterie dell'aria. *Rivista Aeronautica,* (15)3, 580–586.

Bergen, Doris L. (2008): Instrumentalization of Volksdeutchen in German Propaganda in 1939: Replacing/Erasing Poles, Jews and Other Victims. *German Studies Review,* 31(3), 447–470.

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

Di Giovanni, Marco (1991): *I paracadutisti italiani. Volontari, miti e memoria della seconda guerra mondiale.* Gorizia: LEG.

Doherty, Martin (1994): Black Propaganda by Radio: The German Concordia Broadcasts to Britain 1940–1941. *Historical Journal of Film, Radio, and Television,* 14(2), 167–197. Online: https://doi.org/10.1080/01439689400260141

Fridman, Ofer (2012): *Strategiya. The Foundations of the Russian Art of Strategy.* Oxford: Oxford University Press.

Fridman, Ofer (2018): *Russian 'Hybrid Warfare'. Resurgence and Politicisation.* Oxford: Oxford University Press.

Godson, Roy – Wirtz, James J. (2011): *Strategic Denial and Deception. The Twenty-First Century Challenge.* London: Transaction Publisher.

Graham, Kirk Robert (2019): Germany on the Couch: Psychology and the Development of British Subversive Propaganda to Nazi Germany. *Journal of Contemporary History,* 54(3), 487–507. Online: https://doi.org/10.1177/0022009417739365

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

Kilcullen, David (2019): The Evolution of Unconventional Warfare. *Scandinavian Journal of Military Studies,* (2)1, 61–71. Online: https://doi.org/10.31374/sjms.35

Koestler, Arthur (1989): *Schiuma della terra.* Bologna: Il Mulino.

Koutek, Jaroslav (1964): *Quinta colonna all'Est. I nazisti in Cecoslovacchia 1933–1938* [Fifth Column in the East. The Nazis in Czechoslovakia 1933–1938]. Roma: Editori Riuniti.

Lagrou, Pieter (2004): La guerra irregolare e le norme della violenza legittima nell'Europa del Novecento. In Baldissara, Luca – Pezzino, Paolo (eds.): *Crimini e memorie di guerra. Violenze contro le popolazioni e politiche del ricordo.* Napoli: L'ancora del Mediterraneo, 89–102.

Matisek, Jahara W. (2017): Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security,* 10(3), 1–26. Online: http://doi.org/10. 5038/1944-0472.10.3.1589

Mengel, William H. (2007): *Guerilla Diplomacy: Germany and Unconventional Warfare, 1884–1945.* PhD Thesis. Harvard University.

Modrzejewski, Zbigniew (2016): Psychological Operations after the Second World War. *Security and Defence Quarterly,* 12(3), 74–99. Online: https://doi.org/10.35467/sdq/103237

Morris, Lyle J. – Mazarr, Michael J. – Hornung, Jeffrey W. – Pezard, Stephanie – Binnendijk, Anika – Kepe, Marta eds. (2019): *Gaining Competitive Advantage in* *the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War.* Santa Monica: Rand.

Orlow, Dietrich (1999): A Difficult Relationship of Unequal Relatives: The Dutch NSB and Nazi Germany, 1933–1940. *European History Quarterly,* 29(3), 349–380. Online: https://doi.org/10.1177/026569149902900302

Paddock, Alfred Harlan (1980): *Psychological and Unconventional Warfare, 1941–1952: Origins of a "Special Warfare" Capability for the United States Army.* PhD Thesis. Duke University.

Perkins, John (1991): The Swastika Down Under: Nazi Activities in Australia, 1933–39. *Journal of Contemporary History,* 26(1), 111–129.

Plock, Vike Martina (2020): Erika Mann, the BBC German Service, and Foreign-Language Broadcasting during WWII. *Modernism/Modernity,* 27(1), 103–123. Online: https://doi.org/10.1353/mod.2020.0004

Pronay, Nicholas – Taylor, Philip M. (1984): 'An Improper Use of Broadcasting...' The British Government and Clandestine Radio Propaganda Operations against Germany during the Munich Crisis and After. *Journal of Contemporary History,* 19(3), 357–384. Online: https://doi.org/10.1177/002200948401900301

Raychev, Yavor (2019): Roots of the Concept of Hybrid War in Russian Political and Military Thought. *Balkan Social Science Review,* 13, 127–151.

Salata, Oksana (2020): The Radio Propaganda as an Innovative Element of the Military Tactics and Strategies of the Nazi Germany 1933–1941. *Skhid,* 166(2), 42–47. Online: https://doi.org/10.21847/1728-9343.2020.2(166).201722

Schuttel, Lothar (1938): *Falschmirtruppen und Luftinfanterie.* Berlin: Mittler.

Shirer, William R. (1974): *Storia del Terzo Reich.* Torino: Einaudi.

Shirer, William R. (1986): *Gli anni dell'incubo 1930–1940.* Milano: Mondadori.

Sinovets, Polina (2016): From Stalin to Putin: Russian Strategic Culture in the XXI Century, Its Continuity, and Change. *Philosophy Study,* 6(7), 417–423. Online: https://doi.org/10.17265/2159-5313/2016.07.002

Taylor, Philip M. (2007): 'Munitions of the Mind': A Brief History of Military Psychological Operations. *Place Branding and Public Diplomacy,* (3)3, 196–204. Online: https://doi.org/10.1057/palgrave.pb.6000064

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

Vlaemynk, Carlos (1977): *Dossier Abbeville.* Leuven: Davidsfond.

Weinberg, Gerhard L. (1995): Propaganda for Peace and Preparation for War. In *Germany, Hitler and World War II.* Cambridge: Cambridge University Press, 68–82.

Valter Coralluzzo[1] – Fabio De Ninno[2]

# Maritime Coercion and Gray Zone Conflicts

The purpose of this chapter is to provide a broad introduction to issues related to the so-called *gray zone conflicts,* usually described as the space between peace and war. This is a (relatively) new and increasingly relevant form of warfare in which actors seek to achieve their security objectives, or gain strategic advantage, without resorting to direct use of military force, but by engaging in covert or illegal activities that are below the threshold of armed organised violence and do not escalate into war. While such conflicts take place in every domain (land, sea, air, space, cyberspace), the chapter considers only the maritime domain, where, according to the lesson of sea power theorists, the game for regional and world hegemony is being played more and more evidently. After reviewing some cases of gray zone coercion concerning other crucial quadrants of maritime geopolitics, the chapter focuses on the Indo-Pacific region, and especially the South China Sea (SCS) and East China Sea (ECS), where Beijing has long been employing gray zone coercion tactics and strategies in order to gradually change the regional (but also global) status quo in its favour without triggering military conflict or eliciting an anti-Chinese backlash. Some brief considerations on how to develop a coherent and effective strategy to coping with the main gray zone challenges in the maritime domain, particularly that of Southeast Asia, complete the chapter.

## Understanding gray zone conflict

Contrary to what who thinks in terms of a binary peace–war distinction seems to believe, "the space between war and peace in not an empty one, but a landscape churning with political, economic, and security competitions that require

[1] University of Turin. Author of the *Understanding gray zone conflict; China's maritime gray zone operations; How to counter China's gray zone strategy at sea?* subchapters.

[2] University of Siena. Author of the *Gray Zone operations at sea* and *Case studies of maritime coercion* subchapters.

DOI: https://doi.org/10.36250/01237_08

constant attention".[3] Nowadays, many scholars routinely refer to this space as a *gray zone* characterised by conflictual but non-war interactions. In short, gray zone strategies are seen as 'contests of initiative' in which a state eager to change some aspects of existing international environment benefits from moving first and implementing, through the use of military, paramilitary, and/or unconventional capabilities, a strategy of political coercion aimed at forcing opponents into complying with his revisionist goals, but without escalating to overt warfare.[4] In other words, engaging in a gray zone strategy is to make "an effort or series of efforts beyond steady-state deterrence and assurance that attempts to achieve one's security objectives without resort to direct and sizeable use of force".[5] Clearly, despite its perceived novelty, what the concept of gray zone conflict tries to describe, that it is an "activity that is coercitive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war",[6] seems anything but new:[7] it is a well-known phenomenon that has been referred to in the past (and still is referred to) by other names such as low-intensity conflict, military operations other than war, or hybrid, asymmetric, nonlinear and unconventional warfare.[8] Some analysts consider the concept of gray zone conflict to be largely overrated, if not downright meaningless and analytically useless.[9] They argue that gray zone theorists, including under that label too wide a range of behaviours, end up transforming the gray zone "into a catchy catch-all that encompasses nearly all forms of modern conflict, and thus tell us nothing useful about any of them".[10] It is well understood, therefore, why it is essential to define and circumscribe this concept as precisely and rigorously as possible. According to its best-known definitions, gray zone conflict can be conceptualised as "anything short of conventional

[3] Schadlow 2014.

[4] Kuo 2020.

[5] Green et al. 2017: 21.

[6] Brands 2016.

[7] Kapusta 2015.

[8] It has been noted by several scholars that the concept of hybrid warfare seems to be broad and expansive enough to include gray zone strategies. Hybrid and gray zone strategies are certainly related but not synonymous: hybrid warfare methods are generally more violent, therefore, only a select subset of them can be employed in gray zone strategies seeking to maintain short of threshold that results in war. Green et al. 2017; Patalano 2018.

[9] Elkus 2015.

[10] Brands 2016.

war which leverages multiple instruments of national power to intentionally achieved limited, instead of outright, political victories in a deniable manner to gain influence over a system or actor".[11] More precisely, Michael J. Mazarr argues that such a form of conflict:

- pursues political objectives through cohesive, integrated campaigns
- employs mostly non-military or non-kinetic tools
- strives to remain under key escalatory or red line thresholds to avoid outright, conventional conflict
- moves gradually towards its objectives rather than seeking conclusive results in a specific period of time[12]

As scholarly literature suggests, the defining features of gray zone coercion are: measured revisionism, asymmetry, ambiguity, attributive deniability, unconventional tools and tactics, and strategic gradualism. First of all, gray zone strategy is mostly the province of moderately (but not radically) revisionist powers, that is countries dissatisfied with certain aspects (such as rule-setting influence and power–goods distribution) of the existing status quo and their current position, at the regional and/or global level. Alexander Lanoszka notes that gray zone belligerents (and this is all the more true for moderate revisionist states), lacking global (while having local) escalation dominance,[13] are determined to enhance their relative power and capture more influence, but without incurring the costs and risks of a retaliation by stronger, often extra-regional states or coalition of states.[14] In sum, following Michael Green et al., it can be said that "gray zone coercion is most likely when a potential challenger is dissatisfied but the dominant power retains escalation dominance":[15] in such a condition, a dissatisfied state is encouraged to seek more limited changes to the status quo and pursue its strategic goals through more cautious and gradual approaches, through ambiguously aggressive actions designed not to cross the level that usually triggers

[11] Lamb 2020: 4.

[12] Mazarr 2015: 58.

[13] Herman Kahn described escalation dominance as "a capacity, other things being equal, to enable the side possessing it to enjoy marked advantages in a given region of the escalation ladder. […] It depends on the net effect of the competing capabilities on the rung being occupied, the estimate by each side of what would happen if the confrontation moved to these other rungs, and the means each side has to shift the confrontation to these other rungs". Kahn 2010: 290.

[14] Lanoszka 2016.

[15] Green et al. 2017: 29.

conventional military response. It is precisely from the tension between local and global escalation dominance that the other key characteristics of gray zone strategy follow.[16] The first is asymmetry, which can relate to both capabilities (especially military ones, on which escalation dominance heavily depends) and interests (when for example a state values an objective or a disputed issue more than does its adversary, to the point of being more willing, ceteris paribus, to take risks, what may explain why weaker states sometimes win wars against stronger ones). The second is ambiguity, which can take two forms: on the one hand, information ambiguity creates vagueness about facts, and "makes it difficult for other parties to determine what happened, where, when, by whom, and why"; on the other hand, normative ambiguity "makes it difficult for other parties to determine whether a law was broken, a norm was violated, a treaty commitment should be invoked, or even whether the status quo was altered".[17] Moreover, the inherent ambiguity of gray zone challenges exacerbates the problem of plausible and implausible deniability because in order to extract concessions from weaker neighbours, and simultaneously provide them or stronger third-parties a possible rationale to avoid (or otherwise delay) their engagement or escalation, measured revisionists employ a broad range of gray zone coercion tactics that "are frequently shrouded in misinformation and deception, and are often conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down".[18] Among these unconventional practices, "that make attribution too uncertain to justify lethal response",[19] figure severe political and economic coercion, information and disinformation activities, large-scale cyber and space operations, covert actions and proxy support (that is use, whether direct or not, of non-state and para-state groups in order to implement militarised forms of intimidation or territory control), provocation by state-controlled non-military or paramilitary forces and presenting *faits accomplis*[20] to status quo states, sidestepping their redlines and undermining credibility of their commitments and deterrent threats. Finally, the last defining feature of gray zone conflict is that it is gradualist in nature. What can be called strategic gradualism, otherwise

[16] Kuo 2020.

[17] Green et al. 2017: 32.

[18] Brands 2016.

[19] Lovelace 2016: ix.

[20] A *fait accompli* strategy is an effort "to achieve the objective so quickly so as to deprive the defender of the time and opportunity to reverse his policy". George–Smoke 1974: 537; Altman 2017.

known as *salami slicing*[21] or *cabbage peeling,*[22] is a refined incremental approach (already discussed in Thomas Schelling's classical work, *Arms and Influence*)[23] that, in Robert Haddick's words, "involves the slow accumulation of small changes, none of which in isolation amounts to a casus belli, but which add up over time to a substantial change in the strategic picture".[24] Mazarr, for his part, notes that "gradualist approaches are especially appealing to *measured revisionists*":[25] such states, in fact, while employing sequences of incremental moves calculated to unfold over time, bit by bit, rather than to achieve rapid, decisive results, nonetheless manage these moves to sum up to a significant change in the status quo that cannot be reversed except through an escalation that may lead to open conflict. By means of this strategy, also definable as "tailored coercion for incremental revisionism",[26] it is possible to test the reactions of the adversaries and understand to what extent the use of low-intensity coercion is permitted and when it is countered with the threat or use of force.

## Gray zone operations at sea

Coercion at sea below the threshold of open conflict is not a new phenomenon. Forms of armed suasion have been largely used in peacetime to influence international politics at sea, being defined as "gunboat diplomacy".[27] Gray zone

[21] *Salami slicing tactics* can be described as the revisionist practice of slowly (step-by-step) changing the 'facts on the ground', maybe through a series of limited *faits accomplis,* in order to overcome status quo defenders, whose opposition is reduced slice by slice until they realise (usually too late) that they have been completely neutralised and are faced with a dramatic change in the strategic picture (which would have produced a severe crisis, or war, if one had tried to get it all at once) and a dilemma of acquiescing or pursuing a dangerous escalation.

[22] *Cabbage peeling* is a strategy (widely used by China) of setting up infrastructure on disputed islands and then surrounding them with layers composed of fishing boats, coast guard lookouts and warships so that the island remains wrapped, layer by layer, like cabbage.

[23] According to Schelling, "if there is not sharp qualitative division between a minor transgression and a major affront, but a continuous graduation of activity, one can begin his intrusion on a scale too small to provoke a reaction and increase it by imperceptible degrees, never quite presenting a sudden dramatic challenge that would invoke the committed response" Schelling 2008: 67.

[24] Haddick 2014.

[25] Mazarr 2015: 38.

[26] Cronin et al. 2014: 6.

[27] Cable 1999: 1.

operations can be considered an evolution of these traditional forms of coercion, caused by the changes in international landscape, technological change, and an increased involvement of non-military forces as a form of "para-gunboat diplomacy".[28] Pivotal in the definition of gray zone conflicts at sea has been the process of territorialisation of the seas that began in the second half of the previous century, marked by the United Nations Convention on the Law of the Sea (UNCLOS) of 1982. The UNCLOS laid down a comprehensive regime of international law establishing rules for the governance of the oceans, navigation, archipelagic status, transit regimes, exclusive economic zones (EEZs), continental shelf jurisdiction, deep seabed mining, the exploitation regime, protection of the marine environment, scientific research and settlement of disputes. Nevertheless, UNCLOS and territorialisation also sparked increased disputes over maritime jurisdiction, military presence and activities.[29] Current gray zone activities and coercion campaigns at sea are strictly related to claims of sovereignty or sovereign rights over geographical features or water areas. These claims often are used to mount pressure on a country more than to search for a specific solution to a maritime issue. The conduct of powers in gray zone operations usually differs according to the relative strength of the actors involved. Weaker power can employ gray zone activities against a stronger opponent and vice versa with different conduct. In this context, the stronger power usually will not start kinetic exchanges, trying instead to provoke a military response by the weaker power to make the latter appear as the aggressor in an ensuing conflict that it will lose. The scope of gray zone coercion at sea is not to obtain an absolute undermining of the opponent's capability to exercise control of maritime areas. Instead, it is to exercise sufficient interference to undermine the feasibility of another state's control over the sea. Activities of this type can include disruption of offshore activities and offshore petroleum exploration and exploitation. Another key feature is the disruption of maritime traffic. Indeed, merchant ships are also susceptible to gray zone operations: the necessity to avoid conflict could lead to longer routes or the passage to unsafe areas to higher insurance costs. In the last two decades, Russia and China have been excellent examples of this approach to gray zone operations, using a more substantial level of coercion against weaker opponents

[28] Le Mière 2014: 30. Criticism of the gray zone as something new is expressed by Stoker–Whiteside 2020.

[29] Klein 2011.

than would have done against peers or even opponents.[30] For the conduct of gray zone operations non-military forces are pivotal like sea-borne militias, police forces, coast guards and even flotillas of fisherfolk motorboats to avoid open military confrontation.[31] Finally, cyber warfare can impinge on the realm of gray zone operations at sea through cyberattacks against shipping computer systems and the cutting of undersea hydrophone networks and internet cables, damaging navigation infrastructure. Indeed, maritime shipping technologies are vulnerable to attacks to manipulate data, blurring traditional lines between maritime shipping and security. For example, Russia has been called out for cyber hacking technologies related to the Automatic Identification System (AIS) used to share weather station data or to prevent collisions, primarily through narrow waterways.[32]

## Case studies of maritime coercion

The previously underlined characteristics of gray zone operations at sea have already been consolidated in a rich history of examples. Precocious developments were the 'Cod Wars' of 1958–1976. The dispute saw a weaker nation, Iceland, challenging the status quo by combining gray zone activities and political pressure against a stronger opponent, the United Kingdom. The dispute began in 1958 with the unilateral extension of Icelandic territorial waters from 4 to 12 miles from the shoreline. The U.K. replied by sending military vessels to protect British trawlers. The dispute continued in the following two decades due to the extension of Iceland's fisheries limit to 50 miles from the shoreline (1972). It concluded in 1976 with an agreement on the extension to a 200-miles limit of the Icelandic EEZ. During the dispute, Icelandic patrol ships employed wire cutters for the first time, cutting the trawling wires of British trawlers, sabotaging their fishing and endangering their crews. The British opposed Icelandic claims because they could establish a precedent that could impede the Royal Navy from travelling freely and projecting power and cause the expulsion of British fishing fleets from other fishing grounds. Despite its weakness, Iceland won the

[30] Goldrick 2018.

[31] Singh 2018; Martinson 2015; Werner 2018.

[32] Gresh 2020.

dispute and coerced into accepting its claims.[33] Since the launch of the FON (Freedom of Navigation) policy in 1979 and especially after the signing of the UNCLOS convention of 1982, the U.S. Navy engaged in gray zone activities, usually in the form of FONOPs (Freedom of Navigation Operations). The scope of these operations is to challenge unilateral maritime claims impinging on the freedom of the seas. Operations are divided into FON assertions (that is, operations with the primary purpose of challenging excessive maritime claims) and other FON-related activities (that is, operations with some other primary purpose but having a secondary effect of challenging excessive maritime claims).[34] In some cases, as in the 1981 Gulf of Sidra incident, FONOPs led to the use of lethal force. On that occasion, two Libyan MiGs were shot after firing a missile against a U.S. F-14 employed in a naval exercise. The U.S. Navy was deliberately training in a maritime space claimed by Libya, an attitude consistent with the U.S. FON policy of directly challenging territorial waters claims the U.S. refuses to recognise.[35] The incident remarks on the porosity of the border between gray zone operations and open conflict. In general, however, gray zone coercion is usually less violent. Due to its strong territorialised character, the Mediterranean Sea offers some key examples. In 2013, Spain employed gray zone activities in the waters of Gibraltar, including unauthorised oceanographic research and restrictions on the movement of people and goods across the border. The objective was to stop the construction of an artificial reef in Gibraltar. Britain replied by sending warships to exercise in the Mediterranean. Spanish pressure was a peculiar case of gray zone activities combining coercion both at sea and on land toward reaching a maritime objective.[36] In 2018, coercion was employed also by Turkish warships blocking an Italian rig from reaching an area off Turkish Cyprus to start natural gas explorations.[37] Iran and Russia have proven among the most aggressive users of gray zone operations in the maritime domain. Iran's gray zone operations at sea are part of its broader attempt to use perceived American fear of escalation to an undesired all-out war, giving Iranian gray zone operators great freedom to act. The aspect is evident in the development and operations of the Islamic Revolutionary Guard Corps Navy (IRGC), with its

[33] Steinsson 2016.

[34] U.S. Department of Defense 2017.

[35] Ratner 1984.

[36] Del Valle Gálvez 2013.

[37] Caffio 2018.

large inventory of fast light attack craft adapted for 'guerrilla operations at sea', the Iranian use of proxy elements for attacks against international shipping in the Gulf of Oman, and the seizure of tankers by the IRGC, as bargain chip against western economic sanctions.[38] Before the war in Ukraine, Russia's infiltration of submarines in other Baltic nations' territorial waters was considered by experts a form of intimidation, coercion and area denial. This tactic aimed to increase Russia's theoretical area of control and accomplish its political goals without escalating to direct conflict. At the same time, other nations are required to be cautious and defensive. Similar coercion could have been the aim of the Russian deployment of A2/AD (which stands for anti-access area denial) capabilities in the Eastern Mediterranean, this time against Greece and Egypt.[39] In December 2018, Russia also used movement disruption against the Ukrainian naval forces, preventing a tugboat and two gunboats of the Ukrainian Navy from entering the Azov Sea from the Black Sea to reach the port of Mariupol. Russian coastguard vessels, backed by military aircraft and helicopters, rammed the Ukrainian ships and opened fire, injuring six Ukrainian sailors and capturing the Ukrainian crew members, later detained. At that time, Russia still denied its involvement in Ukraine, starting with the 2014 annexation of Crimea and the proclamation of the two separatist republics in the eastern part of the country. According to James Kraska, the incident demonstrates "how adept Russia is at exploiting the seam between the contending peacetime and wartime legal dimensions of the Crimea conflict to create perceptions of a "gray zone" that effectively advance its geopolitical agenda while confusing and demoralizing its critics".[40]

## China's maritime gray zone operations

Undoubtedly, China's rapid emergence as a "true maritime power"[41] that can effectively challenge dominant U.S. influence in the Indo-Pacific region

[38] Eisenstadt 2021; Truver 2020; Nadimi 2020.

[39] Hicks et al. 2016; Altman 2016.

[40] Kraska 2018.

[41] The goal of building China into a *true* "maritime great power" (MGP), as repeatedly stated by President Xi Jinping (whose emphasis on the term 'true' "implies something more than a mere passive facticity", in so far as "it suggests an active plan to produce some kind of significant transformation"), is a central pillar of Beijing's overall strategy aimed at pursuing the 'Chinese dream' in the context of China's 'peaceful rise' and 'national rejuvenation' Yoon 2015: 40, 59.

represents a leading example of gray zone maritime coercion. In this decisive geopolitical quadrant, and especially in the South China Sea (SCS) (called by Robert Kaplan the "throat of global sea routes" and "the 21st century's defining battleground"),[42] Beijing pursues, in fact, its revisionist goals almost entirely in the gray zone, employing "different combinations of influence, intimidation, coercion, and veiled aggression to approach, probe, and, at times, violate perceived U.S./partner redlines while skilfully remaining below the threshold of outright military provocation".[43] Mostly, Chinese activities in the SCS and East China Sea (ECS), while including frequent acts of bullying and intimidation, are carefully calibrated to achieve warlike ends without resorting to warlike violence. These activities have now taken the form of a coherent multidimensional (insofar it involves a broad range of national capabilities) campaign of pressure and creeping expansionism aimed at promoting China's maritime rights and interests (such as asserting its sovereignty on and around contested reefs, shoals and islands in 'near-seas'), but even more at shifting in China's favour the power dynamics that have ensured stability and U.S. primacy in the Indo-Pacific region since the end of World War II. This power-based approach, which can best be described as "nonmilitarized coercion"[44] and contributed to jeopardise geopolitical equilibrium in the region feeding more and more fears about conflict escalation at sea, is perfectly consonant with China's measured revisionism and adoption of a gray zone strategy. Such an approach, as noted above, leverages a wide range of tools and techniques (military, economic, political, diplomatic, legal, communicative and others), including more and more aggressive commercial expansion, intimidating the use of non-violent coercive military force, explicit rejection of the principle of multilateral diplomacy to leverage unequal power in bilateral relations, extensive exploitation of cyber and information operations, increasing island-building and base-construction activities so as to enhance A2/AD capabilities and counter opponents' military interference, strengthening maritime law enforcement capabilities and reorganisation of civilian agencies, "increased tempo operations by maritime law enforcement vessels in disputed areas – all in coordination with civilian fishing vessels, in what might be termed a maritime-style 'People's War'."[45] While the People's

[42] Kaplan 2011: 80.

[43] Freier 2016: 33.

[44] Dutton 2014: 10.

[45] Dutton 2014: 11.

Liberation Army Navy (PLAN) warships, never far from any assertive action in disputed waters, are usually available over the horizon as reserve forces serving to deter China's opponents from considering escalation, a key contribution to Beijing's gray zone operations in the SCS and ECS has come from Chinese maritime law enforcement agencies:[46] these are the China Coast Guard (CCG), which in recent years has rapidly increased in size and modernised its forces, significantly improving China's capacity to assert and defend its maritime claims and to conduct extended offshore operations, and the People's Armed Forces Maritime Militia (PAFMM), which is a subset of Chinese national militia (an armed reserve force of civilians available for mobilisation to perform basic support duties) essentially consisting of vessels indistinguishable from ordinary fishing boats, and that therefore "often puts foreign navies in the quandary of not knowing whether the Chinese craft they encounter are state directed".[47] Clearly, the use of gray zone coercion tactics through the CCG and PAFMM turns out to be doubly advantageous for China: on the one hand, the two agencies (the former operating on the pretext of routine law enforcement, the latter pretending to consist only of ordinary fishermen) "allow Beijing to advance its maritime claims vigorously without being criticized of using traditional gunboat diplomacy to press for its geopolitical objectives"; on the other hand, "the use of these agencies, particularly the PAFMM, provides China some level of plausible deniability should certain operations do not go according to plan".[48] Over the past 15–20 years, in addition to building a modern blue-water Navy,[49] Beijing has employed all these (and other) tools and techniques to support a long series of coercive (but short of war) actions in the Southeast Asian maritime domain. The main goal pursued through this gray zone strategy is to gain

[46] It is worth noting that, according to Alessio Patalano, the gray zone construct, insofar uncritically assumes that the use of force is designed not to cross the threshold of outright military conflict, is particularly problematic within the context of Chinese military and constabulary coercion at sea. Since constabulary coercion, Patalano writes, "is subordinated to the broader objectives of military coercion", which in turn "is a function of a broader strategic intention to project military power within and beyond the confines of the ESCS [that is East and South China Seas], whilst preventing others to do the same […] the hybrid vocabulary better captures the objective risk that war may actually happen if prolonged and systematic acts of coercion are not fully addressed". That is why, according to the author, Chinese maritime coercion is much better described as part of a hybrid strategy than as a gray zone strategy. Patalano 2018: 811, 819.

[47] Tobin 2018: 32.

[48] Galang 2021.

[49] Fanell 2019.

control of the islands and maritime areas included in the so-called nine-dash line (also known as the U-shaped line or the cow tongue), which is a demarcation line first used by the Chiang Kai-shek government in 1947, and adopted with minimal changes in 1949 by the People's Republic of China (PRC), to indicate China's maritime boundaries in the SCS. The area inside the nine-line segments (that, if connected, would enclose an area covering roughly 90% of the SCS) "far exceeds what is claimable as territorial waters under customary international law of the sea as reflected in UNCLOS, and includes waters that are within the claimable EEZs (and in some places are quite near the coasts) of the Philippines, Malaysia, Brunei, and Vietnam".[50] An even better understanding of China's strategic goals in the SCS and, more broadly, in the Indo-Pacific region is gained by referring to the 'two island chain strategy', first formulated in the 1980s by Admiral Liu Huaqing (sometimes called 'China's Mahan'), who made a case for an increasingly strong Navy and laid the theoretical foundation for China's current naval strategy, introducing the concept of 'offshore defence' and making it the cornerstone of the transformation of China's Navy from a permanent coastal defence force to a global projection force. Liu Huaqing outlined the evolutionary stages of this transformation to 2020 as follows: first, China's coastal defence capabilities will be implemented; then, by the end of the 20th century, China will equip itself with a 'green-water Navy', capable of extending its control within the so-called 'first island chain', covering an area of 200 nautical miles from the Chinese coast and including the Kuril Islands, Japan's archipelago, the Ryukyu Islands, Taiwan, the northern Philippines and Borneo;[51] finally, by the year 2020, China's Navy will be able to compete with the world's leading navies and play the role of a full-fledged 'blue-water Navy', capable of controlling the maritime space within the so-called 'second island chain', which farther east extends from Honshu (Japan's largest island, where Tokyo is located) to New Guinea via the Japanese-governed Ogasawara and Volcano Islands, and the U.S. territories of Guam (hosting a major U.S. military base), and the Mariana and Caroline Islands: in this way, China will have direct access to the Pacific on one side and the Strait

[50] O'Rourke 2020: 79.

[51] It is interesting to note that the first island chain can also be considered "a kind of "Great Wall in reverse": a well-organized line of U.S. allies that serves as a sort of guard tower to monitor and possibly block China's access to the Pacific Ocean" Kaplan 2011: 33.

of Malacca[52] and the Bay of Bengal on the other. Liu Huaqing's 'two island chain strategy' thus identifies the Chinese Navy's main areas of action and different lines of defence. The most important of these lines is the one that marks the beginning of the strategic defence zone intended to protect China from incursions or air attacks by enemy forces. Within this 'green water zone', extending to the first island chain, Chinese strategy is aimed at intercepting and neutralising invading forces. That is why Liu's entire strategic concept of offshore defence can be represented as a wide-ranging sea denial operation, involving an implicit recognition of the Chinese Navy's inability to hold its own in a symmetrical confrontation. But let us return to the map of the nine-dash line. On 7 May 2009, in support of its claim of historical rights to the SCS, China submitted to the United Nations Commission on the Limits of the Continental Shelf a document, including this map, which stated that "China has indisputable sovereignty over the islands in the South China Sea and the adjacent waters, and enjoys sovereign rights and jurisdiction over the relevant waters as well as the seabed and subsoil thereof".[53] It goes without saying that China's claims have been considered unfounded, illegal, unreasonable and preposterous by all other states in the region claiming the application of the rules included in the 1982 UNCLOS, which stipulates that each state exercises its sovereignty over territorial waters within 12 miles and has the right to exploit the natural resources found within the 200 nautical miles of the EEZ, and that consequently the other waters of the SCS should be considered international waters. These divergent interpretations have

[52] The Strait of Malacca, which connects the Indian and Pacific oceans and is the shortest sea route between Europe and the Far East, is perhaps China's main Achilles' heel as about 80% of China's energy imports pass through Malacca, and any disruption in the flow of shipping through the strait would seriously jeopardise Beijing's energy security. Precisely to highlight China's vulnerability to this strait and the difficulty of remedying it (maybe by finding alternative routes), former Chinese Communist Party Secretary Hu Jintao coined the expression 'Malacca dilemma' in 2003. One way to solve this dilemma is offered by the so-called 'String of Pearls Strategy'. Such a term refers to a series of ports and support bases for the Chinese navy and civil navy in the Indian Ocean, located in Cambodia, Burma, Bangladesh, Sri Lanka, Pakistan, Djibouti and Sudan. One might think that the 'String of Pearls Strategy' has a strong anti-Indian vocation, but if properly analysed it appears rather as an attempt on the part of the Chinese to secure their supplies from an American blockade in the event of a conflict over Taiwan: either diverting them by land (important in this respect is the Pakistani port of Gwadar, from which a roads and pipelines system is to be built in order to transport imported energy resources from the Middle East directly to the Chinese province of Xinjang) or bypassing the Strait of Malacca (perhaps via the Strait of Lombok).

[53] CLCS 2009.

caused multiple maritime territorial disputes between China and other states bordering the SCS, particularly Vietnam, the Philippines and Malaysia. The subject of the disputes is sovereignty over several island groups such as the Spratlys (which are claimed entirely by China, Taiwan and Vietnam, and in part by the Philippines, Malaysia and Brunei, and which are occupied in part by all these countries except Brunei) and the Paracels (which are claimed by China and Vietnam, and occupied by China) and exclusive control over the surrounding maritime areas. Interestingly, most of the disputed islands were not originally legally classifiable as islands but only as rocks, as they were not permanently inhabited and could not sustain independent economic and social activity. According to UNCLOS, rocks, unlike islands, give no right to control EEZs. The fact that the SCS is characterised by the presence of a myriad of poorly inhabited islands and atolls that make it difficult to draw clear and recognisable boundaries undoubtedly favour the use of coercive gray zone strategies. In addition, until recently, several of the states involved experienced some difficulties in monitoring and surveilling all the islands that make up their territory, making it possible for Chinese military or paramilitary forces to carry out *faits accomplis.* Although there have been maritime and territorial disputes in the SCS in the past, it is mainly since 2010 that China has started to systematically use its own version of the gray zone strategy, referred to as the 'cabbage strategy', indicating the process of wrapping an island in several layers of Chinese control. Generally, the first move is to create a *fait accompli* that determines a form of control, such as the presence of fishermen and the construction of some rudimentary building. This presence is reinforced by the protection of coast guard and then navy ships, making it almost impossible for the other states involved in the dispute to regain control of the island without causing an escalation. The acceleration of this strategy came with the construction of artificial islands. While other states have limited themselves to building small semi-permanent structures for local fishermen, China has promoted a full-fledged process of expanding the SCS small atolls territory by dredging underwater sediments, so as to expand the size of pre-existing islands or even create new ones. Many of what used to appear as semi-submerged atolls now appear as artificial islands capable of supporting forms of economic activity, but also, in some cases, hosting port infrastructures, airstrips and military installations (such as radar and missile batteries). The most prominent examples of the application of the 'cabbage strategy' are Mischief Reef and Fiery Cross in the Spratlys and Tree Islands in the Paracels. Still on the subject of China's gray zone strategy in the

SCS, it is worth recalling the events that took place from April to June 2012, when China gained de facto sovereign control over Scarborough Shoal (which lies well inside the Philippines EEZ, just 140 nautical miles from Manila), first by sending on site two law enforcement vessels to deter the Philippines' presence and then, as part of a gradual escalation, by sending its coast guard and several fishermen and occasionally harassing Philippine vessels. It was a two-month standoff, at the end of which, all attempts at a diplomatic settlement of the crisis having failed, the Philippine vessels left the shoal while China's remained and began denying entry to Filipino fishermen, resulting in a de facto seizure of control by Beijing. Also noteworthy is the Second Thomas Shoal incident, which refers to the facts occurring on March 2014, when Chinese patrol ships repeatedly harassed Philippine vessels likely carrying construction materials to consolidate the Philippine's outpost at Second Thomas Shoal. In particular, on 29 March, a Chinese coast guard cutter crossed the bow of another Philippine supply ship in an effort to block its path. Since then, Chinese ships continued to maintain a presence in the vicinity of the shoal and monitor Philippine vessels entering it. In July 2016, the Permanent Court of Arbitration in The Hague ruled that China's historical claims on the SCS have no legal validity and that changes to the status quo carried out through coercion are illegitimate. Beijing immediately declared that it did not recognise the validity of the Court's ruling, and stated that the islands in question, since they are Chinese territory, cannot be the subject of an interstate dispute requiring a resolution under international law. In the following years, China has continued its construction and militarisation activities in the disputed islands, culminating in the deployment of fighter planes and H6 bomber landing trials in the Paracel Islands in 2019. China's use of gray zone strategy is obviously not limited to the SCS. The dispute over the Senkaku (Chinese: Diaoyu) Islands (a group of uninhabited islets that are claimed by China, Taiwan and Japan, which administers them) is a second major front for China's gray zone strategy. Since the 1990s and 2000s, the dispute has periodically flared up again, creating tense peaks in Sino–Japanese relations and in the triangular relations between Beijing, Tokyo and Washington. A first case occurred in September 2010, when a Chinese fishing trawler collided with Japanese coast guard vessels in water near the Senkaku Islands, triggering a two-week diplomatic crisis due to Tokyo's decision to arrest the skipper and detain his crew, who were, however, released shortly afterwards. Anyway, the most significant crisis occurred in September 2012, when the Japanese central government decided to nationalise some of the Senkaku Islands by purchasing them from their private owner. Although this move was intended to prevent the purchase by Tokyo Governor Shintaro Hishihara, known for his nationalistic views, the decision was seen in Beijing as a serious violation of Chinese territorial sovereignty, to the extent that vehement anti-Japanese protests erupted in major Chinese cities. A year later, in November 2013, Beijing renovated an air defence identification zone (ADIZ) over most of the ESC, in order to identify, monitor, control and react to aircraft entering this zone. On that occasion, both Japan and the U.S. refused to recognise the Chinese ADIZ, conducting overflights of the area to reaffirm both Japanese sovereignty and rejection of the Chinese initiative. Since then, China continued to put pressure on the Japanese military through maritime incursions by civilian or paramilitary vessels, and through violations or attempted violations of Japanese airspace in the area. This has led the Obama Administration to reiterate that the Senkaku Islands are considered part of Japanese territory and therefore subject to the defence clause of the U.S.–Japan alliance. Overall, the gray zone strategy in the case of the Senkaku Islands appears much less effective than in the SCS. In this case, geography provides a focal point on which the defenders can focus their attention so as not to allow Beijing to obtain a *fait accompli.* Moreover, Japan is certainly a more powerful and determined adversary in the defence of its territorial integrity than the other states in the region. Many other cases of gray zone maritime coercion in the SCS and ECS could be cited:[54] similarly to those already examined, they include "collisions of ships and aircraft, military operations in disputed waters and airspace, fishing and law enforcement activities in areas claimed by multiple parties, the use of economic and diplomatic leverage, and land reclamation and construction on disputed features".[55] The analysis of all these cases (differing in timing, subject of dispute, main actors and outcomes) clearly shows that China, having consolidated its position in the SCS, has recalibrated its assertiveness in the area. This did not translate into the complete renunciation of coercive conduct, but rather resulted in the use of such conduct to a lesser extent. China now has less incentive to create critical situations and trigger potential military

[54] One of these is the harassment (on 8 March 2009) of the *Impeccable,* a U.S. Navy unarmed, civilian-operated ocean surveillance ship, which was surrounded by five Chinese vessels aggressively manoeuvring in dangerously close proximity to it, in an apparent attempt to harass his crew. Such an incident "highlighted the potential for diverging views of freedom of navigation to lead to isolated clashes at sea" Bowers 2018: 58.

[55] Green et al. 2017: 2.

escalations, which confirms the thesis that, in the context of the maritime territorial disputes in which it is involved, Beijing is more inclined to resort to military force on those occasions when it perceives itself to be in a condition of relative inferiority. In other words, China does not show a greater inclination to trigger a conflict where it believes it has greater military capabilities; on the contrary, it does so when it perceives its general weakness (not only military) and considers conflict as the only possible solution.[56]

## How to counter China's gray zone strategy at sea?

To some extent the fact that China oriented its conduct towards strategic gradualism can be interpreted as a symptom of the continuing ability of the system of deterrence (mainly based on bilateral alliances) established and consolidated by the U.S. to guarantee extended deterrence to its allies, discouraging openly revisionist attempts. It is not certain, however, that China's systematic (and so far, rather effective) use of gray zone coercion will in the long run fail to erode the credibility of the alliances that bind the U.S. to its Southeast Asian partners, with what serious consequences for the stability of the U.S.-led regional (but also global) order is easy to imagine. Furthermore, it should be remembered that gray zone strategies have significant limitations, starting with the fact that they do not allow for decisive outcomes within a defined period of time. In this respect Mazarr writes: "Gray zone strategies allow states to capitalize on others' vulnerabilities, but they seldom, if ever, offer avenues to achieve decisive results on their own. Beijing cannot be certain of achieving its ultimate goals in the South China Sea through gradual gray zone tactics and techniques alone. If others resist sufficiently, China will ultimately need to decide whether to escalate to more elaborated forms of aggression."[57] On the other hand, the objective difficulty of successfully coping with an accumulation of aggressive Chinese steps (albeit these are part of a subtle and calculated strategy aimed as a whole at producing significant changes to the status quo without provoking a decisive response) could cause, in the long run, decisive reactions by China's opponents, whether or not major thresholds or redlines are crossed.[58] Understanding what lies over

[56] Fravel 2008.

[57] Mazarr 2015: 121.

[58] Mazarr 2015.

the horizon demands thinking rigorously about the lessons to be learned from the past. In perhaps the best work on the subject, the aforementioned *Countering Coercion in Maritime Asia* by Michael Green et al., five lessons are identified that should be drawn from recent incidents of gray zone coercion in the SCS and ECS and which policymakers should take into account if they want to develop a coherent and effective strategy to deter China's coercive actions:

- *Lesson 1: Tailor deterrence strategies.* Leaders should only draw red lines that they are willing to uphold.
- *Lessons 2: Clarify deterrence commitments.* Leaders will have to be clear about the actions they oppose and demonstrate how they may respond in order to credibly deter those actions.
- *Lesson 3: Accept calculated risk.* Risk avoidance encourages coercion by reassuring China that the likelihood of escalation in gray zones is minimal.
- *Lesson 4*: *Tighten alliances and partnerships.* By ensuring that the United States is a constant participant in allied decision making, Washington can dissipate both ally fears of abandonment and U.S. fear of entrapment.
- *Lesson 5: Exercise restraint while demonstrating resolve.* If the United States takes a more robust approach to deterring gray zone coercion, then it should also engage Beijing to demonstrate that Washington still welcomes the rise of a peaceful and prosperous China.[59]

More generally, the ongoing strategic debate on these issues has led to various attempts to outline the main options to effectively counter China's gray zone strategy in the SCS and ECS and its repeated attempts to undermine the rules-based (and Washington-led) regional order. According to Hal Brands and Zack Cooper four basic strategies are available:

1. *Rollback* aims to push China back from its recent gains in the South China Sea and restore the status quo ante; it accepts a substantial likelihood of military conflict as the price of attaining this ambitious objective.
2. *Containment* accepts Chinese gains made to date, in recognition of just how difficult and dangerous would be to reverse those gains, but draws the line firmly – including by threat or use of military force – against further advances.

[59] Green et al. 2015: v–vi.

3. *Offset* does not seek to prevent further Chinese encroachments in the South China Sea, but aims to penalise Beijing for destabilising actions, while also offsetting their impact through measures that strengthen the overall U.S. position in the region.
4. *Accommodation* accepts Chinese dominance of the South China Sea, on the theory that it is simply too costly and perilous to compete with Beijing in its own back yard, and instead seeks to ensure a smooth transition to Chinese regional primacy.[60]

Once the point is made that none of these strategies is perfect as each has its merits and flaws, one can certainly agree with the authors when they identify a shrewd and well-calculated combination of the most compelling aspects of containment and offset as the strategy best suited to protect the U.S. and its allies' geostrategic interests at a reasonable cost.

## Conclusion

As seen, analysis of the nature and scope of the most threatening gray zone challenges in the maritime domain suggests that it is primarily in the Indo-Pacific region that the game on which the definition of international order will depend in the decades to come will be played. In fact, the need for a rising China to display, if only through forms of gray zone coercion, its growing power in the SCS and ECS (as well as, in perspective, globally), places the United States and its allies in a serious dilemma: to pander, at least in part, to China's claims, with the hope (one does not know how well-founded) that China would be willing to share near-seas with others on the basis of mutually agreed rules, or to reject them simultaneously implementing a strategy to contain China's growing power, possibly avoiding falling into Thucydides' famous trap? How the situation will evolve is unknown. What is clear is that, as Kishore Mahbubani puts it, "the real reason why most international waterways remain safe and open, and thereby facilitate the huge explosion of global trade we have seen, is that American Navy acts as the guarantor of last resort to keep them open. Without the global presence of U.S. Navy, our world would be less orderly".[61]

[60] Brands–Cooper 2018: 14.

[61] Mahbubani 2009: 105.

## Questions

1. What are the defining characteristics of gray zone coercion?
2. Who and why does resort to gray zone coercive actions in the maritime domain?
3. What do the salami slicing and cabbage peeling tactics consist of?
4. In what ways has China used gray zone coercion to support its claims in the SCS?
5. How to articulate a coherent strategy for effectively countering China's gray zone coercive actions in the SCS and ECS?

## References

Altman, Dan (2017): By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries. *International Studies Quarterly,* 61(4), 881–891. Online: https://doi.org/10.1093/isq/sqx049

Altman, Jonathan (2016): Russian A2/AD in the Eastern Mediterranean. A Growing Risk. *Naval War College Review,* 69(1), 72–84.

Bowers, Ian (2018): Escalation at Sea. Stability and Instability in Maritime East Asia. *Naval War College Review,* 71(4), 46–65.

Brands, Hal (2016): *Paradoxes of the Gray Zone.* Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737593

Brands, Hal – Cooper, Zack (2018): Getting Serious About Strategy in the South China Sea. *Naval War College Review,* 71(1), 1–21.

Cable, James (1999): *Gunboat Diplomacy 1919–1979. Political Applications of Limited Naval Force.* Basingstoke: Palgrave Macmillan.

Caffio, Fabio (2018): Caso Saipem 12000: chi protegge gli interessi italiani nel Mediterraneo orientale? *Analisi Difesa,* 11 February 2018. Online: https://www.analisidifesa.it/2018/02/caso-saipem-12000-chi-protegge-gli-interessi-italiani-nel-mediterraneo-orientale/

CLCS (2009): *Communication from China to the United Nations dated 7 May 2009.* Online: http://www.un.org/Depts/los/clcs_new/submissions_files/submission_vnm_37_2009.htm

Cronin, Patrick M. – Ratner, Ely – Colby, Elbridge – Hosford, Zachary M. – Sullivan, Alexander (2014): *Tailored Coercion. Competition and Risk in Maritime Asia.* Washington, D.C.: Center for a New American Security.

Del Valle Gálvez, Alejandro (2013): The Gibraltar Crisis and the Measures, Options and Strategies Open to Spain. *ARI,* 32. Online: https://www.files.ethz.ch/isn/170749/ARI32-DelValle_Gibraltar_crisis_measures_options_strategies_Spain.pdf

Dutton, Peter A. (2014): China's Maritime Disputes in the East and South China Seas. *Naval War College Review,* 67(3), 7–18.

Eisenstadt, Michael (2021): Iran's Gray Zone Strategy, Cornerstone of Its Asymmetric Way of War. *Prism,* 9(2), 77–97.

Elkus, Adam (2015): 50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense. *War on the Rocks,* 15 December 2015. Online: https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/

Fanell, James E. (2019): China's Global Naval Strategy and Expanding Force Structure. Pathway to Hegemony. *Naval War College Review,* 72(1), 10–55.

Fravel, M. Taylor (2008): Power Shifts and Escalation. Explaining China's Use of Force on Territorial Disputes. *International Security,* 32(3), 44–83. Online: https://doi.org/10.1162/isec.2008.32.3.44

Freier, Nathan P. (2016): *Outplayed: Regaining Strategic Initiative in the Gray Zone.* Carlisle: The United States Army War College Press.

Galang, Mico A. (2021): Countering Maritime Gray Zone Challanges in Southeast Asia: Examining the Strategic Context. *National Defense College of the Philippines Executive Policy Brief,* 8. Online: https://www.researchgate.net/publication/356915819_Countering_Maritime_Gray_Zone_Challenges_in_Southeast_Asia_Examining_the_Strategic_Context

George, Alexander L. – Smoke, Richard (1974): *Deterrence in American Foreign Policy.* New York: Columbia University Press.

Goldrick, James J. (2018): Special Report. Grey Zone Operations and the Maritime Domain. *Australian Strategic Policy Institute,* October 2018. Online: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ASPI_SR%20131%20Grey%20zone%20operations.pdf

Green, Michael – Schaus, John – Douglas, Jake – Cooper, Zack – Hicks, Kathleen H. (2017): *Countering Coercion in Maritime Asia. The Theory and Practice of Gray Zone Deterrence.* Lanham: Rowman & Littlefield.

Gresh, Geoffrey F. (2020): *To Rule Eurasia's Waves. The New Great Power Competition at Sea.* New Haven: Yale University Press. Online: https://doi.org/10.2307/j.ctv177tk87

Haddick, Robert (2014): America Has No Answer to China's Salami-Slicing. *War on the Rocks,* 6 February 2014. Online: https://warontherocks.com/2014/02/america-has-no-answer-to-chinas-salami-slicing/#

Hicks, Kathleen H. – Metrick, Andrew – Sawyer Samp, Lisa – Weinberger, Kathleen (2016): *Undersea Warfare in Northern Europe.* Washington, D.C.: Center for Strategic International Studies – Lanham: Rowman & Littlefield.

Kahn, Herman (2010): *On Escalation. Metaphors and Scenarios.* New Brunswick: Transaction Publishers.

Kaplan, Robert D. (2011): The South China Sea Is the Future of Conflict. *Foreign Policy,* 15 August 2011. Online: https://foreignpolicy.com/2011/08/15/the-south-china-sea-is-the-future-of-conflict/

Kapusta, Philip (2015): The Gray Zone. *Special Warfare,* 28(4), 19–25.

Klein, Natalie (2011): *Maritime Security and the Law of the Sea.* Oxford: Oxford University Press.

Kraska, James (2018): The Kerch Strait Incident: Law of the Sea or Law of Naval Warfare? *EJIL: Talk!,* 3 December 2018. Online: https://www.ejiltalk.org/the-kerch-strait-incident-law-of-the-sea-or-law-of-naval-warfarw/

Kuo, Raymond (2020): *Contests of Initiative. Countering China's Gray Zone Strategy in the East and South China Seas.* Washington, D.C.: Westphalia Press.

Lamb, Nelson A. (2020): *Identifying Conditions Present in Gray Zone Conflicts: A Structured Focused Analysis of Gray Zone Conflict.* Fort Leavenworth: School of Advanced Military Studies.

Lanoszka, Alexander (2016): Russian Hybrid Warfare and Extended Deterrence in Eastern Europe. *International Affairs,* 92(1), 175–195. Online: https://doi.org/10.1111/1468-2346.12509

Le Mière, Christian (2014): *Maritime Diplomacy in the 21st Century. Drivers and Challenges.* Abingdon – New York: Routledge.

Lovelace, Douglas C. (2016): *Hybrid Warfare and the Gray Zone Threat.* Oxford: Oxford University Press.

Mahbubani, Kishore (2009): *The New Asian Hemisphere. The Irresistible Shift of Global Power to the East.* New York: PublicAffairs.

Martinson, Ryan D. (2015): China's Second Navy. *U.S. Naval Institute Proceedings Magazine,* April 2015. Online: https://www.usni.org/magazines/proceedings/2015/april/chinas-second-navy

Mazarr, Michael J. (2015): *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle: The United States Army War College Press.

Nadimi, Farzin (2020): *Iran's Evolving Approach to Asymmetric Naval Warfare: Strategy and Capabilities in the Persian Gulf.* Online: https://www.washingtoninstitute.org/policy-analysis/irans-evolving-approach-asymmetric-naval-warfare-strategy-and-capabilities-persian

O'Rourke, Ronald (2020): *U.S.–China Strategic Competition in South and East China Seas. Background and Issues for Congress.* Washington, D.C.: Congressional Research Service.

Patalano, Alessio (2018): When Strategy Is Hybrid and Not Grey: Reviewing Chinese Military and Constabulary Coercion at Sea. *The Pacific Review,* 31(6), 811–839. Online: https://doi.org/10.1080/09512748.2018.1513546

Ratner, Steven R. (1984): The Gulf of Sidra Incident of 1981: A Study of the Lawfulness of Peacetime Aerial Engagements. *Yale Journal of International Law,* 7(59), 59–77.

Schadlow, Nadia (2014): Peace and War: The Space Between. *War on the Rocks,* 18 August 2014. Online: http://warontherocks.com/2014/08/peace-and-war-the-space-between/

Schelling, Thomas (2008): *Arms and Influence.* New Haven: Yale University Press.

Singh, Abhijit (2018): Deciphering Grey-Zone Operations in Maritime Asia. *ORF Special Report,* August 2018. Online: https://www.orfonline.org/wp-content/uploads/2018/08/ORF_SpecialReport_71_Grey-Zone_3N.pdf

Steinsson, Sverrir (2016): The Cod Wars: A Re-analysis. *European Security,* 25(2), 256–275. Online: https://doi.org/10.1080/09662839.2016.1160376

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), 2–37.

Tobin, Liza (2018): Underway. Beijing's Strategy to Build China into a Maritime Great Power. *Naval War College Review,* 71(2), 17–48.

Truver, Scott (2020): 'Iran's Gray Zone Navy'. *U.S. Naval Institute Proceedings Magazine,* February 2020. Online: https://www.usni.org/magazines/proceedings/2020/february/irans-gray-zone-navy

U.S. Department of Defense (2017): *Freedom of Navigation (FON) Program.* Online: https://policy.defense.gov/Portals/11/DoD%20FON%20Program%20Summary%2016.pdf?ver=2017-03-03-141350-380

Werner, Ben (2018): Panel: Navy and Coast Guard Operating More in a Maritime 'Grey Zone'. *USNI News,* 9 February 2018. Online: https://news.usni.org/2018/02/09/panel-navy-coast-guard-operating-maritime-grey-zone

Yoon, Sukjoon (2015): Implications of Xi Jinping's "True Maritime Power": Its Context, Significance, and Impact on the Region. *Naval War College Review,* 68(3), 40–63.

Andrea Beccaro[1]

# Influence of Emerging Technologies

This chapter aims to better clarify the impact of modern technology on warfare and in particular on the concept of hybrid warfare. To do this, the chapter is divided into three sections in addition to the conclusions. The first part seeks to clarify the impact of modern technology on warfare by briefly examining the terminology used. The second analyses in more detail the relationship between Emerging Disruptive Technologies and the concept of hybrid warfare. The third part is a focus on the current use of drones on modern battlefields. In this way, the paper intends also to clarify a central theme for understanding war, that is, the relationship between it and technology. In the current context, there is no doubt that the cyber environment and the development of AI (Artificial Intelligence) are expanding the range of possible actions in the context of hybrid threats. The development of information technologies from the 1980s has had a huge impact on the development of new operational possibilities. However, we must never forget that war is a political and social phenomenon, and it has a human dimension that cannot be eliminated. From this point of view, technology is exclusively a tool, more or less advanced and more or less effective depending on the contexts and strategies, of a wider and more complex phenomenon.

## Technology and war in the 21st century

*Multidimensionality.* All wars in history have had multiple dimensions and strategic thought itself has always had at least two dimensions (land and sea). Today, however, modern technology has expanded this aspect transforming the concept of multidimensionality into a central term for understanding the conflicts of the 21st century. The concept can be read from two distinct perspectives. On the one hand, the term indicates that modern operations require multidimensional strategies that must include military, political, economic, information and IT tools. On the other hand, multidimensionality refers to the fact that the

[1] University of Turin.

DOI: https://doi.org/10.36250/01237_09

dimensions of strategy have progressively expanded over the last two centuries. Historically, wars have always taken place on the ground and, therefore, land warfare has always been dominant. With the invention of the internal combustion engine, the submarine and the aircraft, new horizons opened up linked to the vertical dimension of the conflict up to the exploration of space and the use of satellites for the collection of information and for communications. Finally, the information revolution has created a "non-space" that has added a further dimension to strategic thought, namely cyberspace. This represents the real revolution in military operations, since the purely military means still used today are often instruments designed and produced decades ago. It is the skills of communication, acquisition of objectives, surveillance and reconnaissance that today have profoundly transformed both those tools and the battlefield. These new technologies have also had a significant impact on training. On the one hand, technological development and the availability of modern individual weapons on the black market has significantly reduced the difference in firepower between a regular soldier of any Western army and that of an irregular fighter. On the other hand, the latter cannot enjoy the advantages of high-level training that derives from the ability to create realistic scenarios within which to test new tactics, weapons or more simply to teach recruits.[2] The cyber aspects are just one of the many facets and various fields of development linked to new technologies that also offer low-cost solutions to small or medium powers as well as to so-called irregular fighters. This creates a strategic situation in which the distinction between regular and irregular is much more blurred and where conflict is fought, even with non-lethal tools, on several different levels.

*Ambiguity.* Ambiguity indicates duplicity, an ambiguous way of behaving and undoubtedly this is a hallmark of hybrid threats. However, it is certainly not necessary to introduce the term hybrid warfare to understand this aspect because strategy has always been based precisely on the idea of duplicity, of being interpreted in different ways. Luttwak[3] defined this aspect as the paradoxical logic of strategy, namely the fact that in war what appears most logical and simple is probably the worst choice to make precisely because it is the simplest and most obvious option, it is what the enemy is prepared to face. Already Sun Tzu indicated in deception and duplicity one of the distinctive features of military

[2] Boot 2006.

[3] Luttwak 2001.

strategy. For example, in chapter five of *The Art of War*[4] he states that one must give the enemy (the illusion of) a small advantage, so that he will expose himself in the ways we want and then surprise him in a more advantageous context for us. Feints and operations to distract the enemy are central elements to take by surprise in a different sector the enemy who at that point will have positioned his forces and his attention elsewhere. In the 20th century, Liddell Hart[5] with his indirect approach has supported similar ideas precisely with the aim of creating the element of surprise that is the basis of the strategy. Carl von Clausewitz[6] does not directly address the problem but using the terms "fog of war" *(Nebel des Krieges)* and "friction" *(Friktion)* the Prussian underlines how ambiguity pervades all conflicts for the most varied reasons: lack of information, incorrect information, technical problems, human errors, problems relating to the weather or the type of terrain, without forgetting that the actions of the enemy, which we cannot know in advance, constantly modify the environment in which we operate. Therefore, the concept of ambiguity is an element of warfare and strategy that should not surprise. The concept of Gray Zone Warfare[7] is now used to indicate actions of international actors that cannot be identified either as open warfare or as simple peaceful diplomacy actions, they are thus classic ambiguous actions that have the advantage of being easily deniable, but at the same time aim to modify, albeit marginally, to the advantage of those who apply them, the strategic context. But all this constitutes not only the very nature of strategy but also of international politics and diplomacy. Machiavelli spoke clearly of the need to be a fox in politics, emphasising the need to slyly exploit situations and conceal behaviours in order to achieve one's goals. During the Cold War itself, the United States made extensive use of propaganda and hidden or disguised aid such as scholarships, economic aid, etc. to weaken the enemy.[8] What has perhaps changed today is the extent of the ambiguity that derives from the pervasiveness of the media and the Internet. In relation to hybrid threats, one of the major problems is making the political decision-maker understand that certain situations (such as migration or propaganda) can be elements of a broader political conflict strategy.

[4] Tzu 1990.

[5] Liddell Hart 1991.

[6] Clausewitz 1984.

[7] Mazarr 2015.

[8] Robinson et al. 2018.

*Contested Environment.* This term encompasses all attempts by an opponent to disturb the United States and its partners in the entire battle space. For example, an opponent could use long-range ballistic and cruise missiles, cyberattacks, and electronic warfare to attack vital elements of the U.S. military structure, including air bases and communications systems.[9] From the end of the Cold War until the beginning of the 21st century, the United States and NATO were used to operating in environments where enemy forces were only partially able to militarily contend the battle space and, consequently, they developed operational capabilities that exploited that particular strategic situation. *Desert Storm* in Iraq in 1991, *Deliberate Force* and *Allied Force* in the Balkans in the 1990s, *Enduring Freedom* in Afghanistan in 2001, *Iraqi Freedom* in Iraq in 2003 were operations in which, albeit with some limitations, the western air forces were able to operate undisturbed. There were minimal casualties, but in general the skies were dominated by western aircraft. Today, this is no longer the case. To better understand this situation, it is necessary to refer to the concept of A2/AD which creates a sort of security bubble in which American aircraft cannot enter (or rather they can but with a high risk) and here a central role is played mainly by missiles of various kinds. The first modern theatre in which the United States has found itself operating in such an environment, with the exception of the Pacific with China which has been implementing this approach for years, is certainly Syria. The aforementioned operations highlight the fact that the contested environment idea is closely related to air operations, which are fundamental for modern military actions, but which are only one of the elements. If we use a land warfare perspective, however, we see how the concept of contested environment is a-historical since land operations have always been contested by an enemy, more or less strong or more or less prepared. Furthermore, modern technologies create a further context space, that of cyber and communication in general. Threats to communications in a contested environment put at risk the entire centralised command and control system that has prevailed in recent decades.[10] Indeed, as the American scholar Stephen Biddle[11] pointed out in a recent volume, in today's battlefields one of the essential requirements for the actors, whether regular or irregular, is to be able to avoid the enemy's firepower for long enough to carry out their political plans. A first way to do so

[9] Priebe et al. 2019.

[10] Priebe et al. 2019.

[11] Biddle 2021.

is that of stealth, that is to hide from the eyes of the enemy in order not to offer a target, and it is certainly the typical approach of irregular warfare. Nonetheless, starting at least from 1914, even the regular forces have increasingly tried to make themselves invisible, since, given the firepower of modern artillery and the increased accuracy of modern weapons, being identified means being hit. Cover and concealment have thus become central elements for modern regular forces. A second way to avoid the enemy's firepower is that of dispersion which also leads to a confusion between the front line and the rear that is typical of the current strategic context. Typically, the irregular fighters disperse over the territory and mix with the civilian population to "disappear" in the eyes of the security forces. However, even the regular armies have abandoned, starting from 1916–1917, the old concepts of formation in line and in mass, introducing, instead, more flexible deployments composed of small units. This has resulted in the progressive dispersion of forces on the battlefield and, therefore, the density of troops on modern battlefields has drastically changed. This trend, on the other hand, did not affect the irregular fighters who historically have always been very dispersed over the battlespace. Consequently, this trend has made the two ways of fighting, the regular and the irregular one, more similar. Since today the density between the two actors on the battlefield is similar and both have a similar firepower, the clear advantage that the regular armies historically had against these actors has progressively been eroded. The technological advantage, which remains on the side of the state actor, is not able to compensate for this levelling of the number of soldiers on the battlefield. As Biddle notes in every war situation in history, be it regular or irregular, the fundamental dynamics of combat is linked to the desire to defend against enemy fire and at the same time to the need to expose oneself in order to use one's firepower. So, lethality and survival are two dynamics always in play and in search of a balance. Greater dispersion in the field also implies greater independence and this implies the need for a more agile and flexible chain of command, in the style of the German *Auftragstaktik*.[12] The exponential increase in the firepower of modern weapons and their accuracy, even the simplest and most common ones readily available on the market for non-state actors, allows a limited number of fighters to be highly deadly and effective.

*Information Environment.* The term information environment (IE) is new but the concept it describes is not because it defines how information can be

[12] In modern military terminology it can be translated as *Mission Command.*

used to influence the direction and outcome of competition and conflict, or the use of information within the framework of a defined strategy. Any strategic author from Sun Tzu onwards emphasises the important and decisive role of having a superior understanding of one's opponents and the centrality of using that understanding wisely to gain an advantage over them. In short, information is the means by which all the warring parties build mutual understanding of each other and of themselves. Since today we live in a globalised world, the IE of the 21st century is a highly complex "system of systems" on a global level in which information moves and produces consequences with increasing and often high-level and unexpected speed. Such flows are uncontrollable and offer all actors, both state and non-state, important opportunities to develop their influence. In general, IE consists of three dimensions: physical, the environment in which the interaction between geography, infrastructures, individuals, states, cultures, society takes place and where the physical effects occur; virtual, the environment that contains intangible entities; cognitive,[13] afferent to the sphere of perceptions and decisions, constitutes the environment in which the social and psychological effects that influence the behaviour of an individual can be achieved. It is therefore an externally complex and large system impossible to control in its entirety.

*Information Manoeuvring* (IM). This notion is closely related to the previous one. The concept of manoeuvring is clearly not new since every general in history has manoeuvred, more or less effectively, his army on the battlefield in order to win the clash with the enemy. Certainly, more recent, and from various points of view more nebulous, is the concept of IM and to clarify it we could say that it involves the use of information in all its forms to understand the operating environment better than anyone else and, subsequently, to make the most of this advantage. The goal of IM is to model perceptions to ensure that the activities and intentions of the army are adequately recognised by allies, populations and adversaries. IM requires a large degree of integration and is intrinsically linked with capabilities in the cyber, space, maritime and air domains. It, therefore, brings together the forces that work in the cyber field, electronic warfare, surveillance, reconnaissance, counterespionage and influence activities (psychological warfare) to achieve the desired effect. It is a concept that fits well into the notion of Gray Zone Warfare and useful for countering some hybrid threats.

[13] Jervis 1976.

## Emerging and Disruptive Technologies (EDT) and NATO

NATO defines emerging and disruptive technologies (EDT) technologies such as artificial intelligence (AI), autonomous systems, advanced manufacturing, biotechnologies and quantum technologies. Emerging and Disruptive Technologies (EDT) is a notion that highlights the role of modern (and future) technology in the conflicts of the 21st century. There is no doubt that today we are facing a time of profound and rapid changes in technological terms, but great caution is needed in assessing their impact on the international context in general and on future conflicts in particular. First, if we look at the history of war only very few technologies have radically reshaped the dynamics of international conflicts. In fact, most technological innovations have led to incremental advances over a medium to a long period of time. Furthermore, some of those advances have completely disappeared despite having prompted great promise. For example, the introduction of chemical weapons was widely interpreted as a radical change in the way of waging war. Yet, that type of weapons, although repeatedly used even in more recent times, proved to be impractical, easier than expected to counter and less effective than other conventional explosives in inflicting damage and countering enemy operations. Other technologies, on the other hand, became crucial in warfare only after major advances in other areas allowed them to reach their full potential. This is the case, for example, of drones, since unmanned aircraft were already present in the middle of the twentieth century, but it is only with modern information technologies that they could become an essential military tool. This means that even when war technologies have a real and significant impact on the conduct of warfare, it can take decades to be effective in military terms because that technology not only needs to be refined, but also needs to be placed in a suitable strategic and doctrinal context. Secondly, even if today's emerging technologies were ready to introduce major changes in the international system, it would be very likely that they could have contradictory effects, since technologies can be both destabilising (opening unprecedented scenarios for new or old actors, the best recent example is Turkey that using its drones has been able to increase its military and diplomatic leverage in the MENA region) and stabilising (creating equality between previously opposed actors). Nor should it be forgotten that it is probable that other factors may intervene to mediate the effects of new technologies on the international system: geography, the distribution of power, military strategy, domestic and organisational policies and social and cultural variables. As Sechser, Narang and Talmadge note,[14] it is difficult to predict the impact of new technologies because the directions they can take are very different and even contradictory. While some modern technologies are easy to access even for non-state actors with limited resources, as far as EDTs are concerned, they are technologies that require large investments, a good industrial base and time, consequently they remain available to a few actors, namely the United States, China and to some extent Russia. A fundamental problem for understanding EDTs is the fact that they are inherently Dual Use, so the progress made in this area can be (also) destined for civil use and in the same way investments in the civil sector can open up new possibilities in the military field. However, this does not mean inertia since it is now possible to study and examine the EDT sectors on which we must concentrate to understand how these technologies can influence conflicts and international politics. This is what NATO has tried to do in the last years. In London, in December 2019, NATO leaders agreed on a roadmap for the implementation of EDT-related measures. The final document highlights the breadth and scope of new technologies to maintain the technological advantage that NATO has always had over its enemies. Then the document encourages to continue and to increase the resilience of critical infrastructures and energy security (the reference is clearly to Russia). Particular emphasis was given to the security of communications with reference to 5G and the need to exclude possible adversaries (the reference is clearly to China), recognising the need to rely on secure and resilient systems, i.e. on ones managed by allies. Another important aspect is space, an operational domain for NATO, which therefore aims to defend it. At the same time, the pervasiveness of cyberattacks and therefore the need to strengthen the capacity to discourage and defend against this kind of threats is underlined.[15] In February 2021, NATO defence ministers approved an EDT strategy to develop a specific Alliance policy response. In the following March, the NATO Advisory Group on Emerging and Disruptive Technologies published its first annual report[16] which identifies the areas that the Alliance must consider in the context of the new technological landscape. The final document underlines how EDTs are developing at a particularly fast pace and this forces NATO to do the same if it does not want to be overtaken

[14] Sechser et al. 2019.

[15] NATO 2019.

[16] NATO 2020a.

by potential adversaries. To this end, the experts highlighted the need for greater and more integrated cooperation between the Alliance, its members and both the private and public research sectors (universities in particular). Moreover, the working group identified five scientific areas of particular interest:

- First, the key technology sectors: artificial intelligence; quantum computing as well as quantum cryptographic systems and the development of quantum-scale material; data security and therefore algorithms and systems to protect communications and transactions; developments in miniaturisation, energy harvesting and energy storage; the design, synthesis and manipulation of materials at the atomic–molecular level or bioengineering and chemical engineering.
- Second, the socio-technical context, where information systems directly influence change in the physical world and evolve autonomously through detection and data. Here, advances in autonomy, the ubiquity of high-speed communications and other similar advances will rapidly stimulate human–machine interaction.
- Third, the struggle for resources such as water, food, energy and raw materials will continue to grow and intensify. The struggle for data as a resource will be added and this will create new, or reinforce existing, asymmetries on a global level.
- Fourth, space will be the key theatre of the future within which NATO must guide the development of a technologically advanced, complex and articulated environment. The organisation will have to develop internal skills in innovative technologies and innovation and actively participate in the development of new discoveries in order to optimally exploit the brightest minds in industry, government and academia.

What therefore emerges from the document and from the recommendations of the experts is the need for NATO to become an organisation capable of adapting and adopting new technologies at an adequate pace to the technological landscape linked to EDTs. This transformation can only happen if technological literacy is expanded throughout the organisation, an efficient network of Innovation Centres is established, drawing on NATO's existing innovation capabilities, funded projects in this direction and established partnerships with industry and academia. However, in line with some of the recommendations of the NATO Advisory Group on Emerging and Disruptive Technologies at the

Brussels summit of 2021, the NATO 2030[17] agenda was approved with which NATO wanted to launch a new initiative regarding civil–military defence, the Defense Innovation Accelerator for the North Atlantic (DIANA) with the aim of strengthening transatlantic cooperation on critical technologies, promoting greater interoperability and exploiting civil innovation through collaboration with academia and the private sector. In Brussels in 2021, it was also decided to create a fund to finance activities in the EDT sector and in NATO innovation. The fund will invest in start-ups working on EDT and dual technologies in areas critical to the security of the Allies. In particular, the Alliance has identified seven key areas: artificial intelligence (AI), data and information technology, autonomy, quantum technologies, biotechnologies, hypersonic technologies and space.[18] It should not be forgotten that these research sectors must be inserted in a broader technological context of which the four main characteristics that will profoundly influence the future developments of military technology must be pointed out: the characteristic of being intelligent or integrated with AI to create "intelligent" applications technology; be interconnected by exploiting the network and networks of sensors, organisations, individuals and autonomous agents, connected through new encryption methods; be distributed thanks to the possibility of decentralised and ubiquitous storage and computing; and be digital by digitally mixing the human, physical and informational domains. Even more recently, NATO[19] published its strategy regarding AI. The theme is absolutely central both because AI is the technological aspect that can implement all the others and because together with cyber it has the potential to open scenarios that are currently difficult to evaluate. The final document, among other things, highlights some core tasks and sectors related to AI, including: accelerating and integrating the adoption of AI into existing capabilities, improving interoperability; protect and monitor our technologies; identify and safeguard against threats arising from the use of AI by state and non-state actors. Professor Ralph Thiele, expert on hybrid threats with leading publications on the subject and researcher at Hybrid CoE in Helsinki, highlighted some salient points regarding this aspect and specifically highlighted three technologies that will be central:

[17] NATO 2021a.

[18] NATO 2020b.

[19] NATO 2021b.

- First, AI plays a leading role as an engine and multiplier for other technologies and development sectors. Its particular potential lies in the analysis of large amounts of data, in the optimisation of processes, support for decision-making processes and the development of an inter-divisional organisation for understanding situations. However, since AI is currently still a vulnerable technology, it must be handled with caution.
- Second, autonomous systems such as artificial intelligence, machine learning and big data rely primarily on software. The most significant development in this field is undoubtedly that of drones. With the development of technology and greater integration capacity in the not-too-distant future entire swarms of intelligent systems will work together: drones, jets, ships and other interconnected systems. The concepts of human–machine teamwork shape this process. Unmanned Autonomous Systems act, individually or in swarms, as part of a team in close collaboration with human decision makers. While machines take on boring and dangerous operational tasks, humans focus on cognitive aspects and leadership functions, because autonomous systems lack the flexibility of human intelligence.
- Third, quantum science promises to be the driving force of the next revolution. New IT architectures allow the processing and analysis of big data, leading to better search algorithms and faster calculations. A significant consequence in this field is the fact that quantum computers would be able to penetrate the cryptography that states, banks and other actors use to protect their secrets. An important military application for a functional quantum computer is the ability to hack encrypted military servers and servers of an opponent's national infrastructure systems almost instantly.[20]

## Drones in contemporary battlefields

One of the most clear and excellent examples of how modern technology is used on the battlefield is related to the use of drones. We have already discussed in one of the previous chapters of this book *(Different Regional Theatres),* how hybrid groups, such as ISIS, have used such weapon during the fight improving both their military and intelligence gathering capabilities. The brief section is to take into account different case studies that highlight the role of both state

[20] Thiele 2021.

and non-state actors in using this modern technology. It is important to note that although we are used to see drones supporting military operations during land actions, they are used in all military domains, land, sea and air and by both state and non-state actors. An example of this has been the attack on 29 July 2021, when three armed "suicide drones" attacked the *Mercer Street,* an Israeli-managed commercial oil tanker. Two drones missed the tanker during an attempted first strike, but one successfully flew into the *Mercer Street*'s bridge during a second strike.[21] The attack killed a British security guard and the vessel's Romanian captain. Despite the fact that no one claimed responsibility for the attack, experts and analyst said that the available evidence points to Iran. Therefore, this operation was just one of the last actions of a U.S.–Iran "shadow war" that has been simmering across the Middle East for the past years. While it is uncertain who deployed the drones (Iranian regional proxies? Or elements of the Iranian armed forces?), it is well known that Iran has become what we can call a "drone superpower". From strikes on the government-owned Saudi Aramco facilities in eastern Saudi Arabia in September 2019 to attacks on U.S. troops in northern Iraq in July 2021, a string of drone strikes ties back to Iran. Moreover, Iran started to use drones in 1984 when Iran's Islamic Revolutionary Guard Corps (IRGC) formed its first unmanned aerial vehicle (UAV) unit. More recently, Israel's defence minister, Benny Gantz, accused Iran of providing foreign militias from Yemen, Iraq, Syria and Lebanon with drone training at an airbase near the city of Isfahan.[22] However, Iran is not the only actor in the Middle East to use drones and the increasing presence of this war tool in the region is one of the most important and relevant elements of contemporary security and a very concerning tactical development. Research[23] has recorded 440 drone attacks conducted by militants through 2020. Over 98% of them have occurred in the Middle East mainly from two groups, the Islamic State and Houthi rebels in Yemen, responsible for over 80% of these. Another research has found that militant groups use drones especially for disrupting opponent command and logistics and delaying the movement of military personnel and materiel. They do not use drones for what we may call "strategic bombing", i.e. for targeting military centres of gravity,[24] even though defining what is a "centre

[21] The Times of Israel 2021.

[22] Middle East Eye 2021.

[23] Haugstvedt–Jacobsen 2020.

[24] Doctor–Walsh 2021.

of gravity" is a controversial and thorny issue. Summarising the different use of drones by militias in the Middle East, it is possible to list at least three main uses. First, drones, commercial or military ones, are used to support ground operations and the best-known example is ISIS during the battles to defend cities in Iraq and Syria. Second, drones, commercial or military ones, are used to attack logistic hubs, arms depots, critical infrastructure and command headquarters behind front lines. This kind of attack is probably the most common one. The attack against the *Mercer Street* is of this type, but the attacks that Shia militias carried out in Iraq against U.S. troops and bases can also be listed in this category. Although a database of these attacks does not exist, it is possible to say that U.S. troops, bases and facilities (including the U.S. embassy in Baghdad) have been targeted around 60 times between the summer of 2020 and the summer of 2021. It is true that none of these attacks have resulted in fatalities or critical damage, but they did prompt the Biden Administration to order retaliatory airstrikes against the militant groups behind them. Probably the most serious attacks were conducted against airports both in Baghdad and in Erbil, which was targeted at least two times: on 25 July 2021, a drone attack targeted a base near al-Harir, northeast of Erbil; and on 11 September 2021, Erbil International Airport has been targeted by two armed drones. Moreover, at the end of August 2021, eight people were injured in a drone attack on Saudi Arabia's Abha airport. The drone was intercepted and shrapnel hit the runway. It was the second attack on the airport in 24 hours, when a ballistic missile struck the airfield.[25] Two elements of the use of drones in Iraq are relevant and concerning. First, the Iraqi PMF (Popular Mobilization Forces), mostly Shia militias, are supported by Iran and it is known that they used military Chinese drones CH-4B, but also the Iranian drone Mohajer-6s. During a military parade in late June a Mohajer-6 was seen armed with two small munitions similar to the Ghaem series.[26] Second, during the recent Israel–Gaza conflict, it has been claimed that some of the drones flying over Israel had been sent from Iraq or Syria. Iraqi pro-Iran militias, many of them present in Syria as well, continuously threaten that they can attack Israel from Iraq. There was information in February 2021 that drones were launched from the Iraq – Saudi Arabia border toward a royal palace in Riyadh. This fact shows that pro-Iran armed groups in Iraq have chosen this new vehicle, which ensures greater camouflage and target accuracy and greater

[25] Al-Monitor 2021.

[26] Mitzer–Oliemans 2021.

protection for their operations.[27] Moreover, from April 2018 to October 2019, the Houthis executed 115 drone attacks, of these, 62 were conducted against civilian airports or critical infrastructure.[28] The third use of drones is less known because it rarely grabs the headlines but it is very important for the militias in order to improve their military capacities. Several militant groups have used unarmed drones for intelligence, surveillance and reconnaissance operations. Drone-based intelligence, surveillance and reconnaissance offers significant value to militants for relatively little cost or risk. ISIS is again a good example. It used these kinds of drones to re-direct in real time suicide vehicles (SVBIEDs) during the battle of Mosul in order to bypass Iraqi defences and find new ways to approach the designed targets. More recently, it has been reported that the Islamic State's affiliate in West Africa has used drones to place under surveillance the locations and movement of counterinsurgent forces in northeast Nigeria.[29] Since this constant, extensive and widespread use of drones, what is surprising is that such militias have never used the drones to carry out terrorist attacks, even though drones seem particularly well-suited to such a task. The flying drones are not the only threat that comes from unmanned vehicles in the Middle East. In fact, since 2017, Houthi forces in Yemen have been perfecting their use of maritime drones to carry out attacks against maritime vessels and port facilities in the region. As the flying drones, also these attacks have not yet resulted in several fatalities or critical damage but have caused material damage to a number of ships and led to the temporary shutdown of one of Saudi Arabia's port. Moreover, as to the flying drones, the majority of all Houthi maritime drone attacks were directed not against military targets but instead against commercial and civilian ones: four targeted civilian ports and two targeted oil production and distribution facilities.[30] This brief section has showed the considerable and substantial impact of drones used by irregular militias in the Middle East. This is an increasing threat because current technology offers different tools and possibilities that irregular groups can use in the future to improve their military capabilities. We are witnessing a profound technological revolution that, in contrast to what we experienced, for example during the Cold war, is an open one. That means that each group, or even person, can use modern technologies, improve them, combine different tools and

[27] Saadoun 2021.

[28] Weiss 2019.

[29] Foucher 2020.

[30] Haugstvedt 2021.

create something new and unexpected. A similar phenomenon occurred, for instance, in the 19th century with the invention and the development of dynamite.[31] Therefore, it is important to analyse current operations in order to understand beforehand possible evolution and novelties.

## Conclusion

The focus of this chapter on technology must not make us forget that war is an extremely complex and articulated socio-political phenomenon that cannot be understood solely and exclusively through a purely technological interpretation. However, even when speaking of technology, not all analysts agree in outlining which is the best way to implement modern and advanced technologies. From this point of view, a recent article[32] highlights some limitations of modern strategic thought focused on technology. In fact, the two authors, experts on issues related to cyber threats, underline how the same capabilities, which led the United States to exploit the information revolution (the so-called RMA) to their advantage and that made them in the two decades after the end of the Cold War a power superior to all others, have now become troubling vulnerabilities. The U.S. now carries out campaigns that depend heavily on the digital operations so much that they are vulnerable to new cyber threats, but those same campaigns are not yet sufficiently advanced to be able to take advantage of the latest information technologies. The aforementioned NATO documents answer this problem by saying that we need to increase our efforts and further improve our technologies. The authors support a very different thesis that is more in line with the hybrid threats approach because they invite to review old concepts and find a new approach whose objectives must no longer be speed and decision-making advantage, but on the contrary persistence and resilience. The focus should therefore be on building decentralised networks, investing in tactics that decrease the economic cost of warfare, and developing weapon systems and tactics that do not stop working suddenly and catastrophically, but gradually lose their capabilities in a while once hit. The problem that the authors highlighted is not so much related to technological advancement and, therefore, to the fact that other international actors develop more advanced technologies,

[31] Cronin 2019.

[32] Schneider–MacDonald 2020.

but the fact that the threats against modern information technology adapt faster than the information revolution on which Western strategic thought in recent decades has been based. Modern systems are indeed very vulnerable to network failures and data manipulation. Since the beginning of the computer revolution, its supporters have argued that the victory was the result of a greater knowledge on the local situation which would consequently have allowed greater accuracy of the strikes, while increasing both the speed of action and the distance between target and launch platform. Consequently, investments in technology favoured efficiency and speed over safety and resilience and the acquisition of a small number of expensive and elaborate weapon systems (a clear example of this is the endless controversy related to the F-35).[33] On the contrary, today we should invest in resilience and in systems that change the cost equation by favouring quantity over quality and decentralisation over speed. The old networks were, and remain, strongly centralised, today they would be more secure and resilient networks with high density, small nodes and multiple paths. Such networks are less vulnerable to attack and create less of a cascade effect when compromised with single nodes that can continue to operate. In addition, this race towards the latest technological advance has indeed led to some tactical advantages related to the use of highly technological tools, but at the same time has created a great strategic cost problem. The example of the Hamas missiles that nearly ran out of Israel's expensive Iron Dome in May 2021 is just one of many examples that can be given. It would, therefore, be smarter today to invest in cheap products and disposable technology in order to create mass and resilience. It is, therefore, necessary to combine the modern, advanced and expensive (and thus scarce and difficult to replace) weapon systems with cheaper autonomous sensors and platforms designed to create friction and slow down the opponent's action. Another problem created by the digital revolution is the enormous mass of information. At the beginning, many argued that this was good as it would allow detailed knowledge and greater precision. However, today we know that, while not denying those advantages, the flow of information can be transformed into a weapon both to confuse the enemy (the theme of ambiguity returns) and to undermine it internally through propaganda or fake news. In this context, we no longer need more technology, more AI, more information, but men and soldiers able to interpret, understand, reason and, therefore, able to contextualise what they read from the information.

[33] O'Malley–Hill 2015.

## Questions

1. Can you describe the use of drones in the Middle East region?
2. How does NATO approach the problem of Emerging Disruptive Technologies?
3. What is ambiguity?
4. What is contested environment?

## References

Al-Monitor (2021): Drone Attack on Saudi Airport Injures 8. *Al-Monitor,* August 2021. Online: https://www.al-monitor.com/originals/2021/08/drone-attack-saudi-airport-injures-8

Biddle, Stephen (2021): *Nonstate Warfare. The Military Methods of Guerillas, Warlords and Militias.* Princeton: Princeton University Press.

Boot, Max (2006): *War Made New. Weapons, Warriors, and the Making of the Modern World.* New York: Gotham Books.

Clausewitz, Carl von (1984): *On War.* Princeton: Princeton University Press.

Cronin, Audrey K. (2019): *Power to the People. How Open Technological Innovation is Arming Tomorrow's Terrorists.* Oxford – New York: Oxford University Press.

Doctor, Austin C. – Walsh, James I. (2021): The Coercive Logic of Militant Drone Use. *Parameters,* 51(2), 73–84. Online: http://doi.org/10.55540/0031-1723.3069

Foucher, Vincent (2020): The Islamic State Franchises in Africa: Lessons from Lake Chad. *International Crisis Group,* 29 October 2020. Online: https://www.crisisgroup.org/africa/west-africa/nigeria/islamic-state-franchises-africa-lessons-lake-chad

Haugstvedt, Håvard (2021): Red Sea Drones: How to Counter Houthi Maritime Tactics. *War on the Rocks,* 3 September 2021. Online: https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/

Haugstvedt, Håvard – Jacobsen, Jan Otto (2020): Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponised Unmanned Aerial Vehicles (UAVs–'Drones'). *Perspectives on Terrorism,* 14(5), 26–40.

Jervis, Robert (1976): *Perception and Misperception in International Politics.* Princeton: Princeton University Press.

Liddell Hart, Basil (1991): *Strategy.* New York: Meridian.

Luttwak, Edward (2001): *Strategia. La logica della guerra e della pace.* Milano: Rizzoli.

Mazarr, Michael J. (2015): *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle: The United States Army War College Press.

Middle East Eye (2021): Israel's Gantz Says Iran Giving Militias Drone Training Near Isfahan. *Middle East Eye,* 13 September 2021. Online: https://www.middleeasteye.net/news/israel-iran-gantz-militias-drone-training-isfahan

Mitzer, Stijn – Oliemans, Joost (2021): The Militiamen's UCAV: Mohajer-6s in Iraq. *Oryx,* 31 August 2021. Online: https://www.oryxspioenkop.com/2021/08/the-militiamens-ucav-mohajer-6s-in-iraq.html

NATO (2019): *London Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London on 3–4 December 2019. Online: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO (2020a): *NATO Advisory Group on Emerging and Disruptive Technologies. Annual Report 2020.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

NATO (2020b): *NATO, Science and Technology Trends 2020–2040.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO (2021a): *NATO 2030.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf

NATO (2021b): *Summary of the NATO Artificial Intelligence Strategy.* Online: https://www.nato.int/cps/en/natohq/official_texts_187617.htm?fbclid=IwAR235gFvoqQuyrB1iC5EcBSholcs2Anl9Le6O7LRjC7wDJuuHu1BSjh1eI

O'Malley, Derek – Hill, Andrew (2015): Close Air Support in 2030: Moving Beyond the A-10/F-35 Debate. *War on the Rocks,* 28 May 2015. Online: https://warontherocks.com/2015/05/the-a-10-the-f-35-and-the-future-of-close-air-support-part-ii/

Priebe, Miranda – Vick, Alan J. – Heim, Jacob L. – Smith, Meagan L. (2019): *Distributed Operations in a Contested Environment. Implications for USAF Force Presentation.* Santa Monica: Rand.

Robinson, Linda L. – 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.

Saadoun, Mustafa (2021): Iraqi Armed Factions Using Drones against US-led Coalition. *Al-Monitor,* May 2021. Online: https://www.al-monitor.com/originals/2021/05/iraqi-armed-factions-using-drones-against-us-led-coalition

Schneider, Jacquelyn – MacDonald, Julia (2021): The Information Technology Counter-Revolution: Cheap, Disposable, and Decentralized. *War on the Rocks,* 19

July 2021. Online: https://warontherocks.com/2021/07/the-information-technology-counter-revolution-cheap-disposable-and-decentralized/

Sechser, Todd – Narang, Neil – Talmadge, Caitlin (2019): Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War. *Journal of Strategic Studies,* 42(6), 727–735. Online: http://doi.org/10.1080/01402390.2019.1626725

The Times of Israel (2021): Multiple Iranian Drones Used in Deadly Attack on Israeli-Operated Ship – Report. *The Times of Israel,* 31 July 2021. Online: https://www.timesofisrael.com/multiple-iranian-drones-used-in-deadly-attack-on-israeli-operated-ship-report/

Thiele, Ralph ed. (2021): *Hybrid Warfare. Future and Technologies.* Wiesbaden: Springer. Online: http://doi.org/10.1007/978-3-658-35109-0

Tzu, Sun (1990): *L'arte della guerra.* Roma: Ubaldini Editore.

Weiss, Caleb (2019): Analysis: Houthi drone strikes in Saudi Arabia and Yemen. *FDD's Long War Journal,* 7 August 2019. Online: https://www.longwarjournal.org/archives/2019/08/analysis-houthi-drone-strikes-in-saudi-arabia-and-yemen.php

Andrew Dolan[1]

# Hybrid Warfare and Strategic Surprise

There is no single definition of what act or acts constitutes a strategic surprise in warfare but certainly any unpredicted move, which results in a significant and perhaps decisive dislocation of the adversary at the time of that act, would not be too far away from our common understanding. In the literature of security studies, it is a well-recognised area of particular research, arguably because military history is replete with examples of strategic surprise. Are there serious students of Strategic Studies or War Studies who have not heard of Pearl Harbor? The question, however, is less about the general history of strategic surprise and more of its applicability to what we currently label as 'Hybrid Warfare'. Does the latter form of conflict particularly lend itself to 'surprise' as a favoured tool of military engagement, especially beyond the operational level and if so, what might it look like? That strategic surprise is important in any serious engagement is not in question but how should we go about determining if it has a particular resonance with Hybrid Warfare or does it really follow the patterns of other military activities – albeit in different times and places – that encounter surprise only and if particular circumstances allow it?

## A historical overview

In recent times, strategic surprise has become a familiar feature of modern warfare. It has come in many shapes and sizes but generally it seems to follow an acceptable pattern.[2] The Japanese attack on Pearl Harbor in December 1941 has often been the case study benchmark when considering strategic surprise. Despite fragments of indicators and warnings, the attack achieved surprise at various operational levels and certainly impacted on the future conduct of the war itself. The key features of surprise were present for all to see, including the target, the timing, the concealment and the strategic objective. Following on from

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

[2] Betts 1981.

DOI: https://doi.org/10.36250/01237_10

the German offensives in Europe between 1939 and 1941, which demonstrated the strategic and operational surprise attainable from the utilisation of new forms of strategic doctrine allied to new forms of technology – for example the nexus of 'Blitzkrieg' and improved tanks – there was an undoubted gain to be had through the extensive use of surprise.[3] The Cold War and especially the development of significant early warning systems on both sides in one sense made the attainment of strategic surprise more problematic but on another, showcased the potential for surprise through the development and deployment of new technologies. The deployment of the 'Sputnik' satellite was clearly a force multiplier in terms of shock and the complication associated with then traditional concepts of nuclear war fighting. One might arguably claim that the spread of so-called 'proxy' conflicts during this period also benefitted from various forms of surprise, including the Cuban Missile Crisis, the 'Six Day' 1967 and Yom Kippur 1973 Wars in the Middle East and the Soviet invasion of Afghanistan in 1979 as more traditional advantage could not be had in the European theatre. Proxy forces in South East Asia and the Middle East – often using asymmetrical forms of conflict as a platform for surprise – were adept at shifting the central calculations of dominant forces in their region.[4] The period up to the end of the Cold War also created a situation where strategic surprise was becoming more difficult to reconcile alongside strategic unwillingness to use force for any length of time. The Soviet invasions of Hungary in 1956 and Czechoslovakia in 1968 demonstrated a willingness to use force, which was a shock to the system of the 'West' in so far as it highlighted their lack of willingness to respond. Under these conditions of wilful blindness, strategic surprise does not have to be overly sophisticated.[5] The Falklands War of 1982 followed a similar pattern; strategic surprise – if one may call it that – was attained in part through a combination of loose U.K. strategic thinking and assessment and the pruning of what little resources were available that perhaps might have mitigated the effects of the Argentine moves.[6] Of course the more modern examples of strategic surprise – one thinks of 9/11 or the Russian seizure of Crimea in 2014 – deviate little from traditional concepts of surprise. The nature, timing and form of surprise completely dislocate

[3] Wohlstetter 1966.

[4] Brunnstrom 2022.

[5] Handel 1989.

[6] A post-war review of Falklands policy clearly demonstrated the effects of budgetary restrictions reflecting policy and operational options.

traditional forms of calculation, whether in terms of the form of the response or the possibility of a significant retaliation. The wars in Afghanistan and Iraq in the post '9/11' strategic environment demonstrated at times tactical and operational surprise, but the predominant strategic impact was undoubtedly the recent fall of Kabul and the return of the Taliban in Afghanistan and the lack of Western willingness to resist. That was a fundamental strategic surprise.

## Traditional factors

Initiating a military engagement when your opponent least expects it is a hallmark of strategic surprise. It is a hallmark at any military level. This is particularly so if a wider spectrum of your friends and allies are equally caught unaware. Very often, ensuring strategic surprise can largely depend on a level of operational preparedness that even allies remain unfamiliar with. Timing, often positioned alongside the choice of location – the operational environment where this surprise might be achieved in order to generate the greatest military benefit – can significantly impact on one's chances of success. This becomes particularly critical if your choice is being influenced by other critical military factors such as force disposition, the balance of power, an adversary's preparedness or lack of it and very often, considerations of weather or geography. This factor of timing is also important in the wider strategic spectrum including perhaps the geopolitical context, global economics or internal or domestic politics. In a close reading of some classic strategic surprise, one can easily see that timing can be crucial and can have an impact beyond the immediate possibility of victory on the ground. For example, the Japanese attack on Pearl Harbor sought to inflict a crippling blow not only when the U.S. Navy was most likely to be concentrated in Hawaii but in a more regional and global context, as the U.S. authorities had yet to build up military strength in the Pacific region commensurate to the acknowledged Japanese threat and the likelihood of further success for Germany in the European Theatre.[7] Similarly, the North Vietnamese 'Tet Offensive' in early 1968, which in a sense unhinged U.S. military perceptions of the course of the ongoing struggle in Vietnam, from eventual victory to eventual defeat, clearly signified genuine strategic surprise on the back of

[7] Betts 1981.

localised tactical but networked attacks.[8] Of course, it is essential to remember that strategic surprise very often is still achievable despite being observed in part through traditional forms of indicators and warnings. Again, in reference to Pearl Harbor, the post-event investigation clearly highlighted numerous forms of early warning but which were either inadequately assessed, or not acted upon, by the analysis and decision-making chain. Nevertheless, it is fair to say that timing has and is likely to remain a key factor in strategic surprise. Another major consideration in attaining strategic surprise is concealment and deception. These two factors are generally ‘joined at the hip’ in terms of military planning and alongside timing, are major contributory factors to taking one’s adversary by surprise. Deception is also a twin-edged weapon. How often do we see that a defender’s response to an unanticipated attack is complicated or diluted due to one’s own self-deception? Without exploring too deeply into the issue of cognitive dissonance, it is fair to claim that this form of self-deception can and often does aid strategic surprise. The case for the invasion of Iraq in 2003 is frequently cited as evidence of various forms of self-deception as far as analysis of intelligence was concerned. This is arguably unfair on the analytic communities who genuinely believed that a WMD threat clearly existed and in fact such a posture was only maintained in large part through Iraq’s own actions which lent credence to the view that they had in fact some WMD to hide.[9] Military studies are replete with examples of deception and concealment that has contributed to strategic surprise. In the build-up to the D-Day operations in France in 1944, forms of deception included the construction of ‘Potemkin-style’ airfields, military formations and HQs, large tank parks and the use of exercise all indicating future intent but far from the intended target. Such deception was accompanied by the concealment of real formations and troops and the extensive use of false signal communications. Another form of deception and concealment in order to achieve strategic surprise was attempted by Argentina during the Falklands War, with early deployment of maritime forces around the island of South Georgia, was conducted in such a way in order to confuse the U.K. authorities. That such behaviour on the part of Argentina had been seen before contributed to the uncertainty about identifying intent. Therefore, deception and intent are often successful when it seems no different from the routine.

[8] Bowden 2018.

[9] This conviction of Iraqi duplicity was behind much of the sentiment in the UN Security Council, as much as belief in Iraqi deception on the part of the U.S. and U.K.

The surprise attack on Israel in 1973 across the Suez Canal by Egyptian forces is also often cited as an example of the concealment of intent. Yet as much as the deception was about timing and no small amount of tactical and operational surprise, especially through the use of man-portable anti-tank missiles, a salient feature of the surprise aspect of the invasion was the use of more or less commercial applications – high pressure pumps and hoses – to soften up Israeli defensive sand barriers along the Canal in order to breach the defensive walls and facilitate easier passage through the breaches.[10] Students of military conflict quickly acknowledge that the deployment of new military technologies or weapon platforms can impact surprise and deception. The Cold War, given its duration, provided numerous examples, including the Soviet Union's development of an atomic bomb, the so-called 'Sputnik' moment and of course the positioning of missiles in Cuba. All of these examples demonstrate that the development or covert deployment of weapons can contribute to some form of strategic surprise, even if the aim is not to initiate war but simply be better positioned for it should one arise. Deception and concealment under these conditions can certainly impact on calculations of the balance of power. Of course, it will be argued that achieving complete military surprise today is virtually impossible given the vast array of technical surveillance means available to states or military blocs. Sophisticated indicator and warning systems serve to provide early warning of impending moves, which either individually or in tandem with other actions might suggest the prelude to war. Admittedly, such systems can be overcome, although it is undoubtedly likely that in order to do so will require either some form of surprise or in recognition that surprise is not a factor if you possess overwhelming force. Another factor in achieving strategic surprise is the generation of situational complexity in the circumstances in which an adversary has to respond, particularly in terms of decision-making and strategic and operational communication. In late 1944, the German High Command launched an audacious surprise offensive against the Allies at the Battle of the Bulge. Apart from the fact that the offensive was unexpected, in part because the Germans were considered to be incapable of generating such a move, the surprise was attained due to fault intelligence and clear forms of deception at the operational and tactical level. As a case study, this operation demonstrated how important to strategic surprise was the confusion of higher echelons of command and how difficult it

[10] Dunstan 2007.

can be during the 'fog of war' to make decisions.[11] If brought up to date, in a situation saturated by electronic warfare, cyber operations, attaining surprise might still be achievable. The difficult question is how to integrate these various actions that contribute to masking transparency in situational awareness or disrupts the ability to communicate effectively. Add to the mix the problem of active deception measures and a lack of political will and then strategic surprise is quite feasible even today. Proponents of Hybrid Warfare point to the Russian invasion of Crimea in 2014 as a prime example of strategic surprise allied to a reluctance by adversaries – either for political or military reasons – to leave the deception unchallenged. Similarly, the failure to appreciate the consequences of policy can also create a situation that hinders one's ability to react to an unexpected strategic shock. The recent withdrawal of the U.S. and allied military forces from Afghanistan will be subject to forensic autopsy for years to come but in essence, no amount of solid intelligence can help if incorrect conclusions are drawn by policy makers as to the consequences of their policy actions.[12] Strategic surprise comes in many shapes and sizes. It certainly does make sense to place your adversary in a situation whereby they cannot identify your intent (until it is too late to do anything about it), fail to take effective countermeasures and then find himself in a situation, where effective command and control has been removed. Today, technology in part does seem to offer such a capability. Added to an ability to hide in plain sight and the willingness to engage in strategic miscommunication or plausible deniability as it used to be called, the battlefield of today and tomorrow might be a strategic space where complexity and confusion reigns irrespective of how well prepared you are or how sophisticated is your ability to direct and control numerous small sub-strategic unexpected operations in order to achieve a larger strategic element of surprise.

## Technological advancement and emergent technology

When the enemy is able to deploy military technologies in such a way or on such a scale that it makes effective response either futile or too costly, then in

[11] Caddick-Adams 2015.

[12] So soon after the event, it is difficult to gain a complete or even partial insight into the intelligence picture which governed allied responses, although anecdotal speculation would suggest some form of intelligence failure, but more certainly a policy failure.

a sense, they might have achieved a form of strategic surprise. Developments in weapon technology, including enhanced range, velocity, payload, surveillance or kinetic effectiveness are generally a constant in warfare. From the ancient world's 'Greek Fire' to the advent of the 'Dreadnought' through to the atomic and thermonuclear bombs and the satellite, there has been a steady evolution of weapons technology that to some extent has generated at times a form of strategic concern if not complete surprise. However, is the deployment of such novel 'weaponised' technologies sufficient to guarantee success at the strategic level or is the impact they make more suitable at the operational level?[13] There is a school of thought that sees Hybrid Warfare as the crucible of new thinking and imagination on the exploitation of emergent and dual technologies to attain true strategic surprise and victory. Some years ago, Russia's President Putin highlighted artificial technology as a 'game changer' in terms of military dominance and ultimate victory. Why this should be so was easy to appreciate. Developments in numerous new and emergent technologies ranging from nanotechnologies to quantum computing have the potential to stimulate research and create new battlefield solutions for the major and arguably not so major power. Many commentators who operate in the recent field of 'existential risk' even suggest that the empowered non-state actor is as equal a threat as traditional states, with the malicious use of artificial intelligence and life sciences capable of creating biological weapons suitably genetically modified to pose significant small- or large-scale threats. What technologies might contribute to the acquisition of such transformational capability and how would it contribute to strategic surprise? It seems likely that our traditional acknowledgement of weapons evolution is most likely to engender the conditions in which strategic surprise would be most effective, namely that we might fail to determine what constitutes a significant 'revolution in military affairs'. For example, the deployment of forms of Lethal Autonomous Weapon Systems is surely not far off. To date, deployment of such systems has been limited but it would not be unreasonable to anticipate a wider deployment in the future. Greater exploitation of robotics will be significant but greater surprise will be achieved through the introduction of augmented humans – soldiers on the battlefield with augmented capabilities ranging from strength and stamina to the exploitation of personnel weapons with greater accuracy and precision. Add to this mix the acquisition of real time data and communication systems capable of operating unmolested

[13] Cronin 2020.

in space and if required, with an ability to disable competing space systems and the battlefield space might constantly surprise you. A careful reading of the above demonstrates the importance of attaining superiority of networked systems associated with the national capacity to operate a networked society. Military systems are but one element of an integrated social-supporting data system. As such it is a part of critical network infrastructure that requires protection in peace and war. Would the disabling or confusing of such networks constitute strategic surprise? In one sense, it should not come as a surprise that computer networked data systems might become a target in the sense that the disabling of energy systems in Ukraine or similar attacks in Saudi Arabia are little different from bombing attacks in the Second World War on strategic dams in Germany. The obvious difference is the methodologies of attack and the lethality of the consequences. Cyber operations, if successful, can inflict considerable damage and disruption on a society and it would be unwise to appreciate the potential scale of the loss of human life that might occur, even assuming data operations and communication links can be restored.[14] Yet, surprise might be achieved depending on the arrangement and alignment of cyber operations, the targets and the timing. Should security loopholes be identified in critical operating systems within a system of critical network infrastructure, then the time of cyber penetration can afford an aggressive intruder the opportunity to achieve the unexpected, even against the most outwardly protected systems. It is this control over information and its use that provides another typical factor in achieving a form of strategic surprise, namely disinformation. Indeed, some forms of modern, algorithm-based technologies, can so shape information operations that the concept and products of so-called ‘Fake News’ often dominate public discourse of events, including those on the battlefield.[15] Advocates of disinformation are surely correct when they stress how important it can be in times of conflict, from sapping the morale of a hostile public to encouraging state policies which run counter to the best interests of your adversary. Propaganda and psychological operations have always been useful tools in times of war but less developed is an understanding of how a concerted disinformation campaign can, over the longer term, help shape a situation, which if developed and exploited properly, can contribute to strategic surprise. One need only look at the aggressive information policies of Ukraine and Russia, as they seek to control the war’s narrative to

[14] Even – Siman-Tov 2012.

[15] Fridman 2022.

get a sense for how powerful and effective controlled information can be. Yet the fact remains that disinformation is often a dual edged weapon. The sense of disbelief, dislocation and anger experienced should a particular message be found to be untrue can undo years or months of painstaking strategic messaging. Trust is a particularly important concept in people's lives and the general and global generation of 'fake news' is likely to lead to a sceptical public that trusts no sources of information or very few sources. Under those circumstances, using disinformation might become more difficult to manage than hitherto has been the case.[16]

## Utility and impact of surprise

Should hybrid conflict lend itself more to the exploitation of surprise than any other form of conflict or warfare? Do the factors outlined above suggest a greater expectation of the necessity of surprise, an expectation fuelled in part by the rather more fanciful descriptions of what might constitute hybrid war? Each generation tends to see conflict through the prism of their own experiences and circumstances and for some commentators, highlighting the hybrid nature of war seems a reasonable way of explaining the complexities of modern forms of conflict and the technologies associated with it. It can reinforce stereotypes of war. Is there such a thing as 'Hybrid Warfare' and is it appreciably different from wars fought in the past? It is often said that "beauty is in the eye of the beholder" and perspectives on this subject are as numerous as the opinions held but it is perhaps fair to say that there is no undisputed conclusion. Strategic surprise, however, is rarely disputed in terms of its aims and therefore assessing its utility might be more straightforward. Let us look at some basic premises. Is strategic surprise a cost-effective tool for use in times of conflict? The answer would seem to be an unequivocal yes. Warfare is extremely costly and is generally reflected in the downsizing of military formations and equipment holdings as technology increases in sophistication and cost, not to mention development time. Any form of strategic surprise that decreases the need for heavy forces or sustained operations or in extremis, the occupation of foreign territory, should at the very least be explored. Even most recognised forms of hybrid conflict would assume the same set of strategic calculations. The same might be argued in terms of

[16] Fridman 2022.

exploiting dual use technologies, either as a way to maintain an economic balance in terms of military power and as a way to reduce research and development costs or simply as a form of attaining a force multiplier effect. Discussion within hybrid warfare circles stress such asymmetric benefits but frankly such calculation is inimical to all professional considerations of war and peace. The only surprise would be if this were not to be considered a factor. Of course, this exploitation of dual use technologies has traditionally been a hallmark of the dedicated terrorist and if future terrorism or proxy warfare on non-state actor – such as organised crime – seek to influence politics and society through violence, then strategic surprise is even more likely. The attacks on the Twin Towers on 9/11 in New York with hijacked civilian aircraft clearly demonstrated that 'imagination' is an equally vital quality in attaining strategic surprise and perhaps indicates that hybrid warfare irrespective of scale will find the creation of strategic surprise invaluable, less perhaps as a contributory factor to an immediate victory and more perhaps a form of strategic signalling.[17] Yet if hybrid conflict values the role of non-state actors as a form of, or only means of asymmetrical engagement, it is still unlikely to generate strategic repositioning or attain a shift in the balance of power in the absence of other forms of engagement and we have to ask if such actions would generate strategic surprise? One such area of Hybrid Warfare that might be amenable to the utilisation of surprise is in the exploitations of vulnerability in critical networked systems. As described earlier, the ability to complicate command and control, especially at the outset or at least the early stages of a conflict and influence decision-making is one way to secure strategic surprise and therefore it should be anticipated that most of not all future conflicts, hybrid or otherwise, might seek to exploit this area of activity. The attraction of this form of activity lies not in the sense that it might be classified 'hybrid' but rather that it could be particularly effective and create the conditions upon which surprise could be achieved. Networked societies based upon future concepts of the so-called 'network of things' have enormous potential for societies but similarly, the potential for great disruption resides within it. By and large, the developers and producers of 'smart' applications have a less acute interest in security and place a greater emphasis on safety and efficiency. We can already observe the consequences of dedicated and complex cyber penetrations of protected networks that control energy or logistics for example. The non-attributable

[17] Most strategic analysts believe 9/11 was a classic example of strategic signalling, as much as surprise.

cyberattack on an Iranian nuclear site and the manipulation of the plant's systems control and data acquisition systems not only achieved surprise but also brought the vulnerabilities of such systems into stark relief for the world to see.[18] It is unquestionably true that any future conflict will seek to dominate both the real and virtual spaces in which military operations might flourish. Whether this move into the cyber world and the attainment of 'cyber surprise' justifies the label is a moot point. At which stage does operational surprise translate as a strategic surprise in a cyber context? Does global interconnectivity disruption qualify as a feature only to be associated with hybrid conflict or is it simply how conflict evolves under current conditions?

## The Russia–Ukraine Conflict 2022: Hybrid or traditional?

The current phase of the Russia–Ukraine conflict, as reflected in the invasion of Ukraine by Russian forces in February 2022, is but the latest phase in a conflict that has been ongoing since the Russian annexation of Crimea in 2014. Some commentators saw in the strategic surprise achieved by the Taliban in Afghanistan in August 2021 some sort of stimulus to Russian calculations for invasion, particularly in relation to likely Western reaction. Other observers noted that Russia, having used various forms of force and diplomacy during the Syrian civil war, would eventually shift its emphasis to strategic issues nearer home and 2022 was as good a time as any.[19] With a shift in emphasis away from Crimea to the Donbas region, which was wracked by instability and ongoing low-level military engagement, Russia clearly envisaged an opportunity to swiftly intervene militarily to affect the balance of power on the ground. Yet it would be difficult to argue that the subsequent Russian intervention – Hybrid War or not – actually exploited any traditional form of strategic surprise. Indeed, the steady build-up of military force in the Russian–Ukraine border regions and a similar build-up in the Belarus–Ukraine region was hard to miss. Of course, one could plausibly argue that the continuation of diplomatic negotiations and the steady stream of Western politicians seeking to dissuade Russian President Putin from using force was a convenient tool for allowing Russia to bring its military forces up to combat readiness. Subsequent conflict since the invasion seems to

[18] Zetter 2015.

[19] Fridman 2022.

question just what level of combat readiness Russian forces actually acquired and actually what strategic surprise achieved lay in the fact that Ukrainian forces inflicted tremendous punishment on the Russian invaders and which led to a shift in strategic objectives away from conquering Ukraine to hopefully controlling the Donbas region. This was not a strategic surprise that Russia might have anticipated. Of course, the Russian military invasion of Ukraine significantly altered this situation on the ground in Ukraine and globally, in terms of the international legal norms and European and international security. However, does it justify the label of hybrid and more importantly, did this form of conflict lend itself to strategic surprise? Most commentators seem to agree that Russia had been signalling its intent to invade well before the first forces crossed into Ukrainian territory and that this intent – including very public and large-scale military manoeuvres – had been noticed and analysed by western intelligence sources. In short, there was no strategic surprise per se.[20] Inevitably, the ensuing military operations, by definition, had no aim associated with the achievement of strategic surprise but rather the accomplishment of limited military objectives. However, one might argue that inadvertently, the conduct of those operations and tactics on the part of the Russian military, particularly the failure to achieve their objectives, signalled a strategic surprise to their western counterparts. In short, most commentators were surprised to find the Russian military significantly short of its presumed war fighting capability. Western analysts have been repeatedly surprised by the ineffectiveness of Russian military management and operational art and that no amount of technological capability seems able to make up the shortfall. Another early feature of the campaign to date has been the relatively minor role played by cyber operations as a means either to acquire surprise or to affect an operational difference. One particular and notable cyberattack on Ukrainian internet systems was blocked by a U.S. commercial satellite operator. Under hybrid warfare discussions, cyber operations are frequently cited as an integral hybrid activity but in reality, at least in this conflict, it has not really surfaced. Yet if perceived from another angle, one might plausibly argue that Russia's invasion seemed to reflect several hallmarks of a Hybrid Conflict. Aside from the continuing efforts to exploit traditional military firepower, including the managed use of new technologies, especially hypersonic missiles, what the general public might consider as hybrid features seem to be present. We have just

[20] In fact, given the very poor performance of the Russian forces during the initial invasion of Ukraine, suggests that the strategic surprise was actually felt in Moscow more than in Kyiv.

mentioned Cyber Warfare as being integrated from the beginning of operations but perhaps on a scale somewhat less than had been anticipated. Certainly no cyberattack dislocated Ukraine's ability to respond to the initial invasion. That, however, does not reflect the fact that the continued use of cyber weaponry by Russia or against Russia creates some form of tactical surprise and inconvenience. Both sides have not given up on cyber capabilities and in fact, electronic warfare – perhaps not cyber warfare – if blended with other forms of electronic or data disruption is becoming a new hallmark in war and not strictly at the outset as strategists once thought more likely. Another feature of the conflict is the Russian willingness to not only use Proxy forces from the Russian-controlled Donbas region but to also recruit and deploy a range of irregular or non-state actors including individuals and groups representing private military companies (the Wagner Group), forces from Chechnya, the Caucasus and Syria. Obviously, the use of such proxies or irregular forces complicates the battle space and the laws of war but there seems every likelihood that such deployments might well become a regular feature of modern forms of conflict, hybrid or otherwise.[21] Similarly, as the war in Ukraine has dragged on, unanticipated actions seem likely again to reinforce the notion of hybrid and in particular, in relation to the use of food supply as a weapon of war. Russian authorities have seized on their control of Ukrainian grain and its necessity for the feeding of numerous populations globally as a tool to influence both Ukrainian and international behaviour, particularly in relation to economic sanctions. Tempting as it might be to see this as a form of Hybrid Warfare and one that might become more prominent in the future, some commentators will simply view this is as but another example of 'Total War'. One would be forgiven for having sympathy with this view. Yet equally, the ability to exploit international legal arrangements for the smooth operation of free trade, the ability to use sanctions and other forms of dissuasive influence to curtail trade in specific areas or sectors and particularly on parties not directly involved with the conflict seems to be reaching new heights and which takes it beyond traditional concepts of economic warfare. Some observers will finally highlight the global communication and public information war as another feature of modern hybrid war. They also highlight that public perceptions are influenced by fake news platforms and that in Western societies at least, media transparency is frequently subject to malicious interference and claim and counterclaim over the veracity of sources of information, including video

[21] The more recent activities of the Wagner Group seem to be proving the point.

and audio ‘eyewitness accounts’. That this is likely to become a significant ‘real time’ feature of modern conflict does place it somewhat in a different league but whether or not this can generate strategic surprise might be a moot point. Undoubtedly, the technology exists to fabricate reality – so-called ‘deepfake’ products – and in any future crisis, anything that places doubt in the mind of the decision-maker has the potential – depending on the deception – to significantly ‘alter reality’ and result in strategic surprise.

## Conclusion

There is very little in Hybrid Warfare that differs from traditional forms of warfare and as such, one must anticipate attempts in the future to achieve strategic surprise. However, do less typical forms of Hybrid Warfare make it any more likely that surprise can be attained? One might conclude by saying that the potential for achieving surprise in conflict today is no more or no less favourable than it was before. Certainly, the wider application of various forms of new technology, ranging from cyber weapons to ‘deepfake’ products, does offer those responsible for creating deception or concealment some additional opportunities. The way our societies are developing and the greater reliance on information network and data development equally hold out promise for new and imaginative forms of disruption. However, perhaps the future of hybrid might relies less on the blending and integration of numerous forms of traditional forms of activity repackaged and more on the integration of human and machine applications to create a novel form of battle space where attaining surprise is built into the future algorithms of war.

## Questions

1. How would you define the concept of ‘Hybrid Warfare’ and how would you assess the most effective way for strategic surprise to be achieved through this form of conflict?
2. Explain the main differences between traditional modern conflict and the common features most commonly used to describe Hybrid Warfare.

3. In reviewing major global warfare since 1939, identify the most common features of strategic surprise and how these might apply today in terms of hybrid conflict.
4. What activities – if any – led to the Russian attainment of strategic surprise during the invasion of Crimea in 2014?
5. Can forms of terrorism achieve strategic surprise? Discuss.

## References

Betts, Richard K. (1981): Surprise Despite Warning: Why Sudden Attacks Succeed. *Political Science Quarterly,* 95(4), 551–572.

Betts, Richard K. (1982): *Surprise Attack. Lessons for Defense Planning.* Washington, D.C.: Brookings Institution Press.

Bowden, Mark (2018): *Hue 1968. A Turning Point of the American War in Vietnam.* New York: Grove Press.

Brunnstrom, David – Needham, Kirsty (2022): Pacific May Be Most Likely to See 'Strategic Surprise' – U.S. Policymaker. *Reuters,* 11 January 2022. Online: https://www.reuters.com/world/asia-pacific/us-most-likely-see-strategic-surprise -pacific -official-2022-01-10/

Caddick-Adams, Peter (2015): *Snow and Steel. Battle of the Bulge 1944–1945.* Oxford: Oxford University Press.

Cronin, Audrey K. (2020): Technology and Strategic Surprise: Adapting to an Era of Open Innovation. *Parameters,* 50(3), 71–84. Online: https://doi.org/10.55540/0031-1723.2675

Dunstan, Simon (2007): *The Yom Kippur War. The Arab–Israeli War of 1973.* Oxford: Osprey Publishing.

Even, Shmuel – Siman-Tov, David (2012): Cyber Warfare: Concepts and Strategic Trends. *INSS Memorandum,* 117. Online: https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf

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

Handel, Michael I. (1989): *War, Strategy and Intelligence.* London: Routledge.

Wohlstetter, Roberta (1966): *Pearl Harbor. Warning and Decision.* Stanford: Stanford University Press.

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

## *Further reading*

Gooch, John (2004): *Military Deception and Strategic Surprise.* London: Routledge.

Handel, Michael I. (1984): Intelligence and the Problem of Strategic Surprise. *Journal of Strategic Studies,* 7(3), 229–281. Online: https://doi.org/10.1080/01402398408437190

Healey, Jason (2022): Preparing for Inevitable Cyber Surprise. *War on the Rocks,* 12 January 2022. Online: https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/

Jajko, Walter (2012): Strategic Surprise. *The Institute of World Politics,* 19 September 2012. Online: https://www.iwp.edu/articles/2012/09/19/strategic-surprise/

King, Anthony (2021): *Urban Warfare in the Twenty First Century.* Cambridge: Polity.

Metcalf, Mark (2017): Deception Is the Chinese Way of War. *U.S. Naval Institute Proceedings Magazine,* February 2017. Online: https://www.usni.org/magazines/proceedings/2017/february/deception-chinese-way-war

Miller, Paul D. (2017): Responding to Strategic Surprise. *Atlantic Council Strategy Consortium,* 12 May 2017. Online: https://www.atlanticcouncil.org/content-series/strategy-consortium/responding-to-strategic-surprise/

Vandepeer, Charles B. – Regens, James L. – Uttley, Matthew R. H. (2020): Surprise and Shock in Warfare: An Enduring Challenge. *The Strategy Bridge,* 27 October 2020. Online: https://thestrategybridge.org/the-bridge/2020/10/27/surprise-and-shock-in-warfare-an-enduring-challenge

Wasielewski, Philip (2022): *The Evolving Political–Military Aims in the War in Ukraine After 100 Days.* Online: https://www.fpri.org/article/2022/06/the-evolving-political-military-aims-in-the-war-in-ukraine-after-100-days/

Williams, Phil (2010): Organized Crime in Iraq: Strategic Surprise and Lessons for Future Contingencies. *Prism,* 1(2), 47–68.

Daniel Brezina[1]

# Hybrid Warfare: Case Studies

The primary motivation for choosing the topic under the name *Hybrid Warfare: Case Studies* was that many ambiguities and problematic areas in this area had not been addressed in the past. Suppose individual countries are to be sufficiently prepared and leading government officials can respond adequately to the impact of hybrid threats. In that case, it is necessary to streamline decision-making processes. This publication's primary goal is to analyse selected topics of international political and social events and their subsequent application to the concept of hybrid threats. The case studies examine different forms of hybrid threats and, simultaneously, allow gathering information from which to build a "database" for crisis management, national or international. Case studies present valuable lessons that can be used to streamline decision-making processes and create new strategies. The importance of case studies increases if we want to learn from mistakes that have occurred in the past. The problem can be their misunderstanding and eventual rejection by the competent authorities or the public. The basis for the preparation of the publication was the scientific research activity of the author, as well as the opinions and attitudes of many professionals and experts from various domestic and foreign institutions dealing with the issue of hybrid threats.

## Theoretical background

The number and severity of hybrid threats have been increasing in recent years. This phenomenon began to come to the fore especially after the annexation of Crimea by the Russian Federation. Individual countries are confronted with many requirements, the aim of which is to ensure the required level of crisis prevention with an emphasis on hybrid threats and the ability to effectively and efficiently respond to real threats. This is connected with the need to make optimal decisions and effectively use the available resources needed to deal

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

DOI: https://doi.org/10.36250/01237_11

with hybrid threats. With the development of more complex techniques and technologies, the possibility of the emergence of hybrid threats that hurt the natural evolution of human society increases quite often. Questions about preventing their occurrence and solutions are becoming an increasingly topical subject. They can affect a large number of inhabitants and hurt a large area. Their consequences primarily negatively affect the human community and the material, social and cultural values in the territory affected by the influence of hybrid threats. In some cases, the functionality and stability of the overall operation of the state's economy may be threatened and disrupted. In the introduction of the paper, it is necessary to define the basic terms and concepts related to the solved problem. These will be part of the theoretical basis for analysing selected case studies and will allow us to assess the conditions in which different forms of hybrid threats operate. Several factors influenced the choice of individual terms and their concepts. The issue of fighting in a mixed way is quite complicated. It is necessary to have specific knowledge about systems' behaviour, functions and connections to manage the negative consequences of hybrid threats. Hybrid threats are defined as threats using a specific combination of political, military, economic, social and information means and conventional, irregular, catastrophic, terrorist and criminal activity methods with various state and non-state actors.[2] Hybrid threats are interconnected and operate in the disruption of state functions. As part of conducting a mixed operation in the grey zone, the space is not limited by physical barriers. In this context, actors can use cyberspace, media, operational space, diverse spaces of operations, etc.[3] A tool of hybrid threats can be massive disinformation campaigns and the use of social media for propaganda or radicalisation, recruitment and direct control of supporters. A hybrid attack represents the synchronised use of several power tools adapted to specific weaknesses in the entire spectrum of social functions to achieve a synergistic effect. The advantage of a hybrid attack is that it is complicated to assess whether the application of hybrid tools is taking place in the initial stages. These can be applied for a more extended time, with the damage starting to show itself only after a delay when the target's ability to defend themselves effectively

[2] Glenn 2009.

[3] Jurčák–Turac 2018.

due to these attacks is already significantly impaired.[4] Hybrid threats can also be directly or indirectly related to Chaos Theory. The butterfly effect points out that the movement of a butterfly's wings on one side of the planet can, over time, cause a hurricane on the other side of the earth. These are relatively minor events that can trigger crises. A prerequisite for proper and effective prevention, as well as an effective solution to hybrid threats, is an understanding of their essence, the function and tasks of the bodies responsible for their preparation and resolution, their purpose, culture and processes taking place within them.[5] In case of hybrid threats, it is difficult to predict their emergence and comprehensive course. In addition, the negative impact of hybrid threats can cause several secondary crises, whether in the public or private sector. For this reason, the existence of a specific type of management that deals with this issue and is known as crisis management is essential. For the first time, the term crisis management was used and practically applied in 1962 during the Cuban crisis. American President John Fitzgerald Kennedy assembled a group of experts from various fields whose task was to prevent the outbreak of World War III and to find a peaceful solution to the international crisis during the Cold War.[6] Over time, crisis management has established itself in various areas not only of military but especially of a non-military nature, such as politics, the economy and the field of public administration. The subject of crisis management can be a state, or a group of conditions for joint activity, for example, in the military or the economy. Crisis management, as one of the primary tasks in the field of security, includes various military and non-military procedures that must be carried out, whether in the phase of prevention or response to emerging crises. The North Atlantic Alliance (NATO) has various political–military tools at its disposal to deal with problems with an emphasis on hybrid threats that may threaten the security of the territory and the population of all members of the Alliance.[7] The fundamental theoretical model of crisis management (Figure 1) consists of four crisis management processes – prevention, crisis planning, response and recovery.

[4] Cullen – Reichborn-Kjennerud 2017.

[5] Ishikawa–Tsujimoto 2006.

[6] Šimák 2016.

[7] NATO 2022.

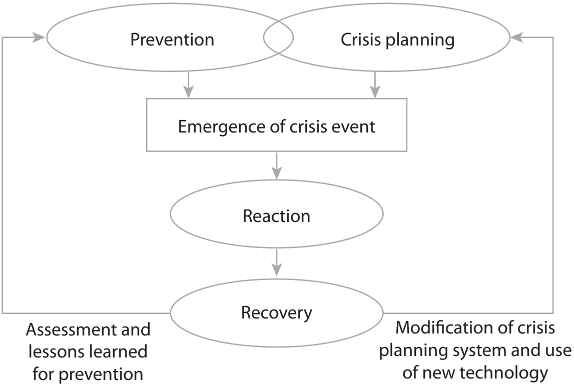
Prevention
Crisis planning
Emergence of crisis event
Reaction
Recovery
Assessment and lessons learned for prevention
Modification of crisis planning system and use of new technology

*Figure 1: The basic theoretical model of crisis management*
*Source:* Horemuž 2010

In the prevention phase, the essential step is identifying and assessing all current risks and threats, followed by processing crisis forecasts and scenarios. The primary goal of prevention is the prevention of adverse consequences of crises through various measures and activities. A separate and no less critical phase of crisis management in the preparatory phase is crisis planning, within which different types of crisis plans are processed.[8] The protection of society created the prerequisites for connecting the prevention phase and the planning documents. The period of preparation for solving crises and their emergence is followed by the period of solving problems. An immediate response to a situation requires the rapid deployment and coordination of the forces and resources necessary to solve it. This phase follows from the direct acquisition of information about the emergence of a crisis and its correct assessment and evaluation. The immediate response is carried out through various activities, the primary objective of which is to save human lives and material values, the environment and cultural monuments. The recovery phase is predominantly developmental, allowing the system to return to its original stabilised (pre-crisis) state. Feedback is of great importance in the basic model of crisis management. It represents a means for improving the quality of crisis management at its various levels.[9] Crisis manage-

[8] Šimák 2016.

[9] Sanseverino-Godfrin 2016.

ment is one of the primary tasks of NATO. As part of implementing an adequate response to emerging crisis phenomena of a natural or military nature, Marinov developed a strategic concept of crisis management within NATO. The model assesses the current situation and creates a comprehensive response through a six-phase crisis management process:

- identification of risk factors with subsequent warning of the population and notification of specific bodies and institutions involved in crisis management
- comprehensive assessment of the crisis phenomenon
- planning phase
- phase of the adequate reaction
- implementation of other necessary measures to minimise the negative consequences of crisis phenomena of a natural or military nature
- transition to a phase that no longer poses a threat to countries that are members of NATO[10]

Marinov's model allows crisis staff and committees within the NATO institution to coordinate their work and provide information to the North Atlantic Council. The individual phases are not precisely given from a time and organisational point of view. They can overlap, and their length depends on the specific situation. One of the basic approaches that will allow us to assess the conditions in which different forms of hybrid threats operate is the analysis of selected case studies. There are five stages to creating a good case study. In the first phase, deciding whether a case study is a suitable method for investigating the selected problem is necessary. The second phase consists of defining the case, the third of data collection and the fourth of their analysis. In the fifth, i.e. the final step, the interpretation occurs, where the researcher's task is to state what he found out about the case during the research.[11] Similarly to the definitions of "hybrid threats" and "crisis management", it is also possible to note considerable terminological inconsistency and ambiguity in the purpose of the term case study. A case study is an ideographic investigation of one individual, family, group, organisation, village or society; its primary purpose is a description. Attempts at explanations are also acceptable.[12] The basis of a case study is

[10] Marinov 2011.

[11] Creswell–Poth 2013.

[12] Rubin–Babbie 2001.

capturing the complexity of cases, describing relationships and their integrity.[13] The premise of the case study is that we can understand many similar cases based on the analysis of one point.[14] A high-quality case study should contain five essential characteristics: the significance of the case, the completeness of treatment, consideration of alternative perspectives, a sufficient amount of data, creativity and attractiveness in therapy.[15] A case in a case study can be explained as a spatially bounded phenomenon observed at one point in time or one period of time. A case in a case study can also represent a fixed phenomenon that is an example of a class of similar phenomena forming a population.[16] The objective of the quantitative research strategy is to standardise specific work procedures. Within the framework of a qualitative research strategy, it is essential how the process of working with the researched object and the specifics of the researched case proceeds, as well as understanding ongoing changes and interactions. As it follows from the individual characteristics of the case study as a research method, many data sources are essential, especially for methodological triangulation. Data analysis is a demanding activity due to its complexity and quantity.

## Case study: Czechoslovak Sudetenland

When examining the definition of the term hybrid war in detail, it can be concluded that the manifestations of this specific type of war are not only characteristic of the period of the 21st century but can be dated much earlier. One of the first ways of conducting a hybrid war was, for example, the annexation of the Czechoslovak Sudetenland to Nazi Germany. The creation of the Czechoslovak Republic in 1918 was preceded by a long academic debate between prominent Czechoslovak politicians and philosophers, which, since the time of Jungmann and Bolzano, concerned the issue of the organisation of the Czech state (territorial principle versus national principle). Tomáš Garrigue Masaryk, the first Czechoslovak President, with his idea of Czechoslovakism, eventually became the most influential thinker and figure in the creation of the

[13] Hendl 2005.

[14] Hendl 2016.

[15] Yin 2009.

[16] Rohlfing 2010.

Czechoslovak Republic.[17] The problem lay in the designation "Czechoslovak" being somewhat imprecise. About 50% of Czechs (approximately 6.8 million), 24% of Germans (approximately 3.2 million), 15% of Slovaks (approximately 1.9 million) and other national minorities such as Hungarians lived in the territory of the then Czechoslovak Republic, in addition to Ukrainians (Rusyns), Jews, Poles and others.[18] President Masaryk offered the Germans to eliminate their anti-Czech attitude and try to build a Czechoslovak state with other citizens. He promised them minority rights and a democratic way of dealing but assured them that the border territory would remain with Czechoslovakia.[19] Soon after the declaration of the Czechoslovak Republic, the military occupation of predominantly German-inhabited territories followed, which, since the end of the 19th century (especially in the Chebsko region), formed one of the pillars of extreme pan-Germanism.[20] The process of assimilation of the Sudeten Germans took place mainly in the form of migrations of the Czech population to create ethnically diverse areas.[21] The year 1938 became a fundamental turning point in the Czechs' view of the Sudeten Germans, especially after the events connected with the signing of the Munich Agreement. The then President Edvard Beneš, in his statement in 1942, stated, among other things, that "the word 'Sudeten', 'Sudetenland', 'Sudeťák' will forever be associated in the Czech lands with the Nazi brutality against us Czechs and democratic Germans carried out in the fatal crisis before and after 1938". Even shortly after the end of the Second World War, various measures were issued that prohibited the use of the designation Sudetenland and similar derived terms.[22] Hitler planned to take responsibility for the Germans in Czechoslovakia. He decided to proceed differently than in the case of Austria. He counted on the use of the Sudeten Germans, who were supposed to facilitate his seizure of Czechoslovakia.[23] If Germany wanted to implement its plans with Czechoslovakia, there had to be a closer German–Italian alliance. This would eliminate the possibility of intervention by France and Britain in favour of Czechoslovakia.[24] The instruction from Berlin was to submit

[17] Kural 1993.

[18] Peschka 2013.

[19] Pavlíček 2002.

[20] Sládek 2002.

[21] Krystlík 2010.

[22] Hruška 2008.

[23] Beneš–Kural 2002.

[24] Čelovský 1999.

proposals that Czechoslovakia could not fulfil, so there could not be an agreement between Czechoslovakia and Germany.[25] A typical example of conducting a hybrid war was the demand of the Sudeten German party, whose goal was the establishment of autonomous municipalities, districts and territorial administration. They should have been under the leadership of district governors, councils and committees and the administration was conducted in the language of the population.[26] Hitler's fascism was greatly strengthened by the withdrawal of the Czechoslovak borderland, especially by the economic and human potential and the weakening of the Czechoslovak army, which Hitler's generals feared.[27] A hybrid war can have different aspects, for example, economic, energy or logistical. Most coal mining, energy bases, and metallurgical and chemical industries were located in separate territories. In the region that remained in Czechoslovakia, agriculture prevailed over the industry. Germany wanted to turn the rest of Czechoslovakia into an agrarian "pendant" of the German industrial wheel. They cleverly determined the new Czechoslovak borders to cut through all the main transport links, which made economic consolidation and eventual defence against attack impossible. The state, territorially crippled in this way, was also crippled by a change in its internal structure. Fascist Germany directly interfered in internal affairs, regardless of the central government. In Munich, the Czech bourgeoisie sacrificed their nation and important positions of power. She left Slovakia to the will of the people's clero-fascists and believed that the economically weak Slovak bourgeoisie would need the cooperation of the Czech capitalists.[28] In the occupied sectors, so-called card files were lists of defendants, where it was written what status belonged to them. It was distinguished, e.g. arrest, resolve, confiscate, police surveillance, etc. The commandos were supposed to provide all the tasks performed by the state police authorities in Germany.[29] The national aspect was one of the most critical aspects of conducting a hybrid war. Most of the German population renounced Czechoslovak citizenship after the occupation of the border and the declaration of the protectorate of Bohemia and Moravia. On the one hand, this change increased their enthusiasm that the territory they lived in was annexed to Germany after many

[25] Kubů–Klimek 1995.

[26] Kural 2002.

[27] Hubenák 1998.

[28] Čapka 1998.

[29] Osterloh 2006.

years. On the other hand, accepting the citizenship of the German Empire also meant military duty. After the outbreak of war in the fall of 1939, most Sudeten men were conscripted into the German army. The border areas suddenly began to face a labour shortage, and, in addition to political issues, they also had to deal with economic and social problems.[30] Czech historians often view the displacement of the Czech population as an expulsion by the Germans and Hitler. Still, most of the Czech population fled "voluntarily" due to the loss of employment and livelihood. Moreover, the Czech population was not expelled by the German authorities but by the Sudeten German Freikorps and the Voluntary Protection Services, which Karl Hermann Frank[31] later stopped. Of course, the biggest concern was the part of the population who moved to the Sudetenland in the interwar period as part of the development of the Sudetenland. The number of old settlers who had always lived there mostly stayed in the Sudetenland. Those residents who owned property acquired through the land reform, Czech nationalists, members of the defence units, officials of the physical education association Sokol and former legionnaires also voluntarily left the Sudetenland. They were all associated with the oppression of the Sudeten Germans for the past twenty years, and they were all worried about how Hitler would react to them.[32] In addition to the controlled eviction, there was also the evacuation of the Czech intelligentsia, especially doctors, judges, officials, teachers, etc., who were heading to the interior or the villages located on the demarcation line.[33] Czechs lived in the city without any cultural and social activities. Only German films were shown in the cinemas, the same in the theatre or concerts. The success was the rescue of four thousand books from the Czech city and district library destined for liquidation. German members of the Hitler Youth group attacked Slovak pupils to prevent them from saving the books.[34] There were arrests of German anti-fascists, communists and social democrats, e.g. in Odary, Opava, Bielovci or Příbor. In the first years of the occupation, the resistance movement was mainly concentrated around the industrial centres of Novojičín and Ostrava. Deputations, petitions and even demonstrations were

[30] Gubič 1997.

[31] Karl Hermann Frank (1898–1946) was one of the highest ranking Nazis within the Protectorate of Bohemia and Moravia during the occupation of the Czech lands from March 1939 to May 1945.

[32] Zimmermann 1999.

[33] Myška 1965.

[34] Andrýsek 1963.

organised against the work in Czech areas, such as Příbor, Kopřivnice, Štramberk or Straník. In the autumn of 1938, illegal groups of Czech and German anti-fascists were formed in Kopřivnica, Štrambersko and Příborsko.[35] An exciting example of German propaganda was the change of the printed newspaper Neutitscheiner Zeitung to Deutsche Volkszeitung. The motif of liberation was visible on all sides. Everything was coloured red, and everything was decorated with portraits of Hitler and swastikas. Hands with broken shackles became an important symbol of liberation from twenty years of suffering alongside the Czechoslovakians. We would also find Germans who did not care about joining the Reich. The Head of the district court and the district judge in Bystrica pod Hostýnom wanted to stay in the rest of Czechoslovakia because they had Czech families and lived in a Czech environment, and did not know the German language. The relocated District Office in Hranice was even involved in staying in the republic. Czech cities and towns sent petitions against the German occupation, and demonstrations were held, due to which martial law was declared. While martial law was not declared in Novojičín in September, October and November 1938, this measure was taken due to Czech protests.[36] Germany built the occupation administration gradually, and its ultimate goal was to pursue a "final solution" to the Czech question. The Nazi occupation was supposed to culminate in the "Germanisation of space and people". It means the ethnic and, thus, for the most part, the physical liquidation of the Czech nation. Efforts for the intellectual liquidation of the country were already manifested after the university riots on 28 October 1939. The shooting of student Jan Opletal and the demonstration at his funeral gave the occupiers an excuse to close all universities, and Czech students lost the right to education. The tactic of dividing Czechoslovakia worked out for Hitler precisely as he planned. Since the Munich Agreement, nothing has prevented him from doing so. Questions of what would have happened if the Western powers had not accepted Hitler's game are difficult to solve today. Richard Chamberlain's policy of "saving peace at all costs" led to the demise of Czechoslovakia and the strengthening of the power of Nazi Germany.[37]

[35] Bartoš 2000.

[36] Trnčáková 2019.

[37] Kováč 1997.

## Case study: The first and second wars in Chechnya

The first and second wars in Chechnya between 1994 and 1996, respectively from 1999 to 2009, can be considered another example of conducting war in a hybrid way. The conflicting groups in the first Chechen war were Russia on one side and Chechen separatists on the other, supported by a smaller number of Islamic fighters from various Islamic countries.[38] At the time of the war, Russia and the Russian army were headed by Boris Yeltsin. On the side of Chechnya, it was mainly the then-president Dzhokhar Dudayev. But military commander Shamil Basayev also played an important role.[39] Within the framework of the first and second wars in Chechnya, specific instruments of warfare were used in a hybrid way. One of the ways can be referring to the nation's collective historical memory. Individual arguments, whether in the form of historical facts or myths, were used as a tool to approve participation in the war conflict and the mobilisation of society. On both sides of the conflict, the nation's historical memory was activated in Chechnya. For example, part of the Chechen ideology was mainly a traumatic history, full of suffering, oppression and fights with Russia for freedom, their land, and the image of Russia as a constant danger and threat.[40] The wars in Chechnya were, among other things, labelled as an information war. The victory of Chechnya in the first war was helped by its victory in the information campaign, namely that Movladi Udugov, a Chechen politician, ideologist and propagandist, created a favourable image of Chechnya. However, in the second Chechen war, Russia learned from its mistakes and used the situation in the information environment to its advantage. Chechen ideology worked with the fact that Chechens are historically, culturally, ethnically and religiously different from Russians and Russia. For centuries, they were variously oppressed, persecuted, or even liquidated by the Russians. Chechnya always had a special status during the Soviet era. This region claimed the right to self-determination and independence after the collapse of the Soviet Union. On the other hand, the Russian side considered Chechnya an integral part of its territory and did not want to give it up.[41] During the war, Chechen separatists combined the conventional way of conducting an armed struggle with the

[38] Karim 2013.

[39] Souleimanov 2012.

[40] Campana 2009.

[41] Cornell 2001.

guerrilla way of fighting. Psychological operations were carried out to sway the local population to their side and, at the same time to carry out criminal activities and terrorist attacks not only on the Chechen Autonomous Republic but especially on the rest of the territory of the Russian Federation. Many of the Chechen separatists' activities have been labelled war crimes. They have resulted in the deaths of many innocent civilians, including children, such as in the Beslan massacre in 2004.[42] In case of the first Chechen war, it is possible to observe hostile groups, the presence of leaders, a clear conflict ideology, demonstrable organisation and communication in groups, and sufficient financing of both sides of the conflict. The conflicting groups in the second Chechen war were the same as in the first, the only difference being the higher rate of involvement of groups of Islamic fighters.[43] A typical manifestation of the leadership conflict in a hybrid way is various terrorist and sabotage actions. The causes and consequences of terrorism in the post-Soviet space as the most severe non-military threat would require a unique analysis. It is a severe problem that the Russian Federation will probably have to face in the future to an increasing extent or to work closely with other states to eliminate it.[44] Terrorist acts of armed men (bandits) related to the so-called first Chechen war (terrorist acts in Budjonnovsk, Kizľar, in 1995 and 1996) had the task of transferring violence and instability beyond the borders of Chechnya. Terrorist acts in the second Chechen war (the controversial explosions of residential buildings in Moscow in 1999, which preceded the invasion of Chechnya by federal troops, the last terrorist attack on the theatre in Dubrovka in 2002, or on the school in Beslan in 2004) were in some way connected with the so-called "Chechen trail" – by persons of "Caucasian nationality" (explosion of trains on the Moscow – St. Petersburg line in 2007 or 2009). However, it is essential that in the fight against terrorism, the Russian political leadership took an uncompromising position and tried to solve the situation violently. The political solution to the Chechen conflict was also influenced by the fact that the majority of the population of Chechnya did not identify with violent (terrorist) ways of fighting nor with Islam, to which Dudayev's regime initially began to lean.[45] Within the first Chechen war framework, it is also possible to discuss the conflict due to the dispute over raw materials. In the Chechen territory, there

[42] Renfrew 2011.

[43] Wilhelmsen 2005.

[44] Souleimanov 2006.

[45] Horemuž 2010.

are relatively large reserves of oil and plants for processing this raw material, and an oil pipeline passes through there, which was already in the Chechen territory during the Soviet era. Therefore, it is possible to assume that, among other things, Russia did not want to lose the stocks of this strategically important raw material and control over the oil pipeline. Economic enrichment was present during the first Chechen war in various criminal activities, but the funds obtained from it were used to finance the conflict.[46] During the second Chechen war, the situation in the case of economic enrichment was different. Before the outbreak of the second Chechen war, individual leaders of military groups in Chechnya also competed for power. For this competition, they used financing from Islamic states and criminal activities of various natures. This financing was used in the interwar period to gain influence and power in Chechnya. Most of them were carried out in exchange for accepting Islamist ideas. This indicates that individual Chechen leaders were not only interested in the future of Chechnya (although it still played a primary role) but also for personal benefit, which is connected with economic enrichment.[47]

## Case study: The second Lebanon War

In 2006, the second war occurred in Lebanon, where Israel and Hezbollah fought against each other. This conflict was not successful on the part of Israel. The row erupted on 12 July 2006, after Hezbollah began shelling Israeli military positions and border villages in northern Israel with rocket launchers and mortars. One of the reasons the Israeli army failed to fulfil its goals was the false hope for the success of the new operational concepts and strategies associated with the revolution in military affairs. The main problem of the Israel Defense Forces, which became apparent in the war with Hezbollah, was that the Israeli army did not function as a whole.[48] In practice, it looked like the structure and equipment of the Israeli army had already been adapted to the new standards related to the revolution in military affairs. However, operationally the army still functioned based on the concepts of low-intensity conflict and limited conflict. Among other things, the fact that Hezbollah knew how to use the experience of the wars against Israel

[46] Dunlop 1998.

[47] Wilhelmsen 2005.

[48] Marcus 2015.

to counter many aspects of the new strategy, inspired by the revolution in military affairs, played an important role. Hezbollah demonstrated this approach, for example, by hiding its soldiers among the local population so that the Israeli army would not be able to identify key Hezbollah positions and neutralise them with precision-guided weapons. In addition, Hezbollah also focused on counterattacks. These consisted, for example, of guerrilla forms of attacks, asymmetric tactics, or persistent rocket attacks aimed at Israeli population zones.[49] No operational and tactical doctrine with elements of a revolution in military affairs can effectively act against an ideologically motivated and determined enemy, who uses simple but effective technologies and relies on decentralised forms of management and command. On the other hand, attributing the failure and low effectiveness of the Israeli forces in the war in Lebanon in 2006 is an oversimplified perception of reality. The Lebanon war cannot serve as empirical evidence for the new operational strategy of the Israel Defense Forces because it was not actually implemented in this conflict.[50] A typical manifestation of the hybrid war in the conflict between the Lebanese Hezbollah and Israel can be considered to be the use of, for example, the partisan way of conducting information warfare, psychological warfare, and criminal and terrorist activities. In the fight against the Israeli armed forces, the leadership of Hezbollah was able to concentrate, use and coordinate the attacks and movements of paramilitary units, criminal groups and terrorist cells, set traps and use Iranian military, financial, material and technical support. Attacks on Israeli troops were preceded by a massive information campaign aimed at Arab and Muslim communities and the world public as part of the hybrid way of conducting the battle. Photos of dead civilians, destroyed buildings, and videos showing the suffering of older men, women and children, bombed civilian homes, schools and hospitals after Israeli attacks were intended to gain sympathy for themselves and condemn Israel. Photos and videos were immediately sent to all the world's media and published on the Internet. As a result, there were reactions from many countries, which demanded an end to Israeli attacks on Lebanese territory, accused of committing war crimes, and psychological pressure was put on the leading political and military leaders of the Jewish state.

[49] Kober 2008.

[50] Adamsky 2010.

## Case study: Russian Federation cyberattack on Estonia

The large-scale and sophisticated cyber operation began on 1 May 2007, and lasted 22 days. The reason for the attack was supposed to be the relocation of a Red Army monument from the centre of Tallinn. First, the opening pages of the official websites were removed and replaced with images that defamed the Prime Minister. Several hacked websites were replaced with Russian propaganda or fake apology sites, but most attacks were aimed at shutting them down. An Estonian Ministry of Defence spokesman compared these attacks to those against the United States of America on 11 September 2001.[51] Internet communication immediately collapsed, and servers were overwhelmed. Russian-speaking residents took to the streets of the capital Tallinn. The domestic population of Estonia began to feel fear and insecurity. The attack was directed not only at press institutions but also at large commercial banks. Information systems were blocked, and Estonians of Russian origin invaded the capital's centre. Subsequently, the sale of fuel and typical food commodities was interrupted. Estonia expected the Russian Federation to send military convoys to their country. However, no alarm was declared, the border guard did not announce any interventions, and Estonian airspace was not violated. It was about operations in cyberspace. The situation was also complicated because attackers constantly improved their malicious attacks to avoid filters. It means that whoever was behind it was sophisticated, fast and intelligent.[52] At the time of the attack, about 98% of the territory of Estonia was covered by the Internet, two-thirds of the population used the Internet daily, and more than 95% of banking operations were conducted electronically.[53] The only possible defence was to cut the Internet connection between Estonia and the rest of the world. The main goal of the attack was to destabilise society in Estonia. A Botnet network was used in the attack. This technique, working on the principle of the Trojan horse, makes it possible to carry out attackers' commands directed at tens of thousands of computers, control them remotely and conduct massive attacks. It was necessary to ensure the protection of the media. Without access to information, people are unable to understand individual contexts. The cyberattacks on the Estonian Government are considered the first-ever case of

[51] The Economist 2007.

[52] Raboin 2007.

[53] Centre of Excellence – Defence Against Terrorism Ankara 2008.

cyber warfare. As it was a politically motivated and highly coordinated attack on the government of a sovereign state by another state, the definition of cyber terrorism, in this case, is no longer sufficient.[54]

## Case study: The war in Georgia

The war in Georgia began on 1 August 2008, when Georgian troops started shelling Tskhinvali – the capital of the separatist region South Ossetia, including residential areas – with mortars, grenade launchers and small arms. The first people died, the first material damage occurred, and as Georgia continued to concentrate and deploy its forces on the borders of South Ossetia, the evacuation of civilians to North Ossetia began.[55] On 7 August, units of the Georgian armed forces shelled Tskhinvali and other Ossetian cities again. The war finally broke out in full on 8 August 2008, the opening day of the 29th Summer Olympics in Beijing. Georgia surprisingly attacked South Ossetia after signing a ceasefire, surrounded its capital and launched a massive offensive. They also attacked the Russian barracks and killed ten Russian soldiers during the attack. Russia requested an extraordinary session of the UN Security Council. After Georgian troops continued to attack Tskhinvali and other Ossetian cities by land and air, the South Ossetian Parliament asked Russia for help. This launched a counter-offensive a few hours later by units of the 58th Army, which radically changed the balance of forces on the battlefield. After the expulsion of Georgian troops from South Ossetia, Russian military units continued to attack Georgian armed forces, military facilities, warehouses, bases and command posts and advance through Georgian territory. They stopped 55 km from Tbilisi when Russian President Dmitry Medvedev ordered them to end military operations in Georgia.[56] Both sides of the armed conflict waged an intense information war, which made it difficult to separate the facts from the deliberately spread misinformation. In addition to Moscow and Tbilisi accusing each other of killing civilians and creating a humanitarian disaster, Moscow blamed Georgia for unleashing the bloodshed and likened its actions in South Ossetia to genocide. In contrast, Georgian President Mikheil Saakashvili accused Russia of trying to subjugate

[54] Tisdall 2010.

[55] Kyselová 2008.

[56] Ivančík 2016.

his country. Later, a report (commissioned by the European Union) was drawn up by a team led by Swiss diplomat Heidi Tagliavini directly stating that there was a massive Georgian sniper and artillery attack on the city of Tskhinvali on the night of 7–8 August 2008. This was considered the beginning of the state of war.[57] Three years later, the Prime Minister of Georgia, Bidzina Ivanishvili, also accused President Saakashvili and his supporters of being responsible for starting the war with Russia in 2008. The independent Georgian commission of inquiry reached the same conclusion, which dealt with the causes and consequences of escalating the situation in the Caucasus in 2008.[58] On the other hand, Russia was criticised by several parties and by several prominent politicians for the entry of Russian troops into the territory of Georgia. In the report above, the European Union accused Moscow of provocations and his disproportionate reaction to the attack on Russian soldiers. Three main themes dominated the information war:

- Georgia and especially its President Saakashvili were the aggressors
- Russia was forced to intervene to defend its citizens and prevent a humanitarian catastrophe
- The West has no legitimate reason to criticise Russia because Russia only did what the West did in 1999 in Serbia and Kosovo

In parallel with the information war against Georgia, cyber warfare also occurred. Several prominent Georgian websites were hacked and altered, including those of the Georgian President, the Ministry of Foreign Affairs, the National Bank, the Parliament and the Supreme Court. These cyberattacks were centrally directed and coordinated. In addition, Russian airborne troops and special purpose forces played an important role.

### Case study: Cyberattacks on Iran's nuclear facilities

Cyberattacks also often affect such areas as the energy industry and the supply of network services and utilities in general (heat, water, etc.). An attacker or their group tries to gain access to crucial information or infrastructure elements (power plants, distribution systems, control centres) to control them or upload malicious code into them that will execute specific commands. This is helped by

[57] Euractiv 2009.

[58] Hlavné Správy 2012.

the fact that, at present, there is almost no complex energy or network system that would be managed without the use of information technology.[59] One example of a cyberattack on an energy facility is the attack on a uranium enrichment plant in 2010. This attack aimed to delay or completely stop the start-up of a nuclear power plant in Iran. From the point of view of cyber warfare, the most significant is the Stuxnet worm, also called the "father of cyber weapons".[60] This specific form of hybrid warfare aimed to disable and destroy several hundred uranium enrichment centrifuges by altering their rotational frequency. First, they spun above the permitted limit and then slowed down to an extended speed. This caused their collapse, financial losses and delays in commissioning the power plant itself. Given the architectural complexity of Stuxnet, it is very likely that its authors were experts with substantial financial potential. For this reason, the USA and Israel were suspected of the attack.[61] The capabilities of this worm were such that it is considered the most expensive and challenging project in the history of malware to date. Stuxnet reportedly contained security certificates stolen from legitimate software companies, used several zero-day vulnerabilities, and was able to spread both over a computer network and via a USB device. The initial infection is believed to have originated from an employee or supplier's USB drive. The attack itself had three phases. In the first phase, the infected worm targeted the MS Windows OS. In the second phase, it infiltrated the Windows-based Siemens Step7 software, which he further compromised and gained access to the PLC (programmable logic automaton) controlling the uranium enrichment centrifuges, which also became infected. In the final phase, Stuxnet used two techniques to self-destruct the centrifuges. First, there was an adjustment of the frequency of change of spins of centrifuges above and below safe operating values. Subsequently, it caused over pressurisation of the centrifuge and thus an increased load on the rotor. Stuxnet was also able to hide its presence both because it had control over communication with the PLC and also through the use of rootkit functions. In one year, Stuxnet is believed to have damaged a fifth of the centrifuges at Natanz and contributed to the slowdown of Iran's nuclear program.[62]

[59] Beránek–Dvořák 2016.

[60] Langner 2013.

[61] Zetter 2011.

[62] Ivezic 2018.

## Case study: The war in Libya

The causes of conflict are identical to the objects of mutual incompatibility, that is, the publicly declared incompatible interests of the primary actors involved. We can register the split of opinion and attraction between the parties involved on several levels, namely political, ideological, religious and economic. In the political dimension, understanding the incompatibility of interests is relatively simple. The decentralisation of political power and the absence of a central, generally acceptable government represented an opportunity for several militarily significant and influential actors to try to legislate their political agenda and thus become a dominant actor in post-revolutionary Libya.[63] The revolutionary public sentiment that began to spread across the Middle East also hit Libya on 15 February 2011, when security forces in Benghazi arrested prominent lawyer Fathi Terbil, representing the families of more than 1,000 prisoners killed by security forces during the Abu Salim prison riot in 1996. After being released on the same day, Terbil set up a web camera in Benghazi's main square to film families protesting his arrest. Security forces intervened and suppressed the protests. The video quickly spread across the Internet. This demonstration occurred two days before the so-called "day of anger" planned by youth groups via Facebook and Twitter for 17 February 2011. The protests, concentrated in the eastern part of Libya, centred on Benghazi, soon spread to other cities. By 21 February 2011, almost all of Libya, fuelled by the regime's brutal response, which also brought casualties and was marked by panic, was in revolt. By the end of the month, the insurgents (although organisationally incompetent) imposed control over the eastern half of the country. But Muammar Gaddafi made it clear that he was ready to fight. In early March, forces loyal to the leader began successfully attacking cities and oil facilities in the east of the country to regain lost territory.[64] The insurgents suffered thousands of casualties but were able to seize and control several cities, including Benghazi. The rebels and volunteers could continue to the port of Cyrenaica. These troops were undisciplined, poorly trained and confused; they controlled less than one-third of the territory and even less of the natural resources. An incredible number of rivalries emerged between the self-proclaimed members of the transitional council.[65] The specific reason

[63] Gartenstein-Ross – Barr 2015.

[64] Bix 2011.

[65] Cordesman et al. 2011.

for conducting a hybrid war in Libya was, of course, also an economic interest. Libya currently has an oil wealth of more than 48 billion barrels of oil. Control of oil fields and elements of the oil infrastructure is therefore desirable for all the essential actors of the civil war. This was also reflected in the dynamics of the conflict since locations rich in oil or necessary in the context of its transportation or processing are the places of the most frequent and intense armed clashes.[66]

## Case study: Russia's annexation of Crimea

Having learned from the conflict with Georgia, Russia used a wide range of military (symmetric and asymmetric), political, economic, information, propaganda, diplomatic and cyber means of warfare during the successful annexation of Crimea in the spring of 2014. By Gerasimov's concept of a hybrid war, it turned out that Moscow was not about eliminating the enemy but dominating him. The use of conventional military force has become almost useless. Controlling the minds of the Crimean population, soldiers, sailors and members of other armed forces resulted in them betraying their state and supporting the aggressor under the informational and psychological influence (pressure). By doing so, they enabled Russia to achieve the set goal.[67] The operation took place according to the prepared scenario. After the transfer of well-armed, equipped and trained personnel, critical administrative buildings, offices, airports and military bases were quickly occupied. A supply of destabilising civilian groups was ensured to provoke discontent among the local population. Special forces, intelligence services and members of private security agencies with experience in Transnistria, Chechnya and Bosnia and Herzegovina were deployed. At the same time, informational and psychological warfare continued, focusing on the elimination of places of resistance.[68] Ukraine was not at all prepared for such a situation. Its new political leadership was incapable of taking decisions adequate to the problem and issuing meaningful orders to the state's armed forces. Due to the absence of orders from the highest representatives of the country, their command was unable to manage, organise and certainly not coordinate the activities of individual armed and security forces and take effective and efficient

[66] *OPEC Share of the World Crude Oil Reserves* 2017.

[67] Bērziņš 2014.

[68] Beskid 2014.

countermeasures to prevent the annexation of the peninsula. The problem also consisted of the Ukrainian army and the security troops being underfunded, insufficiently armed, equipped and supplied for a long time. Low levels of preparedness and training, with little or no experience in combat operations, resulted in low levels of loyalty to the government.[69] In case of the annexation of Crimea and the conflict in Southeastern Ukraine, unlike the Russian–Georgian war in 2008, all methods of conducting a hybrid war, both military and non-military, have already been fully demonstrated. Russia and its supported separatists can deploy many troops and military equipment into the conflict within the military dimension. According to the U.S. Department of Defense, in November 2014, Russia had 7,000 soldiers in Ukraine (not including Crimea). More than 40,000 of them have been deployed in Ukraine, which Russia denies. On the contrary, it accuses the United States and NATO countries of helping the Ukrainian armed forces, both regular and irregular, through advisers from the armed forces, special forces and intelligence services and private military and security companies financed by them. Russia and Russian organisations, on the other hand, actively support (logistically, materially and personally) the separatists, who represent a combination of the local population, citizens of Russia and other countries of the former Soviet Union, including several volunteers from Slovakia, the Czech Republic and other European countries. Within the non-military dimension, it is necessary to point out the use of diplomatic, economic, informational, cyber and humanitarian tools. For example, Russian diplomacy strives on the ground of world organisations to defend its activities and weaken Kyiv's position, mainly by promoting the federalisation of Ukraine. Among the economic instruments, it especially concerns the manipulation of the price of imported Russian natural gas and restrictive non-tariff measures on Ukrainian food products. Sanctions in the form of a ban on importing various types of food and goods to Russia or using Russian airspace by Ukrainian airlines are also unpleasant for the Ukrainian economy. Russia also uses the so-called new propaganda, which does not aim to convince the recipient of the information, but mainly to make him uncertain about what is true and what is not and what can be believed. To maintain the support of the domestic population, Russia uses a wide range of media, especially state television, which, with its coverage of Ukraine, can significantly influence not only trained but also Ukrainian public opinion. An essential role in this area is also played by paid internet bloggers, who contribute to discussions on domestic

[69] Jones 2014.

and foreign websites expressing support for Russian activities and questioning anti-Russian views and actions. As part of the use of cyber tools, several cyberattacks on websites and systems of Ukrainian state institutions, transport networks, websites of volunteer battalions, and cyberattacks using malware or spyware can be mentioned. Within the framework of non-military instruments, we cannot forget the supply of food, medicines, material and equipment through humanitarian convoys from Russia and the fulfilment of other tasks under the guise of humanitarian activities.[70] The conflict in Ukraine has shown that some key battles may take place in cyberspace or the communications sphere rather than on land, sea or air. This conflict is an example of an operation in which the use of conventional forces was minimised. Throughout the conflict, Russia used the possibilities offered by modern technology and media. This led to the mobilisation of his supporters, the demonisation of his enemies and the enemy government's demoralisation.[71] In this context, we can talk about the so-called information war, which represents a set of activities, often mutually coordinated in terms of goal, place and time. They extract, disable, change, damage or destroy the information or its resources. This makes achieving advantages in combat or victory over a specific opponent. Thus, through informational and psychological influence, Russia managed to influence the minds of the Crimean population, military and other armed forces, who subsequently switched to Russia's side and thus helped the annexation of Crimea.[72]

## Results and discussion

The paper's primary goal is to analyse selected cases of international political and social events and their subsequent application to the concept of hybrid threats. The content of the methodology is the analysis and comparison of selected forms of hybrid threats through case studies. An evaluation table of these case studies was created to analyse selected forms of hybrid threats through case studies, followed by their comparison (Table 1). The columns contain chosen case studies, and the rows represent the criteria – selected characteristics of individual

[70] Ivančík 2016.

[71] Lange-Ionathamischvili – Svetoka 2015.

[72] Unwala–Ghori 2016.

case studies. The desired characteristics are the different types and forms of means used for the conduct of hybrid warfare.

*Table 1: Evaluation table of selected case studies*

| **Criteria – Case Studies** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| Military means | Yes | Yes | Yes | No | Yes | No | Yes | Yes |
| Political means | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Economic means | Yes | Yes | Yes | No | No | No | No | Yes |
| Information resources | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Cyber means | No | No | No | Yes | Yes | Yes | Yes | Yes |
| Propaganda means | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Diplomatic means | No | No | No | No | No | No | No | Yes |
| Psychological means | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Terrorist means | No | Yes | Yes | No | No | No | No | No |
| Media resources | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| Controlling the minds of the population | No | No | Yes | Yes | No | No | Yes | Yes |
| Destabilising units | No | No | Yes | No | Yes | No | No | Yes |
| Protest potential of the population | Yes | Yes | Yes | Yes | No | No | Yes | Yes |

*Source:* Compiled by the author

The evaluation table of selected case studies was processed through comparison. The assessment of the case studies was carried out primarily based on selected professional literature from various authors dealing with the issue of hybrid threats, including consultations with specialists and experts from institutions dealing with the issue of hybrid threats, such as the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš, the Academy of the Police Force in Bratislava, the General Tadeusz Kościuszko Military University of Land Forces in Wroclaw and the Occupational Safety Research Institute in Prague. The selection and formulation of evaluation criteria, or characteristics of individual case studies, were influenced by several facts. The evaluation criteria were designed to consider the structure and nature of hybrid threats in the past with practical application to the current global security environment. All the mentioned case studies have a different nature of the action of various forms of hybrid threats. Each selected case study has its specific position, principles and environment in which the participants used the mixed threat factors. Hybrid warfare is not a new type of warfare but a form that has been present since the beginning of written history. The combination of regular and irregular military forces and other measures aimed at destabilising the adversary is not new. However, about hybrid warfare in the past, the critical dimension today is to achieve dominance in the information domain. The importance of acquiring information dominance is visible in the analysed hybrid war examples (Lebanon, Crimea). The use of propaganda-psychological warfare in combination with intelligence operations and other types of coercion is aimed at destabilising society and facilitating external intervention to gain control over it. An essential means and characteristic feature of conducting a hybrid war is the use of the population's protest potential (dominant in the conflicts of the Arab Spring, Estonia and Ukraine). When discussing defence against hybrid threats, the role of external factors (NATO, EU) is often emphasised. However, suppose the attacked society, nation, or state cannot face the first attack. In that case, the external assistance could be delayed or fail if the attacking party achieves the desired goals with quick actions. This means that the first line of defence is the preservation of the social cohesion of the attacked community (example of Chechnya). The state's resistance to hybrid combat will be maintained and built. In hybrid warfare, the aggressor seeks to quickly achieve victory in situations where he is unprepared or unable to launch a conventional military attack. Suppose the attacked state can successfully counter the first attack. In that case, the aggressor is faced with withdrawing or further escalating the crisis by conducting direct military intervention (a situation sought to be avoided by using hybrid warfare). Even if the aggressor succeeds, maintaining long-term social cohesion in the attacked state creates an opportunity to negate the aggressor's success. National identity is crucial for maintaining social cohesion.

## Conclusion

States have power structures that manage available resources in peace. These structures aggregate various military headquarters, facilities and organisations created for filling, training and arming military units. The tactical level mainly uses standardised forms, but they are different from the structures built in times of war and other crises. The military system includes regular and active units, reserves and militias. Some elements even cooperate with irregular forces. Analysing new threats and preparing to act against them is essential to ensure security. However, in case of hybrid threats, this process is complex. The hybrid adversary is fast-changing, flexible and adaptable. This contribution had the ambition to clarify its structure to understand its possible action better. However, it is necessary to realise that its structure is extensive and diverse. The activities of the individual components can be managed from one coordination centre to achieve the maximum synergistic effect, or the individual elements are independent, and each pursues its interest. When creating enemy forces of a hybrid nature for the needs of military exercises, it is, therefore, necessary to simulate the complexity of individual actors in the operational environment, determine their mutual relationships and create combat formations in which they will operate on unique battlefields. Hybrid threats are a new type of threat in the global security environment. For the effective elimination of hybrid threats, it is necessary to prepare the security forces of the state focused on these threats. Preparation should include the implementation of interdepartmental and military exercises aimed at the decision-making process, command and control systems, and tactical activities. For the practices to be as similar as possible to reality, it is necessary to focus primarily on creating the structure and combat formations of hybrid threats. Training units before deployment into an operational environment requires a different approach than in the past. Teams must be prepared to carry out a full range of operations in the face of a wide range of possible threats and, simultaneously, be ready to face third parties whose interests may differ. None of the hybrid threats is purely military. The above analysis of the content of the training aid can be an inspiration for the future training of units of the Slovak Armed Forces. Even though the concept of hybrid wars has undergone a complex development since its beginnings, numerous conferences, workshops, round tables and publications, we cannot say that it has reached clear limits. We cannot precisely characterise this type of war, what else belongs to it and what does not. It is documented by several definitions, which are empirical, and almost every conflict, whether state or non-state, can be included in this type of war. Instead, the concept is associated with the complex action of various actors, with the problematic use of military and non-military tools, which are aimed not only at the state's military power, or the North Atlantic Alliance but at the whole society. The presented structure of hybrid threats serves primarily as a training aid. The threat must be an uncooperative adversary, able to screen all the capabilities and critical tasks necessary for success. However, it must be tailored to the specific requirements of particular training. In most cases, however, in addition to creating the structure itself, it is also necessary to develop the battle's organisation and the units' assignment to tasks and activities. Various tools and means for modelling and simulating hybrid threats or their secondary consequences also serve this purpose. Their primary goal is to facilitate the work of commanders in making decisions from the point of view of the offered options, even if the commander himself must make the final decision. It is advantageous to use this possibility either during the preparation and planning of operations or only during exercises for real situations at different levels and types of command.

## Questions

1. What significance did the personality of Tomáš Garrigue Masaryk have in connection with the independence of Czechoslovakia?
2. What terrorist and sabotage actions took place during the first and second Chechen war?
3. Describe the main problem of the Israel Defense Forces during the second Lebanon war.
4. Describe the three main themes that dominated the information war in Georgia in 2008.
5. In which case studies has protest potential of the population not been used as part of the tools of hybrid warfare?

## References

ADAMSKY, Dmitry (2010): *The Culture of Military Innovation. The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford: Stanford University Press.

ANDRÝSEK, Rudolf (1963): Nový Jičín za německé okupace (10. 10. 1938 – 6. 5. 1945). In OTTO, Karel et al. (eds.): *Čtení o Novém Jičíně. Soubor statí a vzpomínek k oslavám 650 let Nového Jičína.* Nový Jičín.

BARTOŠ, Jozef (2000): Odpor a odboj ve vládním obvodu Opava 1938–1945. In RADVANOVSKÝ, Zdeněk (ed.): *Historie okupovaného pohraničí 1938–1945.* Ústí nad Labem: Univerzita J. E. Purkyně, 157–175.

BENEŠ, Zdeněk – KURAL, Václav (2002): *Rozumět dějinám: vývoj česko-německých vztahů na našem území v letech 1848–1948.* Praha: Gallery.

BERÁNEK, Michal – DVOŘÁK, David (2016): Kybernetické útoky v energetice. *IT Systems,* (9). Online: https://www.systemonline.cz/it-security/kyberneticke-utoky-v-energetice.htm?mobilelayout=false

Bērziņš, Jānis (2014): *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.* Online: https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Beskid, Jan (2014): Vojna novej generácie realizovaná na Kryme. In *Národná a medzinárodná bezpečnosť 2014 – zborník vedeckých a odborných prác.* Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

Bix, Herbert P. (2011): The North African – Middle East Uprisings from Tunisia to Libya. *The Massachusetts Review,* 52(2), 329–347.

Campana, Aurélie (2009): Collective Memory and Violence: The Use of Myths in the Chechen Separatist Ideology, 1991–1994. *Journal of Muslim Minority Affairs,* 29(1), 43–56. Online: https://doi.org/10.1080/13602000902726756

Čapka, František (1998): *Dokumenty a materiály k národním dejinám 1918–1945.* Brno: Masarykova Univerzita.

Čelovský, Boris (1999): *Mnichovská dohoda, 1938.* Praha: Tilia.

Centre of Excellence – Defence Against Terrorism Ankara (2008): *Responses to Cyber Terrorism.* Amsterdam: IOS Press. Online: http://public.eblib.com/choice/publicfullrecord.aspx?p=334204

Cordesman, Anthony H. et al. (2011): Symposium: The Arab Uprisings and U.S. Policy. *Middle East Policy,* 18(2), 1–28.

Cornell, Svante E. (2001): *Small Nations and Great Powers. A Study of Ethnopolitical Conflict in the Caucasus.* London: Routledge.

Creswell, John W. – Poth, Cheryl N. (2013): *Qualitative Inquiry and Research Design. Choosing Among Five Approaches.* Los Angeles: SAGE.

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

Dunlop, John B. (1998): *Russia Confronts Chechnya. Roots of a Separatist Conflict.* Cambridge: Cambridge University Press.

Euractiv (2009): Správa EÚ: Rusko je víťaz, Gruzínsko agresor. *Euractiv,* 1 October 2009. Online: http://www.euractiv.sk/obrana-a-bezpecnost/clanok/sprava-eu-rusko-je-vitazgruzinsko-agresor-013720

Gartenstein-Ross, Daveed – Barr, Nathaniel (2015): *Dignity and Dawn. Libya's Escalating Civil War.* The Hague: ICCT.

Glenn, Russell W. (2009): Thoughts on "Hybrid" Conflict. *Small Wars Journal,* 2 March 2009. Online: http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf?q=mag/docs-temp/188-glenn.pdf

Gubič, Otto (1997): *Jasné slovo o minulosti: česko-německé vztahy – fašismus a antifašismus na Karlovarsku 1933–1945.* Karlovy Vary: Okresní Výbor Českého Svazu Bojovníků za Svobodu.

Hendl, Jan (2005): *Kvalitativní výzkum. Základní metody a aplikace.* Praha: Portál.

Hendl, Jan (2016): *Kvalitativní výzkum. Základní metody a aplikace. 4., prepracované a rozšírené vydanie.* Praha: Portál.

Hlavné Správy (2012): Budúci premiér Gruzínska: Za vojnu s Ruskom je vinný prezident. *Hlavné Správy,* 25 October 2012. Online: http://www.hlavnespravy.sk/ivanisvili-saakasvili-a-jeho-ludia-suzodpovedni-za-patdnovu-vojnu-s-ruskom/40917

Horemuž, Martin (2010): Bezpečnostná politika Ruskej federácie z pohľadu geopolitiky. *Medzinárodné vzt'ahy (Journal of International Relations),* 8(2), 115–130.

Hruška, Emil (2008): *Sudetoněmecké kapitoly.* Praha: BMSS-Start.

Hubenák, Ladislav (1998): *Slovenské a československé dejiny štátu a práva v rokoch 1918–1945.* Banská Bystrica: Univerzita Mateja Bela.

Ishikawa, Akira – Tsujimoto, Atsushi (2006): *Risk and Crisis Management.* Singapore: Shumpusha Publishing.

Ivančík, Radoslav (2016): Hybridná vojna – vojna 21. storočia. *Kultura Bezpieczeństwa. Nauka–Praktyka–Refleksje,* (22), 205–239. Online: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ceon.element-2157653d-6c10-39e2-9e75-5c3fa98fe5c3/c/pdf-01.3001.0012.2654.pdf

Ivezic, Marin (2018): *Stuxnet: The Father of Cyber-Kinetic Weapons: While Stuxnet Is Gone, the World Now Knows What Can Be Accomplished Through Cyber-Kinetic Attacks.* Online: https://www.csoonline.com/article/3250248/stuxnet-the-fatherof-cyber-kinetic-weapons.html

Jones, Sam (2014): Ukraine: Russia's New Art of War. *Financial Times,* 28 August 2014. Online: https://www.ft.com/content/ea5e82fa-2e0c-11e4-b760-00144feabdc0

Jurčák, V. – Turac, Jan (2018.): *Hybridné vojny – výzva pre NATO. Bezpečnostné fórum 2018.* Banská Bystrica: Interpolis.

Karim, Moch Faisal (2013): How Ethnic Civil War Transforms into Religious Civil War: Evidence from Chechnya. *CEU Political Science Journal,* 8(1), 54–78.

Kober, Avi (2008): The Israel Defense Forces in the Second Lebanon War: Why the Poor Performance? *Journal of Strategic Studies,* 31(1), 3–40. Online: https://doi.org/10.1080/01402390701785211

Kováč, Dušan (1997): *Dejiny Československa.* Bratislava: Academic Electronic Press.

Krystlík, Tomáš (2010): *Zamlčené dějiny 2.* Praha: Alfa Nakladatelství.

Kubů, Eduard – Klimek, Antonín (1995): *Československá zahraniční politika 1918–1938: kapitoly z dějin mezinárodních vztahů.* Praha: ISE.

Kural, Václav (1993): *Konflikt místo společenství? Češi a Němci v Československém státě (1918–1938).* Praha: Nakladatelství.

Kural, Václav (2002): *Češi, Němci a mnichovská křižovatka.* Praha: Karolinum.

Kyselová, Marianna (2008): *Ruská invaze do Gruzie.* Online: http://www.epolis.cz/clanek/ruska-invaze-do-gruzie.html

Lange-Ionathamischvili, Elina – Svetoka, Sanda (2015): Strategic Communications and Social Media in the Russia Ukraine Conflict. In Geers, Kenneth (ed.): *Cyber War in Perspective. Russian Aggression against Ukraine.* Tallinn: NATO CCD COE Publications. Online: https://www.caleaeuropeana.ro/wp-content/uploads/2015/12/cyberwarinperspective_lange_svetoka_121.pdf

Langner, Ralph (2013): Stuxnet's Secret Twin. *Foreign Policy,* 19 November 2013. Online: http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack

Marcus, Raphael D. (2015): The Israeli Revolution in Military Affairs and the Road to the 2006 Lebanon War. In Collins, Jeffrey – Futter, Andrew (eds.): *Reassessing the Revolution in Military Affairs. Transformation, Evolution and Lessons Learnt.* London: Palgrave Macmillan, 92–111. Online: https://doi.org/10.1057/9781137513762_6

Marinov, Ivo (2011): *NATO Crisis Management.* National Defence Academy, Operational Art Department. Online: https://docplayer.net/24781706-Nato-crisis-management.html

Myška, Milan (1965): Novojičínsko od Mnichova k 15. březnu. In Král, Jaroslav et al. (eds.): *Mnichov není jen historie. Sborník materiálů z ideologické konference OV KSČ v Novém Jičíně k 25. výročí Mnichova dne 9. října 1963.* Nový Jičín.

NATO (2022): *Crisis Management.* Online: http://www.nato.int/cps/en/natolive/topics_49192.htm

*OPEC Share of the World Crude Oil Reserves* (2017). Online: https://www.opec.org/opec_web/en/data_graphs/330.htm?fbclid=IwAR2zQsMTteWDrJknXVsIPpJ_bjBijYF5OMW_ZA_jwypLYsl1yf-JbWMSTiM

Osterloh, Jörg (2006): *Nationalsozialistische Judenverfolgung im Reichsgau Sudetenland 1938–1945.* Mnichov: Collegium Carolinum.

Pavlíček, Václav (2002): *O české státnosti: úvahy a polemiky.* Praha: Karolinum.

Peschka Otto (2013): *Jak to bylo doopravdy mezi Čechy a Němci: o Češích, Němcích a jiných tématech na pozadí memoárů člena smíšené rodiny, který pochází ze Sudet.* Ústí nad Labem: Paprsky.

Raboin, Bradley (2011): Corresponding Evolution: International Law and the Emergence of Cyber Warfare. *Journal of the National Association of Administrative Law Judiciary,* 31(2), 602–668.

Renfrew, Barry (2011): *Chechnya.* Online: http://www.crimesofwar.org/a-z-guide/chechnya/

Rohlfing, Ingo (2010): *Methodologies of Case Studies.* ECPR Summer School on Methods and Techniques. Online: https://www.uni-bamberg.de/fileadmin/bagsb/externe_Seminare/rohlfing-case-study-research-2014-ecpr-ssmt.pdf

Rubin, Allen – Babbie, Earl (2001): *Researchmethods for Social Work.* Belmont: Brooks/Cole.

Sanseverino-Godfrin, Valérie (2016): The Problems of the Late Implementation of the Legal Prevention Measures for Flood Risk. *Flood Risk 2016 – 3rd European Conference on Flood Risk Management,* 7, 1–11. Online: https://doi.org/10.1051/e3sconf/20160713010

Šimák, Ladislav (2016): *Krízový manažment vo verejnej správe. Druhé prepracované vydanie.* Žilina: EDIS.

Sládek, Milan (2002): *Němci v Čechách.* Praha: Pragma.

Souleimanov, Emil (2006): *Terorismus ve světle geneze ideologie a technologie asymetrických konflikt.* In Souleimanov, Emil (ed.): *Terorismus. Válka proti státu.* Praha: Eurolex Bohemia, 13–63.

Souleimanov, Emil (2012): *Konflikt v Čečensku: Minulost, současnost, perspektivy.* Praha: SLON.

The Economist (2007): A Cyber-riot. *The Economist,* 10 May 2007. Online: http://www.economist.com/node/9163598

Tisdall, Simon (2010): Cyber-warfare 'Is Growing Threat'. *The Guardian,* 3 February 2010. Online: https://www.theguardian.com/technology/2010/feb/03/cyber-warfare-growing-threat

Trnčáková, Adriana (2019): *Novojičínsko v době zářijové krize roku 1938.* Brno: Masarykova univerzita, bakalářská diplomová práce.

Unwala, Azhar – Ghori, Shaheen (2016): Brandishing the Cybered Bear: Information War and the Russia–Ukraine Conflict. *Military Cyber Affairs,* 1(1), 1–11. Online: https://doi.org/10.5038/2378-0789.1.1.1001

Wilhelmsen, Julie (2005): Between a Rock and a Hard Place: The Islamisation of the Chechen Separatist Movement. *Europe–Asia Studies,* 57(1), 35–59. Online: https://doi.org/10.1080/0966813052000314101

Yin, Robert K. (2009): *Case Study Research. Design and Methods.* London: SAGE.

Zetter, Kim (2011): How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *Wired,* 11 July 2011. Online: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zimmermann, Volker (1999): *Die Sudetendeutschen im NS-Staat: Politik und Stimmung der Bevölkerung im Reichsgau Sudetenland (1938–1945).* Essen: Klartext.

Éva Jakusné Harnos – Péter Bányász[1]

# Social Media: An Instrument of Public Diplomacy and a Weapon of Psychological Operations

Social media provides opportunity for citizen participation in democratic deliberation because it allows an exchange of opinions and information without the intervention of editors and opinion leaders. Nevertheless, it can also be used as a weapon in psychological operations because it can hide the source of misleading information and merge into the online discourse without the target audience realising it. This chapter examines two major areas of impact of the social media. On the one hand, it can be an instrument of including citizens in a new form of public diplomacy called peer-to-peer diplomacy. The first part of the chapter summarises the role of modern media in shaping political opinion in a transparent way. In addition, it highlights the theoretical background to its impact, then introduces a case of the successful application of social media for promoting a country. In contrast to this, the second part of the chapter explains why and how social media becomes a weapon in psychological operations. It draws attention to the total surveillance and isolation which the social media technologically allows. It takes its examples from recent events: among others, from the Russia–Ukraine war.

## Introduction: The development of the modern media

Since the evolution of mass media, that is, the appearance of the news industry with the institutionalisation of news production and mass news consumption from printed newspapers in the late 19th century, scholars have been researching its impact on societies. Technological advancement has resulted in other forms of media, such as radio, television, satellite broadcast, and, in our time, the Internet and social media platforms. Contemporary researchers distinguish conventional

[1] Ludovika University of Public Service.

DOI: https://doi.org/10.36250/01237_12

media (print newspapers, radio, television) from digital media (the Internet and social media platforms). The major distinguishing features are the production of content and the degree of interaction between the content providers and the content consumers. From these aspects, conventional media is often described as comprising top-down processes in which small privileged groups of journalists and media workers create content for the public in close cooperation with, and, in fact, under the control of the elite.[2] In this context the gatekeepers (for instance, the editors) filter information and decide on publication dependent on the dominant ideology and values of the given society. Apart from gatekeepers,[3] institutions (boards) may be functioning in order to control the flow of information to the public and the legal and ethical standards of news reporting. Contrary to this vertical model, the digital media is usually seen as a horizontal, more decentralised model, in which many provide content for many, mostly free of the strict control of institutions, gatekeepers, boards and regulations. The digital media could lead to new forms of citizen participation; however, it poses some dangers that will be discussed later. As mentioned above, the methodology of analysing the content and assessing the impact of mass media communication started to evolve since its appearance.[4] In the early phase of research, the Direct Flow Theory was formulated and it was believed that mass media content had a direct effect on every individual who was exposed to it. In the 1950s, the Theory of Two-Step Flow was developed by Katz and Lazarsfeld.[5] The novelty of this theory was the inclusion of interpersonal relationships in its model of political communication because it attributed relevance to personal contacts in spreading and recycling information broadcast as well as the creation of individual engagement. Thus, the definition and the role of opinion leaders was regarded slightly different: they were viewed as members of the small, interconnected networks which constitute society. The Two-Step Flow Theory was later further developed into the Multistep Flow Theory.[6] In the Internet Age, due to technological disruptions, network studies have come under spotlight again, which underpins the significance of the Two-Step, and of the Multistep Flow Theories.

[2] Van Dijk 1988.

[3] Shoemaker 2016.

[4] Lazarsfeld et al. 1944; Berelson 1952; Van Dijk 1988; Krippendorff 2004; Fairclough–Fairclough 2012; Neuendorf 2017.

[5] Southwell 2016.

[6] Katz 1987; Brosius–Weimann 1996.

## Modern media and public diplomacy

The media assumed powerful roles from the beginning, two of which are especially important from the perspective of politics and international relations. First, it was soon recognised by political elites as an essential tool for establishing a link between themselves and their constituents. Thus, media campaigns and agenda setting were exploited as early as the late 19th century.[7] Second, it was understood that the information disseminated by the media shaped the perception of the facts and events of the world by the audience.[8] Consequently, media became an effective means of foreign policy for agenda-setting, constructing shared knowledge, shaping beliefs and public attitudes.[9] Constructivism in international relations research actually holds that global political discourse, mostly disseminated by the media, plays a decisive part in forging, strengthening or weakening international ties.[10] Models of communication for the media are mostly founded on interpersonal oral communication,[11] which reflects the evolution of human language, writing and society. This also explains why human networks play a crucial role in conveying information. The efficiency of combining technological and human networks has been the basis of the development of an innovative form of public diplomacy: peer-to-peer diplomacy. The term "public diplomacy" is relatively new: it was created in 1965 and became widely used after the end of the Cold War.[12] However, taking into consideration that it involves the dissemination of state-sponsored news favourable to the objectives of the stakeholder, the practice is as old as history. The five major areas of public diplomacy are listening, advocacy, cultural diplomacy, exchange diplomacy and international broadcasting.[13] The latter underscores the importance of news production, even though much of it seems to be out of state control in the era of social media. Before the discussion of new forms of public diplomacy, its possible connections with persuasion and propaganda need to be clarified. Due to the fact that the term 'propaganda' was discredited in two world wars, during the Cold War ideological struggle and in

[7] Hampton 2010.

[8] Gerbner 1985; Philo 2010.

[9] Seib 2010.

[10] Wendt 1999; Hurd 2008.

[11] McQuail–Windahl 1993.

[12] Cull 2008.

[13] Cull 2008.

deceptive political campaigns, for instance, to justify wars,[14] it has been avoided in order to delineate persuasive activity that is intended to be transparent and democratically controlled. Nevertheless, today's definitions of propaganda are quite similar to the classic ones. For example, Lasswell and Leites, among the first propaganda scholars, defined propaganda as "the manipulation of symbols as a means of influencing attitudes on controversial matters".[15] Contemporary researchers Jowett and O'Donnell say: "Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behaviour to achieve a response that furthers the desired intent of the propagandist."[16] Public diplomacy is sometimes placed in the triangle of hard power, soft power and smart power.[17] It may offer a clue to the classification of various types of influence, whose diverse names are confusing to the public, such as public relations, information and influence operations, marketing and advertising, strategic communication – just to mention a few. Terminology seems to be a means of influencing on its own, because any activity perceived as adverse can be labelled "propaganda", "manipulation" or "fake news" by an opponent. The report entitled *NATO 2030: United for a New Era* (2020) recommends that allies build shared terminology for hybrid threats, which would obviously lead to shared situational awareness and more united action against adverse activities, one of which is deceptive foreign propaganda. Bakir et al. propose a comprehensive theoretical framework founded on a continuum ranging from consensual forms of persuasion, which are transparent, to non-consensual forms, which are not transparent and comprise deception, incentivisation, coercion and deceptive coercion.[18] If the use of persuasive techniques is recognised in modern democracies as well as in international relations, the systematic description and analysis of various types of persuasion will be possible, including widely accepted methods of peer-to-peer public diplomacy. A comprehensive framework will also make it possible to distinguish between the state organised participation of volunteer citizens in promoting their country, conducting transparent activities, and troll armies hired for clandestine activities.

[14] Marlin 2003; Jowett–O'Donnell 2015.

[15] Lasswell–Leites 1965: 177.

[16] Jowett–O'Donnell 2015: 7.

[17] Nye 2008.

[18] Bakir et al. 2019.

## Peer-to-peer public diplomacy and social media

Joseph Nye explains that soft power is the ability of a country to attract others, especially with one's culture and values, which may result in an ability to manipulate the agenda of political choices available to others.[19] The recognition that civil society generates much soft power has led to the development of peer-to-peer public diplomacy. The process was facilitated by various factors: the loss of the prestige of state designed information and influence operations, the results of research into social networks and social media platforms and the re-evaluation of personal contacts and face-to-face encounters. As it was mentioned earlier, in international relations states have always tried to target the citizens of other states and this has become possible in the internet era. For instance, Israel launched a 'peoplehood diplomacy' project in 2010 and 2011 involving their public and the Jewish diaspora as advocates so as to improve the image of the country.[20] Following the identification of tools, messages and campaigns, Israeli citizens who volunteered were prepared for conveying positive messages globally. Thus, networks in foreign societies were created or activated faster and more effectively than in conventional, state-run public diplomacy activities. Messages were personalised making use of the enthusiasm and creativity of the participants, while they were still financed and controlled by the state. A remarkable idea of the project was dealing with misinformation, prejudice and stereotypes about Israel: a website was constructed as a resource for both foreign and home audience, where advocates could find evidence to counter hostile attitude. In case of the diaspora, careful selection and training preceded the activities of the advocacy delegations. The collection of contact information allowed the multiplication and extension of the social relationships of the networks. On the whole, the innovation of peer-to-peer diplomacy lies in its adaptation to the realities of the 21st century. It has included in its inventory the interaction between the digital world and the physical world; the merging of home audience and foreign audience; the blurring boundaries between state and non-state actors; the transformation of genres and social events; the global reach of individuals and, most of all, active and passive network building. The sections below, however, will highlight that the very same inventory of the Internet, namely, of the social media can be used as a weapon in psychological operations. In the ninth chapter of *Hybrid Warfare*

[19] Nye 2004.

[20] Attias 2012.

*Reference Curriculum. Volume II,*[21] the authors have already pointed out that they will write in more detail about the psychological operations in the context of the Ukrainian–Russian war. First, the concept of psychological operations will be defined. Psychological operations aim to impact the cognitive dimension to influence the selected target group.[22] The target group may not only be the enemy but also the allies or even a country's own population. For example, political campaigns aim to influence their own voters to mobilise them, their opponents' voters to stay at home, and the hesitants to vote according to the goals of the campaign designers. Even if in a different way, it is an activity that is as old as mankind. When the prehistoric tribes put bones on themselves and painted their bodies red to look more terrifying, thereby scaring away enemies, it came under this field of activity. With the evolution of technology, more and more new tools were used to influence the chosen target groups, and the spread of mass media led to a paradigm shift. Totalitarian regimes preferred to spread propaganda through mass media. This is one of the reasons why NATO avoids using the term propaganda in its information operations, as it has a negative connotation due to its Nazi and Soviet ideological and political implications. Consequently, NATO uses the terminology of 'targeted communication'.

## The negative impacts of social media

The emergence and spread of social media have been another important milestone in psychological operations. Social media has transformed many aspects of our lives, but the early positives of its use have quickly reversed. A series of studies have shown that it causes severe depression among young people,[23] significantly increasing anxiety.[24] Today, social media has become a serious weapon to influence individuals and societies. This can be attributed to several factors:

- Social networking sites gather data on tens of thousands of aspects of their users. To give just one example, they capture the messages that have been sent and those that have been typed but deleted before being

[21] Krasznay et al. 2024: 187–205.

[22] Narula 2004.

[23] Merrill et al. 2022.

[24] Wolniewicz et al. 2018.

sent.[25] As a result, the algorithms of social networking sites, combined with artificial intelligence and machine learning, can predict what users will do, when they will do it, and what they will do weeks in advance. In addition to information about individuals, open source information gathering is also relevant for trend analysis, where reactions to specific processes can be examined in real-time. More importantly, given sufficient data, future events can be predicted with high accuracy. For example, János Kertész, a Hungarian network researcher, and his co-authors have shown in a study that the trend analysis of a film's Wikipedia page can predict with 85% accuracy what the box office revenue will be on the first weekend of the film's release.[26]

- The Snowden case in 2013 demonstrated that social networking sites had become a tool of almost total surveillance by national security services.[27] In case of anti-democratic states, this is a fundamental way of controlling and oppressing the state's citizens. Consider, for example, the social credit system in China.[28]
- Social networking site algorithms create so-called opinion bubbles, which are amplified by the post-truth phenomenon.

In the absence of pluralistic consumption habits, this automated selection process adjusted to the user's behaviour may result in the development of a so-called filter bubble; that is, the user will only find those contents at media sites that they regularly consume, whereas they will encounter few or no contradicting contents; however widespread they may be otherwise.[29] Consequently, such a filter bubble potentially leaves the impression on the user that their narrowed perspective on reality is objective, encompassing reality as it is. A closely related concept is the recently expanding post-truth phenomenon, which essentially contributes to the impact of fake news on political decision-making.[30] The term post-truth refers to a state of affairs when public opinion is driven by emotions and beliefs rooted in personal convictions rather than being based on facts. In this

[25] Sleeper et al. 2013.

[26] Mestyán et al. 2013.

[27] Bányász 2014.

[28] Chen–Grossklags 2022.

[29] Spohr 2017.

[30] Lewandowsky et al. 2017.

situation, objectivity gradually loses its importance in reality perception while being replaced by many parallel subjective realities. This process contributes not only to the absorption of fake news but also to the confusion deliberately generated by disseminating alternative information questioning the validity of mainstream news releases. This latter activity is referred to as noise-making, which is aimed at undermining public trust in the institutions of democracy, thus impairing the perceived legitimacy of the current government. Noise making is commonly used by the national security agencies of authoritarian states, particularly against the Member States of the European Union, since fragmenting the EU hinders the Member States from standing up in unity as a global political actor, which leaves more scope to the political ambitions of the noise-making states. Researchers found that fake news, particularly fake political news, spread more rapidly, reached a wider audience, and underwent deeper absorption in all observed information categories, in some cases significantly exceeding the dissemination of valid news. It is also worth noting that people spread fake news faster than botnets.[31]

## Online deception in the Russia–Ukraine war

The Ukrainian–Russian war has given the experts many surprises. Everyone was counting on the dominance of previously assumed Russian capabilities in psychological operations, which have been used in an increasingly sophisticated way since 2014. After the beginning of the war, Russian psychological capabilities did not even approach the success of Ukrainian operations. The Russian national security services recognised the importance of filter bubbles and post-truth and successfully campaigned to reinforce mistrust. Covid-19 has strengthened this trend, significantly increasing the spread of pseudo-scientific content and reducing citizens' trust in science and democratic institutions. The various absurd fake news did not eliminate each other but fused into a new paradigm. An example from the first days of the war in Hungary: "Well, do you see Chemtrail stripes in the sky lately??? You haven't!!!!!!!!! Now, do you understand what Putin bombed?? The Ukrainian bio labs where these toxins were produced for us and […] their airports where the planes carrying the toxins took off!!! No more flu and Covid!!!!!!!!! Putin's bombs exploded for us! Ukraine was the dep

[31] Vosoughi et al. 2017.

stat’s (meaning Deep State – author’s note) war base!!! All the chemical sprays came from there, and all the poisons in our food came from there!!! So who is thanking Putin???? Bless his every step!!!”[32] We have corrected the spelling mistakes in the quote, which were otherwise numerous. In this Facebook post, several conspiracy theories appear, such as the hidden state, Covid as a biological weapon, chemtrail and genetically modified foods. As the algorithm creates a bubble for users, this content is spread mainly among those who already believe in this narrative. The bubble undermines these ambitions. In our opinion, the Russian lack of success can be explained by previous Russian achievements. However, in wartime, convincing others to support our narrative is crucial, and this requires convincing new audiences. Before the war, the independent press in Russia was not particularly strong, but after the beginning of the war it was almost eliminated by the Russian Government. For this reason, the Ukrainians had to be incredibly creative to inform the Russian population about the war by following the facts and not just with the narrative created by Russian propaganda and censorship. From the beginning of the war, it was vital for Ukraine to strengthen the morale of the population, while at the same time weakening the morale of the Russian soldiers, which was done with great creativity. As we have already pointed out in the mentioned study, cyberattacks and psychological operations influence each other. The fact that cyber volunteers have hacked into the records of the Russian armed forces and published the personal data of the soldiers who were fighting in Ukraine is a perfect illustration of this. Based on this, they started to call family members of soldiers who had been killed or taken prisoner of war in Ukraine to inform them about the soldiers’ condition. On the one hand, this informed Russian citizens that there was a war going on – the Russian narrative still says there are only special military operations today. By reporting on the condition of the troops, the morale in the Russian hinterland was reduced, and the appropriate questions were used to extract information about troop movements. Finally, a campaign was started whereby Russian soldiers who had been captured could inform their mothers by filling in Google Forms that they had been taken prisoners of war and that if their mothers came to collect them, they would be freed. In one stroke, this boosted

[32] To this day (July 2023), the user is very active on Facebook in spreading the Russian narrative similarly. Of course, the user may be a fake profile, but this does not diminish its importance. People who have accepted this narrative will encounter this sharing in the same way as if a real person had posted it. We cannot cite the original post to protect the individual’s rights.

the morale of Ukrainian soldiers, reinforcing their feeling of superiority while at the same time significantly lowering morale among Russian soldiers. Both countries have a strong interest in influencing international public opinion. As the war continues, Russia is attempting to reduce the unity of European Union members and strengthen the narrative among European citizens that sanctions do not harm Russia, only the EU. The purpose of this is to change the government's support for Ukraine by eroding the public's support. To neutralise this, Ukraine is also working hard since continued support is a matter of survival. Artificial intelligence will be the next game changer for fake news campaigns. Today, we already have numerous videos in which public figures say things they would not otherwise say.[33] This is known as Deepfake, whereby artificial intelligence montages the faces of public actors – even in real time – onto the actors' faces, and add their voice. As machine learning evolves, this technique will become more sophisticated in the future. This will further erode trust in a supposed truth.

## Conclusion

The technological potential of the social media may be exploited for either good or bad purposes. On the one hand, it can become a tool of transparent and democratically organised persuasion and shape public opinion and international relations in a beneficial way. This was illustrated by the case of peer-to-peer diplomacy introduced in Israel. On the other hand, social media may be a source of disinformation, of spreading fake news and deepfakes. In such a case it can be transformed into a malevolent force, like in political fake news campaigns, or in disseminating pseudo-scientific information like in the Covid-19 pandemic. Our examples were taken from psychological operations during the Russia–Ukraine war. In summary, it can be concluded that social media has a positive effect if it is used for connecting users and reality, and it has a negative effect if it is used for isolating users from one another and from reality.

[33] In this context, it is worth searching YouTube for the video from 2018 entitled *You Won't Believe What Obama Says in This Video!*

## Questions

1. What was the effect of the development of the media on political communication?
2. Why is peer-to-peer diplomacy also called "people's diplomacy"?
3. Does social media connect users or isolate them? Please give your opinion.
4. Which technological opportunities of the social media can be exploited in psychological operations?
5. Please discuss: how can resilience to online deception be improved?

## References

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

Bakir, Vian – Herring, Eric – Miller, David – Robinson, Piers (2019): Organized Persuasive Communication: A New Conceptual Framework for Research on Public Relations, Propaganda and Promotional Culture. *Critical Sociology,* 45(3), 311–328. Online: https://doi.org/10.1177/0896920518764586

Bányász, Péter (2014): Spies Act as a Spy: The Edward Snowden Case. In Sopóci, Milan et al. (eds.): *Manažment. Teória, výučba a prax 2014* [Management. Theory, Education and Practice 2014]. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 194–210.

Berelson, Bernard (1952): *Content Analysis in Communication Research.* New York: The Free Press.

Brosius, Hans-Bernd – Weimann, Gabriel (1996): Who Sets the Agenda? Agenda-Setting as Two-Step Flow. *Communication Research,* 23(5), 561–580. Online: https://doi.org/10.1177/009365096023005002

Chen, Mo – Grossklags, Jens (2022): Social Control in the Digital Transformation of Society: A Case Study of the Chinese Social Credit System. *Social Sciences,* 11(6). Online: https://www.mdpi.com/2076-0760/11/6/229

Cull, Nicholas J. (2008): Public Diplomacy: Taxonomies and Histories. *The Annals of the American Academy of Political and Social Science,* 616(1), 31–54. Online: https://doi.org/10.1177/0002716207311952

Fairclough, Isabela – Fairclough, Norman (2012): *Political Discourse Analysis. A Method for Advanced Students.* London – New York: Routledge.

Gerbner, George (1985): Mass Media Discourse: Message System Analysis as a Component of Cultural Indicators. In Van Dijk, Teun A. (ed.): *Discourse and Communication.* Berlin: De Gruyter, 13–25. Online: https://doi.org/10.1515/9783110852141.13

Hampton, Mark (2010): The Fourth Estate Ideal in Journalism History. In Stuart, Allan (ed.): *The Routledge Companion to News and Journalism.* London – New York: Routledge, 3–12.

Hurd, Ian (2008): Constructivism. In Reus-Smit, Christian – Snidal, Duncan (eds.): *The Oxford Handbook of International Relations.* Oxford – New York: Oxford University Press, 298–316.

Jowett, Garth S. – O'Donnell, Victoria (2015): *Propaganda and Persuasion.* Thousand Oaks – London: SAGE.

Katz, Elihu (1987): Communications Research Since Lazarsfeld. *Public Opinion Quarterly,* 51(4, Part 2), S25–S45. Online: https://doi.org/10.1093/poq/51.4_part_2.s25

Krasznay, Csaba – Bányász, Péter – Jakusné Harnos, Éva (2024): Geopolitical Context, Ideologies and Motivations. In Jobbágy, Zoltán – Zsigmond, Erika (eds.): *Hybrid Warfare Reference Curriculum. Volume II. Elective Seminars.* Budapest: Ludovika University Press, 187–205.

Krippendorff, Klaus (2004): *Content Analysis. An Introduction to Its Methodology.* Thousand Oaks – London – New Delhi: SAGE.

Lasswell, Harold D. – Leites, Nathan (1965): *Language of Politics.* Cambridge, Mass.: The MIT Press.

Lazarsfeld, Paul F. – Berelson, Bernard – Gaudet, Hazel (1944): *The People's Choice. How the Voter Makes up His Mind in a Presidential Campaign.* New York: Columbia University Press.

Lewandowsky, Stephan – Ecker, Ulrich K. H. – Cook, John (2017): Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. *Journal of Applied Research in Memory and Cognition,* 6(4), 353–369. Online: https://doi.org/10.1016/j.jarmac.2017.07.008

Marlin, Randal (2003): *Propaganda and the Ethics of Persuasion.* Peterborough: Broadview Press.

McQuail, Denis – Windahl, Swen (1993): *Communication Models for the Study of Mass Communications.* London: Routledge.

Merrill, Renae A. – Cao, Chunhua – Primack, Brian A. (2022): Associations between Social Media Use, Personality Structure, and Development of Depression. *Journal of Affective Disorders Reports,* 10. Online: https://doi.org/10.1016/j.jadr.2022.100385

Mestyán, Márton − Yasseri, Taha − Kertész, János (2013): Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data. *Plos ONE,* 8(8). Online: https://doi.org/10.1371/journal.pone.0071226

Narula, Sunil (2004): Psychological Operations (PSYOPs): A Conceptual Overview. *Strategic Analysis,* 28(1), 177–192. Online: https://doi.org/10.1080/09700160408450124

NATO (2020): *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

Neuendorf, Kimberly A. (2017): *The Content Analysis Guidebook.* Thousand Oaks – London: SAGE. Online: https://doi.org/10.4135/9781071802878

Nye, Joseph S. (2004): *Soft Power. The Means to Success in World Politics.* New York: PublicAffairs.

Nye, Joseph S. (2008): Public Diplomacy and Soft Power. *The Annals of the American Academy of Political and Social Science,* 616(1), 94−109. Online: https://doi.org/10.1177/0002716207311699

Philo, Greg (2010): News, Audiences and the Construction of Public Knowledge. In Stuart, Allan (ed.): *The Routledge Companion to News and Journalism.* London – New York: Routledge, 407−416.

Seib, Philip (2010): News and Foreign Policy: Defining Influence, Balancing Power. In Stuart, Allan (ed.): *The Routledge Companion to News and Journalism.* London – New York: Routledge, 496−506.

Shoemaker, Pamela J. (2016): The Gatekeeping of Political Messages. In Kenski, Kate − Jamieson, Kathleen H. (eds.): *The Oxford Handbook of Political Communication.* Oxford: Oxford University Press, 347–358. Online: https://doi.org/10.1093/oxfordhb/9780199793471.013.42

Sleeper, Manya – Balebako, Rebecca – Das, Sauvik – McConahy, Amber Lynn – Wiese, Jason – Cranor, Lorrie Faith (2013): *The Post that Wasn't: Exploring Self-censorship on Facebook.* Proceedings of the 2013 Conference on Computer Supported Cooperative Work, San Antonio, Texas, 23–27 February 2013, 793–802. Online: https://doi.org/10.1145/2441776.2441865

Southwell, Brian (2016): Two-Step Flow, Diffusion, and the Role of Social Networks in Political Communication. In Kenski, Kate − Jamieson, Kathleen H. (eds.): *The Oxford Handbook of Political Communication.* Oxford: Oxford University Press, 683–694. Online: https://doi.org/10.1093/oxfordhb/9780199793471.013.024

SPOHR, Dominic (2017): Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media. *Business Information Review,* 34(3), 150–160. Online: https://doi.org/10.1177/0266382117722446

VAN DIJK, Teun A. (1988): *News as Discourse.* Hillsdale: Lawrence Erlbaum Associates.

VOSOUGHI, Soroush − MOHSENVAND, Mostafa 'Neo' − ROY, Deb (2017): Rumor Gauge: Predicting the Veracity of Rumors on Twitter. *Association for Computing Machinery,* 11(4), 1–36. Online: https://doi.org/10.1145/3070644

WEIMANN, Gabriel (2017): *Multistep Flow of Communication. Evolution of the Paradigm.* Hoboken: Wiley.

WENDT, Alexander (1999): *Social Theory of International Politics.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9780511612183

WOLNIEWICZ, Claire A. – TIAMIYU, Mojisola F. – WEEKS, Justin W. – ELHAI, Jon D. (2018): Problematic Smartphone Use and Relations with Negative Affect, Fear of Missing Out, and Fear of Negative and Positive Evaluation. *Psychiatry Research,* 262, 618–623. Online: https://doi.org/10.1016/j.psychres.2017.09.058

# About the Authors

*Péter Bányász* – graduated in Political Science from the Faculty of Law and Political Science of the Eötvös Loránd University; then he obtained his doctorate at the Doctoral School of Military Engineering of the Ludovika University of Public Service. His research interests include the human aspect of cyber security, network theories of psychological operations, and the relationship between privacy and surveillance. He is a Lecturer at the Faculty of Public Governance and International Studies of the Ludovika University of Public Service and a researcher at the Institute for Cyber Security Research. He is also an active member of several scientific societies. He was the founding chairman of the Kápolnai Pauer István Youth Club of the Hungarian Association of Military Science, which as the head of its youth club, mentors several talented undergraduate and master students interested in military science.

*Andrea Beccaro* – is Professor of Strategic Studies, International Relations and Security Studies at SUISS, University of Turin. He worked in several research institutes (Freie University, Berlin; College of Europe Warsaw; IRAD, Rome) and his research is mainly focused on strategic thinking, security issues on the MENA region (mainly on Iraq, Syria, Libya), modern terrorism (mainly ISIS), and theory and practice of irregular warfare, i.e. counterinsurgency and modern evolution. His last works include: Non-State Actors and Modern Technology, in *Small Wars and Insurgencies,* 2023; Russia, Syria and Hybrid Warfare: A Critical Assessment, *Comparative Strategy,* 2021; ISIS in Libya and Beyond, 2014–2016, *The Journal of North African Studies; The "Gray Zone Warfare" Notion. The "Gerasimov Doctrine" and the Russian Approach to "Hybrid" Operations,* CeMiSS, Rome, 2020.

*Daniel Brezina* – currently works and lectures at the Department of Security and Defence of the Armed Forces Academy of General Milan Rastislav Štefánik. He is also engaged in scientific and research activities oriented towards the optimisation of decision-making processes of crisis management in the conditions of the Armed Forces of the Slovak Republic in the prevention and resolution of crisis phenomena of a non-military nature. He presented the results of project activities at international conferences at home and abroad. He is the recipient of the award for the best journalistic contribution for 2019 in the field of Regional Development and Rural Development. He is the author of a scientific monograph entitled *Rozhodovacie procesy na nižších úrovniach krízového riadenia* [Decision-making Processes at Lower

Levels of Crisis Management], in which he emphasises the application of proposals for improving the activities and organisational measures of crisis management bodies at the level of self-government and local state administration. From 2022, he is the main representative for the Slovak Republic in the System Analysis and Studies Panel within the North Atlantic Alliance.

*Valter Coralluzzo* – is Associate Professor of International Relations at the University of Turin, where he also teaches Foreign Policy Analysis and Strategic Studies. He has served as Director of CISP, an Italian Interuniversity Centre for Peace Studies, and is a member of the editorial board of *Rivista di Politica.* His main research interests focus on transformations of war, international relations theory and Italian foreign policy. His publications include: *La politica estera dell'Italia repubblicana, 1946–1992,* 2000; *Conflitti asimmetrici. Un approccio multidisciplinare* (edited together with Marina Nuciari), 2006; *Oltre il bipolarismo,* 2007; *Democrazie tra terrorismo e guerra,* ed., 2008; *Religioni tra pace e guerra. Il sacro nelle relazioni internazionali del XXI secolo* (edited together with Luca Ozzano), 2012; *Percorsi di guerra,* ed., to be published in 2025.

*Fabio De Ninno* – is Assistant Professor of Contemporary History at the University of Siena, member of the editorial board of Italia contemporanea and of various international research groups. He is a specialist in military and naval history and has published extensively on the history of the Italian Navy and the Italians at war in international journals. His main naval history work is *Fascisti sul mare. La marina e gli ammiragli di Mussolini,* 2017.

*Marco Di Giovanni* – is Associate Professor in Contemporary History at the University of Turin and Vice-President of Strategic Studies School Courses. He also teaches History of War Crimes and History of Military Institutions. He serves as Coordinator of the Master in International Political and Military Studies, University of Turin and CASD (Rome) and Coordinator of the Master in Global Strategy and Security, University of Turin and CASD (Rome). His main research interests focus on History of Military Institutions, Violence and War in History, Contemporary History. His publications include: *Scienza e potenza,* 2005; *Le regole della battaglia,* ed., 2013; *Le nuove giustificazioni della tortura nell'età dei diritti,* ed., 2017; *A European Framework for Military Institutions? International Integration and European Perspectives in Military Rhetorics after the Second World War* in the volume edited by Manuela Ceretta and Barbara Curli entitled *Discourses and Counter-discourses on Europe,* 2017; *Approcci "non convenzionali" alla guerra totale. Il caso della Germania nazista* *nella transizione politica degli anni '30: una riflessione prospettica* in the volume edited by Valter Coralluzzo entitled *Percorsi di guerra,* to be published in 2025.

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

*András Edl* – is a PhD student at the Ludovika University of Public Service with a broad experience both in the private sector (i.e. Morgan Stanley) and the state administration (i.e. Ministry of Foreign Affairs and Trade). He holds a broad range of international scholarships at the University of Vienna, Austria (2018), Josai International University, Japan (2016–2017), Qingdao Binhai University, China (2014). He is enthusiastic about global security, space activity and security, psychology (especially education) and societal issues. His research area are actual trends and developments of the space industry, and the relationship between space programs and international security.

*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.

*Éva Jakusné Harnos* – is an Applied Linguist and Political Discourse Researcher. She holds a PhD in Linguistics (Eötvös Loránd University, Budapest, 2005). Has been working in higher education since 2003. She is an Adjunct Professor, specialising on propaganda research, persuasion, deception, fake news and security studies. A curriculum developer, the author of course books on the language of politics and military terminology. A participant of the EUSecure blended and MOOC curriculum development project funded by the European Union.

*Eitan Shamir* – is a Senior Lecturer at the Political Science Department, Bar-Ilan University and a Senior Research Associate at the Begin Sadat Center for Strategic Studies (BESA Center). Prior to his academic position, he was in charge of the National Security Doctrine Department at the Ministry of Strategic Affairs, Prime Minister's Office. Before joining the Ministry, he was a Senior Fellow at the Dado Center for Interdisciplinary Military Studies (CIMS) at the IDF General Headquarters. He is expert on insurgencies and combat doctrine. His research interest and publications focus on topics such as strategy, command, military innovation and reforms, and military culture.

*Bálint Somkuti* – is a Military Historian and a Security Policy Expert. He specialises in modern warfare, irregular and guerrilla warfare, as well as other forms of interest advancement. He is the co-author of *Kis háborúk nagy hatással* [Small Wars with Big Impact]. A regular guest in military and security policy issues in various TV and radio shows in Hungary, but also in places such as Belarus and South Africa.

*Enrico Spinello* – is a Senior Officer of the Italian Army. He works in the IT Army Education and Training Command and School of Applied Military Studies, Turin as Section Chief for University and External Relations and he is the Coordinator for International Mobility at SUISS, University Interdepartmental School for Strategic Science. He is a teacher at SUISS and he is involved in several Erasmus KA2 research projects in the security and defence area. He is the IT Army Representative in the Executive Academic Board (EAB), Implementation Group (IG) at the European Security and Defence College (ESDC) and IG Vice Chair for Education.

The third volume offers a selection of topics suggested for those who wish to further deepen their theoretical knowledge on the subject matter. This volume consists of elective lectures in which the 20th and the 21st centuries are compared considering the wide presence and relevance of non-military instruments fused together with the kinetic and operational dimension, making the boundaries between state of war and peace indefinite. The phenomenon of strategic surprise will be analysed thoroughly, and it will be shown whether it has a particular resonance with Hybrid Warfare or does it really follow the patterns of other military activities. The defining characteristics of gray zone coercion will also be addressed in light of its specific relevance to the maritime domain. For the intellectually hungry, the salami slicing and cabbage peeling tactics will be introduced, too. The advantages and disadvantages of “hybrid warfare strategy” will be contemplated in various political and military contexts. Again, regional considerations will be analysed in a more thorough way. Some case studies will also help to put the issue into context, such as the war in Chechnya, in Georgia or the second Lebanon war, and more. Once again, the topic of social media will be raised, it being an important instrument not only for public diplomacy but also as a weapon of psychological operations using misleading information and merging it into the online discourse without the target audience realising it.

9 789636 531096