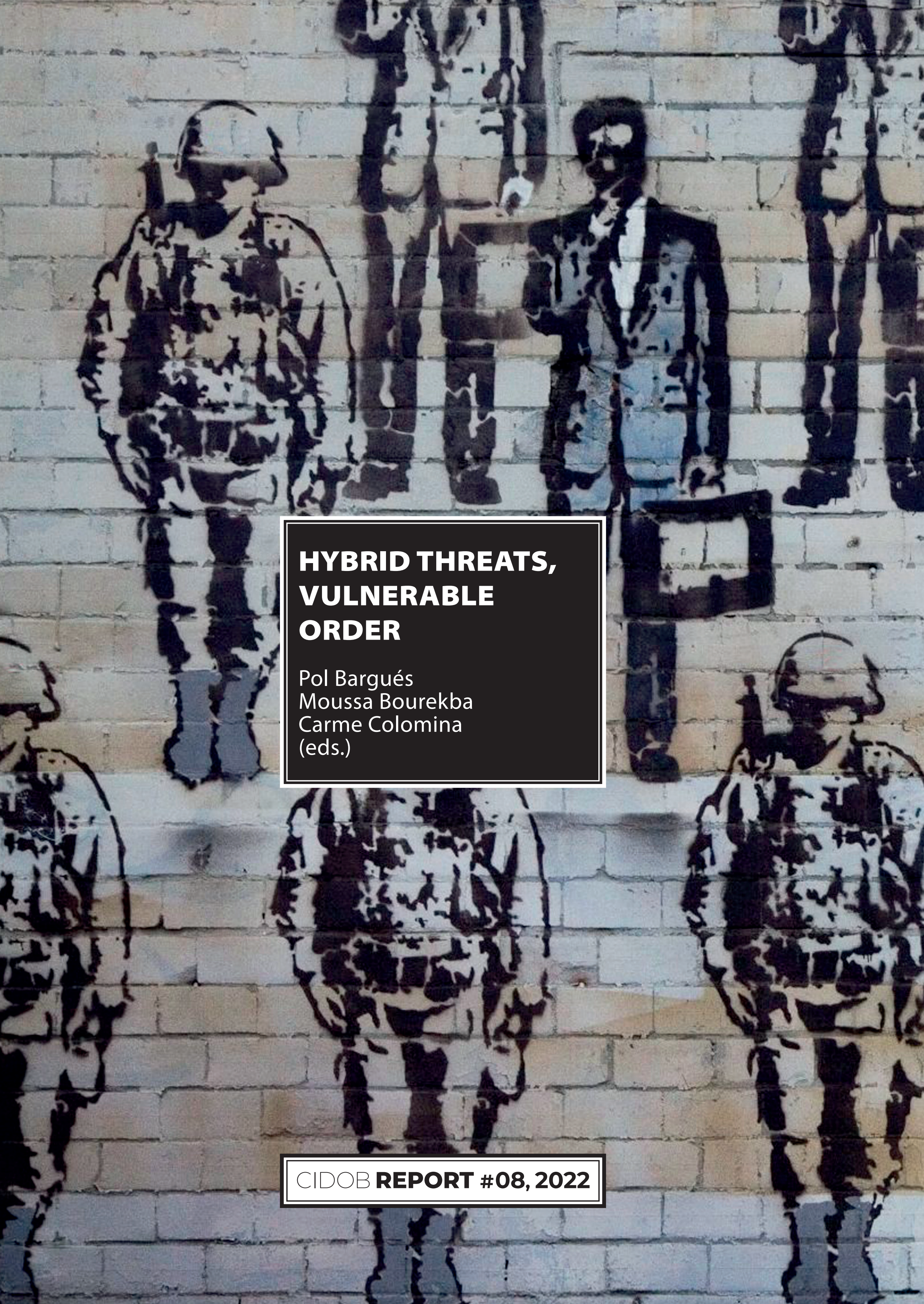

HYBRID THREATS, VULNERABLE ORDER

Pol Bargués
Moussa Bourekba
Carme Colomina
(eds.)

CIDOB **REPORT #08, 2022**

HYBRID THREATS, VULNERABLE ORDER

Pol Bargués, Moussa Bourekba
Carme Colomina (eds.)

CIDOB REPORT # 08
Barcelona, September 2022
ISSN: 2564-9078

CIDOB
BARCELONA
CENTRE FOR
INTERNATIONAL
AFFAIRS

Edited by: Pol Bargués, Moussa Bourekba and Carme Colomina

CIDOB
Elisabets, 12
08001 Barcelona
Tel.: 933 026 495
www.cidob.org
cidob@cidob.org

Print: Promotion Digital Talk S.L.
ISSN: 2564-9078 • E-ISSN 2564-9124
Depósito legal: B 11820-2017

Edition: Elisabet Mañé
Design and layout: Joan Antoni Balcells
Web and technical support: Sílvia Serrano
Sales and shipments: Marta Lizana
Production: Anna Busquets Ferré

Barcelona, september 2022

Cover
Thomas Hawk, "Soldiers and Suits".
https://www.flickr.com/photos/thomashawk/91024106/in/photolist-93wi9-7AcQeF-8qYk3a-aqZ5do-bALwwk-7srmF1-dy6PvW-yp9qip-262qeEw-km964-cVvVbs-29L3HBg-eMTwa3-ecFP7V-a7xKDz-8E9FFC-ndrV2-zx3qX2-6Hhgs1-2bY5HR1-4ySCY-KXgCU-9jbHK8-7W97uG-K97jYR-aBxWU5-x6rkHu-9m5sqN-q6ULbi-4K9y1G-6pZ32n-4LojPy-2B2nK-2Kv8n6-mGiJxz-L53iMG-4zhNCh-8N72Cn-biWfN4-bs8LVj-zCk3j-6DbBai-cgbqyJ-aj1XxK-9NV89b-2WNbMH-8DVkGv-zVfvG-4Lyxbv-4K9xCN

CONTENTS

CIDOB REPORT
# 08- 2022

PROLOGUE

Pol
Morillas
Director, CIDOB

Hybrid threats – conventional and unconventional tactics deployed in conflict scenarios or in the geopolitical tussle between leading global actors – are an increasingly destabilising factor in the international order. In the West, NATO's most recent Strategic Concept, presented at its Madrid Summit (June 29–30th 2022), reiterated that strategic competitors «interfere in our democratic processes and institutions and target the security of our citizens through hybrid tactics», and «conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion». The European Union, meanwhile, has been producing instruments, strategies and joint communications to coordinate internal and external policies and thereby increase European resilience to hybrid threats since at least 2016, around the time its Global Strategy was published.

Far from a solely Western phenomenon, hybrid tactics are gaining prominence on several continents. In Africa, hybrid operations to support extremist groups have been detected, elections have been interfered with and critical infrastructure attacked. In 2021, for example, South Africa's energy supply was sabotaged on more than one occasion, affecting major industries and exacerbating the country's energy crisis. In the Indo-Pacific, hybrid threats are growing «in breadth, application and intensity». And, with the invasion of Ukraine ongoing, Russia accuses the West of launching a «total hybrid war» against it, even as the Kremlin regularly uses destabilisation tactics as part of its playbook. With international relations dominated by geostrategy and realpolitik, hybrid tactics proliferate, hindering cooperation and trust in global governance institutions.

But what is new about these threats? Unconventional tactics like the use of proxies, insurgent groups and propaganda have been deployed in countless wars throughout history in order to destabilise or punish the enemy. Even in times of peace during the 20th century, interstate competition included crude strategies involving espionage, propaganda, economic battles, meddling in democratic processes and instigating insurgencies (Johnson, 2018). It may be that the rise of hybrid conflicts – or the increased perception of them – is due to a new awareness of vulnerability among those who believed themselves invulnerable.

IT MAY BE THAT THE RISE OF HYBRID CONFLICTS – OR THE INCREASED PERCEPTION OF THEM – IS DUE TO A NEW AWARENESS OF VULNERABILITY AMONG THOSE WHO BELIEVED THEMSELVES INVULNERABLE.

As its starting point, this *CIDOB Report* takes the observed growth in hybrid tactics and the threats perceived as such, along with a generalised concern about the hybrid. Two key factors help us understand this growth: on the one hand, the increasing interdependence between states and, on the other, the exponential diversification of hybrid tactics.

In terms of the first factor – interdependence – greater connectivity in international relations, especially since the end of the Cold War, facilitated the spread of globalisation and economic, commercial, energy, political and cultural exchanges. It was assumed that connection and interdependence between countries would curb the appetite for conflict while, at the same time, contributing to development, democratisation and peace around the world. However, as Mark Leonard argues, this «hyperconnectivity» also gives opportunities to states that are prepared to exploit the vulnerabilities of others. For Leonard, «the trick is to make your competitors more dependent on you than you are on them – and then use this dependency to manipulate their behaviour» (2016: 15). Interdependence, thus, also has its downsides and can be used to exploit vulnerabilities and exacerbate confrontation between great powers, or even between opposing or polarised communities within a society. This has led actors like the European Union to reinforce their strategies to grant themselves greater strategic autonomy.

The second factor is the diversification of hybrid tactics. From migration to disinformation, electoral interference, the use of natural resources and computer viruses, anything can be turned into a weapon that can be launched from anywhere with unpredictable consequences. The exploitation of the vulnerabilities of others has also been facilitated by civil and military technological developments, as well as state and non-state actors' use of information and communication technologies. The digitalisation process, meanwhile, has exponentially multiplied disinformation's capacity to spread and penetrate.

Faced with this new scenario in which hybrid threats are growing based on the exploitation of interdependence and the diversification of tactics, which strategies and methods are used to address these conflicts? What impact do hybrid threats have on today's societies? What political responses are proposed? This *CIDOB Report* addresses the challenge hybrid threats pose in today's societies and aims to contribute to the debate at a time when the international context is characterised by war returning to Europe, rising contestation and polarisation in the liberal international order, the crisis of multilateralism and global governance norms and the post-pandemic geopolitical transformation.

THE EXPLOITATION OF THE VULNERABILITIES OF OTHERS HAS BEEN FACILITATED BY CIVIL AND MILITARY TECHNOLOGICAL DEVELOPMENTS, AS WELL AS STATE AND NON-STATE ACTORS' USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. THE DIGITALISATION PROCESS, MEANWHILE, HAS EXPONENTIALLY MULTIPLIED DISINFORMATION'S CAPACITY TO SPREAD AND PENETRATE.

To do this, the authors focus on some of the main hybrid threats, as well as the development of hybrid conflicts in various regions of the world. In the next chapter, Pol Bargués and Moussa Bourekba contextualise the emergence of hybrid conflict as a concept and examine its analytical and practical advantages. The second chapter deals with disinformation as a tool of geopolitical confrontation, as Carme Colomina analyses how technological transformation has amplified the impact of information wars. Chapter 3, by Blanca Garcés-Mascareñas, reflects on the instrumentalisation of migration by state actors within the frameworks of various hybrid conflicts affecting several European countries. In chapter 4, John Kelly highlights the increasing use of disinformation tactics to destabilise democratic regimes and outlines the main challenges with addressing the multifaceted threat disinformation poses to democracies. Along these same lines, Manel Medina Llinàs, author of chapter 5, demonstrates how cyberspace has been added to the map of traditional conflict battlefields – land, sea and air – and how the use of cyber weapons has become a strategic challenge in the context of hybrid conflicts.

Thereafter, the volume focuses on geographical spaces of confrontation. The sixth contribution to this *CIDOB Report* addresses the concept of resilience in a conflict characterised by the combination of hybrid tactics and conventional warfare: Russia's ongoing invasion of Ukraine. Andrey Makarychev and Yulia Kurnyshova argue that Ukrainian society's response to this conflict is also hybrid, since it does not fit the traditional top-down structure by which an attacked/invaded state normally manages a civil response, but instead shows a high degree of autonomy and self-organisation. Given the increasing influence of the proliferation of hybrid conflicts on the global stage, Guillem Colom Piella's contribution examines the evolution of NATO's strategic frameworks for detecting, countering and responding to hybrid threats. Inés Arcos Escriche, author of chapter 8, goes further in this direction in her analysis of China's expansion strategy. The hybrid is nothing new in Chinese foreign policy. Indeed, its age-old hybrid strategy deploys a genuine mix of diplomatic, economic and military tools to promote and defend its core interests of sovereignty and territorial integrity, even in times of peace. The final chapter addresses another region of the world in which a confrontation combining conventional and unconventional methods is blurred: the Maghreb. In his contribution, Eduard Soler analyses the growing tensions between Morocco and Algeria and underlines that, rather than replacing conventional threats, hybrid tactics could precede or even encourage an armed confrontation.

References

Johnson, Robert. 2018. «Hybrid War and Countermeasures: A Critique of the Literature», *Small Wars & Insurgencies*, vol. 29, 1, 2018, 141–163.

Leonard, Mark**.** *Connectivity Wars: Why Migration, Finance and Trade are the Geo-Economic Battlegrounds of the Future*. European Council on Foreign Relations, 2016 (online). [Accessed on 14.09.2022]: https://ecfr.eu/wp-content/uploads/Connectivity_Wars.pdf

WAR BY ALL MEANS: THE RISE OF HYBRID WARFARE

Pol Bargués
Research Fellow, CIDOB

Moussa Bourekba
Researcher, CIDOB

CIDOB REPORT
# 08- 2022

Concept, origins and criticisms

Hybrid warfare became a popular concept in NATO military discussions in the early 2000s as a way to describe new ways of waging war that combined regular and irregular methods. Hybrid tactics, including urban guerrilla warfare, sophisticated weaponry like drones, disinformation, kidnapping and even terrorism, were used by state and non-state actors in the violence produced by the international interventions in Afghanistan and Iraq, the interfaith war between Sunnis and Shiites, the strategies of transnational terrorist groups like Al Qaeda and the war between Israel and Hezbollah. Such attacks were multiple, heterogeneous, almost always plagued by uncertainty, and paid little heed to the rules of war. Hybrid warfare thus represented a shift away from the «old wars» of the 20th century, like World War I and II, which were characterised by conventional confrontations between regular armies, while also adding complexity to the «new wars» of the 1990s, like those in Bosnia, Sierra Leone and Liberia, in which networks of state and non-state actors clashed over identity politics, and which were managed by international peacebuilding missions (Kaldor, 2001).

However, the differences between these conflicts were probably insubstantial: what really changed was the perspective of the West. In the 1990s, blinded by a period of integration, prosperity and the perception of victory at the end of the Cold War, the United States and its Western allies failed to understand the wars being waged by others over territory, economic and strategic interests, identity and religion (Bargués-Pedreny, 2018). But in the 2000s, with the «Global War on Terrorism» in full sway, the rise of hybrid tactics brought an end to the «self-delusion» of the 1990s, when it was believed that international institutions could limit and regulate peace and war (Johnson, 2018: 143).

Soon after, hybrid threats were contaminating peaceful areas as much as conflict zones. In 2014, «little green men» in unmarked uniforms entered Crimea to take control of infrastructure, facilitate a referendum and annex Ukrainian territory for Russia. The evidence of continual cyberattacks, disinformation campaigns, interference in democratic processes and the mobilisation of migrants at the European Union's external borders have seriously harmed EU–Russia relations. Hybrid attacks blur the boundaries between war and peace. They exploit the opportunities of an interconnected and globalised world to weaken the adversary without expending resources on the conventional battlefield (Colom Piella, 2018).

HYBRID ATTACKS BLUR THE BOUNDARIES BETWEEN WAR AND PEACE. THEY EXPLOIT THE OPPORTUNITIES OF AN INTERCONNECTED AND GLOBALISED WORLD TO WEAKEN THE ADVERSARY WITHOUT EXPENDING RESOURCES ON THE CONVENTIONAL BATTLEFIELD.

Critical voices stress that the «hybrid» is not a new phenomenon – that a range of tactics have featured in almost all conflicts throughout history. Unconventional methods have been noted since at least the Punic Wars, when the Romans used demoralisation and attrition tactics, attacked supply lines and avoided direct combat to fight a Carthaginian army that was superior on the battlefield (Carr & Walsh, 2022). Other critical studies argue that hybrid warfare is a Eurocentric catch-all concept that helps the West explain the strategies of third parties using examples as disparate as the war in Ukraine, the conflict between Morocco and Algeria and the deliberate mobilisation of migrants for political purposes (Johnson, 2018). So, if other concepts already exist to describe today's conflicts, like *asymmetric warfare*, *complex irregular warfare*, *connectivity wars*, *fourth or fifth generation warfare* and *grey zones*, what added value does speaking of hybrid warfare bring?

It is the escalation of these tactics that has placed the concept back in the spotlight. In Europe, like in other regions of the world, government and international organisations' security strategies increasingly reflect a perception that hybrid threats are always lurking – in times of peace and war – on land, at sea, in the air, online and even in space. This conceptual chapter, which aims to lay the foundations for the analysis in this *CIDOB Report*, focuses on three features of hybrid warfare that are shaping international relations today. First, the uncertainty that surrounds hybrid warfare, which makes it difficult to separate war from peace and to prove who is behind an attack. Second, the diversification of tactics for exploiting other states' vulnerabilities. And, finally, the aims of these tactics, which seemingly seek to undermine the adversary's values and the legitimacy of their political systems. Destabilisation is the goal, rather than victory.

Uncertainty, multiplicity and confusion

Long gone are the days when hostilities between states began with formal declarations of war. Analysts have highlighted that hybrid tactics often remain below the threshold of war in order to wear the opponent down while avoiding larger-scale confrontation and the risks of mutual destruction, as might be the case in a clash between nuclear powers like Russia and NATO member states (Friedman, 2018). Hybrid tactics complicate peacetime and inter-state relations, making wars more uncertain and confusing.

In fact, hybrid warfare abounds with uncertainty. It is difficult to trace responsibility for cyber and other types of attack, or to prove who has organised disturbances. It is impossible to know who began a disruptive rumour, and fake news is difficult to deny. In a conventional war the state and the army are usually responsible for the fighting, but hybrid warfare may involve proxies, hackers, criminal gangs, drug traffickers, paramilitaries, terrorists and private contractors like Blackwater, G4S Secure Solutions and the Wagner Group.

HYBRID WARFARE ABOUNDS WITH UNCERTAINTY. IT IS DIFFICULT TO TRACE RESPONSIBILITY FOR CYBER AND OTHER TYPES OF ATTACK, OR TO PROVE WHO HAS ORGANISED DISTURBANCES. IT IS IMPOSSIBLE TO KNOW WHO BEGAN A DISRUPTIVE RUMOUR, AND FAKE NEWS IS DIFFICULT TO DENY.

The second notable feature that bears on contemporary international relations is the use of new destabilisation tactics. Unimaginable a few years ago, they are increasingly diverse. Tanks and machine guns are deployed in combination with sophisticated weaponry like drones, hypersonic missiles and hybrid insect micro-electro-mechanical surveillance systems. These technologies are not only in state hands, but also of terrorists, criminals and drug traffickers. Terrorist groups use social media to recruit fighters, foment hatred, spread propaganda and prepare attacks. States allow hundreds of migrants across borders over a few hours to generate sensations of overflow and vulnerability in a neighbouring country. Disinformation helps polarise societies and delegitimise institutions, and multinational companies participate as private actors in conflicts and international relations (see the chapters by Garcés Mascareñas and Colomina in this volume).

These diverse tactics are deployed to attack and exploit other states' economic, political and diplomatic vulnerabilities. Key to this is how globalisation and interdependence, which have facilitated cooperation and exchange, have also opened up opportunities to launch attacks and generate tension. In the words of Mark Leonard, «[i]nterdependence, once heralded as a barrier to conflict, has turned into a currency of power, as countries try to exploit the asymmetries in their relations». Every connection is susceptible to instrumentalisation, and thus scepticism and mistrust have grown between the great powers. As Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security Policy and Commission's Vice-President, wrote in the prologue to the European Union's Strategic Compass: we live in a world shaped by power politics in which «everything is weaponised and where we face a fierce battle of narratives».

STATES ARE INCREASINGLY RESORTING TO HYBRID TACTICS BECAUSE THEY OFFER AN UNBEATABLE STRATEGIC ADVANTAGE, HELPING ACHIEVE CERTAIN OBJECTIVES, WHETHER POLITICAL, ECONOMIC OR OF ANOTHER NATURE, WITHOUT CLOSING THE DOOR TO ANY FORM OF NEGOTIATION OR DIPLOMATIC OR ECONOMIC RELATIONS.

The third significant feature of these hybrid conflicts is their goals. Just as their beginnings are tricky to pinpoint, they do not necessarily seek a «victory» that brings the conflict to an end (O'Driscoll, 2019). So if they are not deployed to win war or peace, what are the goals of hybrid tactics? Disinformation, manipulation and electoral interference seek to undermine the legitimacy of institutions, the trust in administrations and to alter election results. Hybrid tactics produce instability and erode democracy, create political polarisation and destroy coexistence and consensus.

States are increasingly resorting to hybrid tactics because they offer an unbeatable strategic advantage, helping achieve certain objectives, whether political, economic or of another nature, without closing the door to any form of negotiation or diplomatic or economic relations. With no declaration of war or open conflict situation between two states the possibility of discussing peace and negotiating always remains. From this perspective, hybrid warfare usually costs considerably less than the burdens of a conventional war. It is easier to begin, as it evades direct responsibility; the means are logistically less complex and economically less costly; and it is politically less risky, as military victory is not the end goal.

Conclusion: hybrid times

Hybrid warfare is not a new phenomenon, but it has proliferated at a time when the West is feeling its hegemony being contested and international norms are being undermined. Studying hybrid tactics helps us understand the growing uncertainty that surrounds situations of both peace and war, and underscores the number of methods and means that allow an actor to achieve certain objectives. In other words, as a concept, it can help us focus on how actors relate to each other and how they intend to fight. The implications for the international order are profound. This mode of conflict is repeatedly used by state and non-state actors for the purposes of military, political, economic and social destabilisation. Rules are broken, relationships deteriorate. The strategic advantages offered by hybrid tactics, along with the low costs of resorting to them, are the reasons for their proliferation and intensification. From this perspective, we need to rethink our analytical and strategic frameworks in order to minimise the destabilising effects of this new generation of conflicts.

References

Bargués-Pedreny, Pol. *Deferring Peace in International Statebuilding: Difference, Resilience and Critique*. London: Routledge, 2018.

Carr, Andrew & Benjamin Walsh. «The Fabian strategy: How to trade space for time», *Comparative Strategy*, 41:1, 2022, 78–96.

Colom Piella, Guillem. «Guerras Híbridas. Cuando el contexto lo es todo». Revista Ejército 927, 2018, 38-44.

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

Johnson, Robert. «Hybrid War and Its Countermeasures: A Critique of the Literature», *Small Wars & Insurgencies*, vol. 29:1 (2018), 141–163.

Kaldor, Mary. *Las nuevas guerras: la violencia organizada en la era global*. Barcelona: Tusquets, 2001.

O'Driscoll, Cian. *Victory: The Triumph and Tragedy of Just War*. Oxford: Oxford University Press, 2019.

WORDS AS WEAPONS: FROM DISINFORMATION TO THE GLOBAL BATTLE FOR THE NARRATIVE

Disinformation is a key tool in the armoury of hybrid threats. It generates instability and erodes democracy, creates political polarisation and harms social coexistence and consensus. The ability to alter information and data – so decisive for obtaining power – poses a threat to democratic processes. It is also being deployed in the service of a technological and digital confrontation that is shaping a new bipolarity on the international agenda. However, the truly offensive capacity of words as weapons lies less in the content of the message than in the power social networks grant for them to go viral and achieve penetration.

Carme Colomina
Research Fellow,
CIDOB

CIDOB REPORT
# 08- 2022

In 1998, General Vladimir Slipchenko, then Vice President of the Russian Academy of Military Sciences, stated that «information is a weapon just like missiles, bombs, torpedoes, etc. It is now clear that the informational confrontation becomes a factor that will have a significant impact on the future of the war themselves, their origin, course and outcome».

Military logic and technological transformation have converged in a digital space in which the internet has become one of the crucial fields of destabilisation. In *The Road to Unfreedom: Russia, Europe, America* (2018), Timothy Snyder writes that the most important part of Russia's 2014 invasion of Ukraine was the information warfare designed to undermine reality. Between that initial cyber offensive, the largest in history, according to Snyder (although it didn't make headlines in the West), and the digital frontline of the Russian invasion of Ukraine that began on February 24th 2022, the hybridisation of the conflict and the contestation of the global order underwent their own acceleration.

For the West, the war in Ukraine is the first to go viral, being broadcast over social media in real time and narrated on the basis of fragments of images that attempt in just a few seconds to convey the threats, fears, heroic acts and devastation. The online story does not always match the offline facts. In truth, though, it is not the first war to be mediated by social networks. Syria was the laboratory for evading an international media blackout using a torrential flow of online content provided by local activists and journalists from within the country. This, in turn, raised major ethical questions about information circuits and the veracity of sources.

But Ukraine could become the first war to pit the two major global digitalisation models and their respective platforms against one another. Russian and Chinese techno-authoritarianism versus the US Silicon Valley model. Telegram and Tik Tok's power to shape the global narrative about the war versus US technology giants' involvement in the conflict as private actors aligned with Western strategies to exert political pressure, to capture and control data (from mapping to censorship), or to provide analysis and technical information to strengthen the Ukrainian government's security.

(Dis)information is a weapon in wartime and a hybrid threat to peace. It is a non-military tool that can be used to disrupt and destabilise civic spaces, with consequences for local, regional and national security. But its truly offensive capacity resides less in the content of the message than in the power social networks grant it to go viral and penetrate. Hence, it is first essential to understand how digital interconnection has transformed social relations and power balances at a global scale, both between major powers and between the new international relations actors (state, non-state and private). Disinformation cannot be separated from the socio-psychological factors, technical drivers and incentives that are intrinsic to our hyperconnected times (Van Raemdonck and Meyer, 2022).

Algorithmic order

The internet is the infrastructure on which our daily life is built. Technology has transformed our experience of immediacy, plunging us into an infinity of (dis)information possibilities, a profusion of sources and stories – true or not – offered to us by the internet with no need for intermediaries. Post-truth does not just mean lies. It means a distortion of the truth that is above all laden with intentionality. In this space, information competes with contradictory stories, hoaxes and half-truths, conspiracy theories, messages of hatred and attempts to manipulate public opinion. The explosion of online disinformation has led «a new social harm» (Del Campo, 2021) to emerge via a range of types of falsehood – both legal and illegal – that impact public discourse and human security.

Old-style propaganda has been exponentially amplified by technology and hyperconnectivity and its power and sophistication have multiplied. The possibilities are vast: social networks (open or encrypted); bots (software applications that execute automated tasks) and microtargeting techniques, such as dark advertising, which is psychometrically targeted to influence public opinion and poison the discursive atmosphere; artificial intelligence systems fed data and trained to mimic humans or reproduce human cognition; and audio and video manipulation techniques that change our perceptions and lead us to distrust even our ability to discern what is and is not true.

(DIS)INFORMATION IS A WEAPON IN WARTIME AND A HYBRID THREAT TO PEACE. IT IS A NON-MILITARY TOOL THAT CAN BE USED TO DISRUPT AND DESTABILISE CIVIC SPACES, WITH CONSEQUENCES FOR LOCAL, REGIONAL AND NATIONAL SECURITY. BUT ITS TRULY OFFENSIVE CAPACITY RESIDES LESS IN THE CONTENT OF THE MESSAGE THAN IN THE POWER SOCIAL NETWORKS GRANT IT TO GO VIRAL AND PENETRATE.

For Byung-Chul Han (2022), «infocracy», or the digital world's «information regime», is a form of dominance in which information and its processing through algorithms and artificial intelligence decisively determine both economic and political social processes. The ability to alter information and data – so decisive for obtaining power – poses a threat to democratic processes.

Algorithms are exploited by companies like Cambridge Analytica to create profiles based on people's gender, sexual orientation, beliefs and personality traits to be used for political manipulation. Societies are vulnerable because we are vulnerable as individuals. We are exposed to the opaque order and will of algorithms that Cathy O'Neil elevates to the category of «weapons of math destruction».

Disinformation, defined by the European Commission as «false information, deliberately created to harm a person, social group, organisation or country», aims to destabilise societies and directly attacks civic spaces with the aim of fomenting polarisation and unease, if not outright conflict (Freedman et al., 2021; Medina, in this volume). But misinformation does not spread in a vacuum. Its ability to penetrate public debates, to confuse, and to undermine trust in institutions and electoral processes, for example, is often based on existing socio-cultural divisions. It targets pre-existing vulnerabilities and groups of people supposedly inclined to trust such sources and narratives, and who may willingly or unwillingly contribute to their dissemination. Abuses of power, dysfunctional political systems, inequalities and exclusion are breeding grounds for disinformation (Van Raemdonck and Meyer, 2022).

The identification of these vulnerabilities in order to generate messages that exacerbate them is considered to pose a hybrid threat to democratic systems, which are more exposed due to their open nature. In Chantal Mouffe's (1999) agonistic model, conflict and challenging the political and social status quo are essential parts of pluralism in deliberative democracies. But when disinformation violates the right to hold opinions without interference (article 19 of the ICCPR), increases citizens' vulnerability to hate speech or strengthens state and non-state actors' ability to undermine freedom of expression it becomes a threat to human rights and the bases of democracy. Disinformation in all its forms – from lies to incitement to hatred, via memes and audiovisual manipulation – are, thus, not only «weapons of mass distraction», they often form part of deliberate disruption strategies to alter the perceptions of public opinion. In these cases, along with the goal of causing harm or making profit that characterises this false content, there are usually strategies and techniques designed to maximise their influence. The aim is to undermine the adversary's values and the legitimacy of their political system (Bargués and Bourekba, in this volume).

THERE ARE NO GEOGRAPHICAL LIMITS TO THE MANIPULATION ATTEMPTS, AND THEY DO NOT HAVE A SINGLE ORIGIN. IN RECENT YEARS, FACEBOOK AND TWITTER HAVE LISTED SEVEN COUNTRIES (CHINA, INDIA, IRAN, PAKISTAN, RUSSIA, SAUDI ARABIA AND VENEZUELA) THAT USE THE PLATFORMS TO CONDUCT FOREIGN INFLUENCE CAMPAIGNS TO SWAY GLOBAL AUDIENCES. SOCIAL NETWORKS ARE A NEW INSTRUMENT OF GEOPOLITICAL POWER.

When analysing the actors responsible for disinformation, UNESCO's Working Group on Freedom of Expression and Addressing Disinformation distinguishes between the authors of the content and those in charge of distributing it: between instigators (direct or indirect), who are active at the origin of the disinformation; and agents (influencers, individuals, organisations, governments, companies and institutions), who are in charge of spreading the falsehoods (Bontcheva and Posetti, 2020). The agents who spread the falsehoods, conspiracies and threats – voluntarily or involuntarily – and act as amplifiers of the disinformation may, in turn, be victims of manipulation or attempts to exploit social vulnerabilities. The result is increased scepticism and lower trust in institutions. Today, the consensuses that structure democratic societies are weaker.

This is by no means solely a Western phenomenon, and the threats do not only come from outside. The polarisation that has grown in global politics, especially over the last five years, has shown social media's power to radicalise public discourse. From the January 6th insurrection on Capitol Hill in Washington to the Rohingya genocide in Myanmar; and from the exploitation of the US racial conflict using fake accounts and online trolling to the «brutal and unrelenting» disinformation campaign promoted by the Russian and Syrian governments (according to a Bellingcat investigation in 2018) against the White Helmets, the NGO in charge of investigating the flagrant human rights violations committed by both countries' armies during the Syrian war.

Post-truth geopolitics has transformed threats and strategies. As the World Economic Forum's *Global Risks Report* warned in 2019, «[n]ew technological capabilities have amplified existing tensions over values—for example, by weakening individual privacy or deepening polarization—while differences in values are shaping the pace and direction of technological advances in different countries».

Geopolitical order

There are no geographical limits to the manipulation attempts, and they do not have a single origin. In recent years, Facebook and Twitter have listed seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela) that use the platforms to conduct foreign influence campaigns to sway global audiences. Social networks are a new instrument of geopolitical power that have enthroned certain recently emerged global disinformation actors and are disrupting the traditional hegemonies over the international narrative.

As well as digitalisation processes, the COVID-19 pandemic also accelerated what Josep Borrell, the EU's High Representative for Foreign and Security Policy, calls a «global battle of narratives», further fuelling the sense of Western vulnerability. It is not a new sensation. For over a decade, the digital world had been shaking the structures of the post-1945 order. In 2011 then Secretary of State Hillary Clinton warned the United States Congress that her country was immersed in «an information war and we are losing». Clinton was referring to the global presence of RT (Russia Today), China's CCTV (launched in 2009) and the power Al Jazeera demonstrated when covering the Arab Springs. The Global South had its own narrative about the transformations challenging traditional power structures and longstanding instruments of US soft power like CNN were losing global presence. Ironically, Clinton's White House candidacy ended up falling victim to this information war and the central role online tools and discourse played in deciding the outcome of the 2016 US elections.

Since the pandemic infodemic broke out, the magnitude and speed of this transition have increased the feeling not only of vulnerability but of both the United States and the European Union losing influence, as they have felt compelled to rethink their roles amid the new dynamics of political and technological power.

The internet has been the great multiplier of this process of hegemony loss in the global discourse, as the United States must face its own tactics being deployed by Russia and China, the new political, economic and security allies of much of the Global South. Paradoxically, the hybrid threats challenging Washington's spheres of influence are deployed via the large platforms that have globalised the power of Silicon Valley.

Through the varied ways it uses technology, geopolitics is shaping the information society. As General Slipchenko foresaw, a conflict is underway in this information space not only because of a power struggle, but because of a clash between the models that shape it. Words carry implicit mental frameworks and specific values. That is why they have become the hybrid weapon in this conflict. Disinformation provides fertile space for influence to the new state and private actors that are increasingly decisive in the power struggle underway in the new digital global order.

References

Bontcheva, Kalina and Posetti, Julie (eds.). «Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression», *UNESCO Broadband Commission Report*, September 2020.

Del Campo, Agustina. «Disinformation is not Simply a Content Moderation Issue», in *Issues on the Frontlines of Technology and Politics* (Feldstein, S. editor), pp. 23–24. Carnegie Endowment for International Peace, 2021 (online). [Accessed on 21 February 2022].

Freedman, Jane; Hoogensen Gjørv, Gunhild and Razakamaharavo, Velomahanina. «Identity, stability, Hybrid Threats and Disinformation», *ICONO 14, Revista de comunicación y tecnologías emergentes*, vol. 19, no. 1, June 2021, pp. 38–69

Han, Byung-Chul. *Infocracia. La digitalización y la crisis de la democracia*, Penguin Random House, April 2022.

Mouffe, Chantal. «Deliberative Democracy or Agonistic Pluralism», *Social Research*, 66(3), 1999, pp. 745–758.

O'Neil, Cathy. *Armas de destrucción matemática: como el big data aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing, 2016.

Snyder, Timothy. *El camino hacia la no libertad*, Galaxia Gutenberg, Barcelona, 2018.

Van Raemdonck, Nathalie and Meyer, Trisha. "Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat", in Luigi Lonardo (ed.)

Addressing Hybrid Threats: European Law and Policies, VUB, 2022.

THE «INSTRUMENTALISATION» OF MIGRATION

Migration is increasingly being instrumentalised at the European Union's external borders. In February 2020, the Turkish government sent over 13,000 people to its border with Greece. In May 2021, over two days, Morocco permitted the irregular entry of 10,000 people into Ceuta. In autumn 2021, the Belarusian regime took its turn, facilitating the arrival of thousands of people at the borders with Poland, Latvia and Lithuania. In this context, Brussels has been swift to describe thousands of people reaching its borders (families and minors included) as a serious «hybrid threat» to its «security». NATO took a similar line in its new Strategic Concept, calling the actions of «authoritarian actors» who «instrumentalise migration» attacks on states' sovereignty and territorial integrity.

Blanca Garcés Mascareñas
Senior Research Fellow, CIDOB

CIDOB REPORT
# 08- 2022

The instrumentalisation of migration is nothing new. The American political scientist Kelly M. Greenhill (2010) has called its use as a weapon of political and military warfare the «weaponisation of migration». Taking a long-term historical perspective, Greenhill distinguishes between coercive intentions, where migration is used as a foreign policy tool for applying pressure to other states; dispossessive intentions, where the aim is to annex certain territories or to consolidate power; and economic motivations, where the goal is financial gain.

In the instances mentioned above, the intentions of Turkey, Morocco and Belarus are clearly coercive: migration is instrumentalised in order to force change and obtain concessions from the EU. The Turkish President Recep Tayyip Erdoğan sought increased financial aid for hosting refugees and support for Turkish military operations in northern Syria. Morocco was responding to what it saw as an act of disloyalty – the hospitalisation in Spain of Brahim Ghali, leader of the Polisario Front – and ultimately demanded collusion on the issue of Moroccan sovereignty in Western Sahara. Belarus, with Russian backing, pressured the EU not to meddle in its internal affairs.

Each time, the EU is aghast at these instances of «blackmail». On the one hand, it blanches at the «outrageous», «cynical» use of refugees for political purposes by third countries. On the other, it has no compunction about describing the arrival of thousands of people (including families and children) as a serious «hybrid threat» to its «security», against which it is consequently «at war» in both rhetoric and the deployment of national armies at the border. The EU has responded with force and even a rarely seen unity, not realising that in the end it is the victim of little more than its own actions. This is true in several ways.

First, the EU is a victim of its own actions because it overreacts. As it fears nothing more than another «migration crisis», the blackmail is guaranteed to succeed. In the end, the number of people is not what counts. What really matters is fear: the fear some parts of the electorate feel about migrants, and governments' fears of the division and chaos the EU and the member states display on each occasion. Some experts have claimed that Russia's invasion of Ukraine also sought to destabilise the EU with a new «wave» of refugees. This time, however, despite the numbers reaching millions rather than thousands no overreaction occurred. The proximity of the refugees and, above all, a war experienced as its own (with a perceived common enemy) are the reasons this unconventional tactic has failed this time.

Second, the instrumentalisation of migration is really the result of outsourcing migration control and international protection to neighbouring states. By forcing them to control the bloc's borders and take in the refugees they were no longer willing to receive, the EU and its member states placed their fates in their neighbours' hands. In exchange for control and containment, they offered incentives, from development aid funds to potential trade and visa agreements. Now the neighbours are the ones seeking to impose their conditions. Few wishes to admit it, but it was the EU, and the member states themselves that first instrumentalised migration. And the ways they went about it are far from trivial.

Over recent years, the EU has been resorting to increasingly informal solutions. Bilateral agreements have given way to other more flexible and ad hoc forms of agreement, which are inserted into broader cooperation frameworks. Unsurprisingly, these negotiations have been carried out mainly at member state level – at the EU level any measures tend to be much more standardised. The result is increased flexibility and bargaining power at the expense of transparency. This should not negatively impact the necessary oversight by each country's legislative and judicial authorities, or those at European level. The misnamed EU–Turkey deal of 2016, which was meant to curb irregular arrivals to Greece, provides the best example of the risks of this informality. When asked to assess the deal's legality, the Court of Justice in Luxembourg declared that it lacked the jurisdiction to rule on an informal pact between Turkey and the member states.

Third, and finally, the EU has only itself to blame when, for all these reasons, it is willing to abandon its own core principles. Declaring war in response to neighbouring countries' instrumentalisation of migration (understood as hybrid tactics) opens the door to exceptions. In late 2021, Poland declared a state of emergency, with all that implies in terms of suspending fundamental rights, unlimited use of force by the army and the militarisation of large areas to which press and NGOs were denied access. The same happened with push backs in Greece, which flagrantly violate the law and have been a constant in recent years. On each occasion, the political use of migration by third countries has been used as a justification to limit fundamental rights recognised in domestic, European and international law.

VIEWING MIGRATIONS AS HYBRID THREATS ORCHESTRATED BY THIRD COUNTRIES HAS PROVIDED THE PERFECT BACKSTORY. EVEN IF MIGRANTS ARE PERCEIVED AS VICTIMS, THEIR ROLE AS PRESSURE «WEAPONS» IN THE HANDS OF NEIGHBOURING STATES' GOVERNMENTS SIMULTANEOUSLY MAKES THEM THE MAIN ENEMY.

This shift is not only taking place in certain border countries. In December 2021, the European Commission published a proposed regulation to provide member states with a legislative framework to respond to such situations. According to this document, the instrumentalisation of migrants is when a «third country instigat[es] irregular migratory flows into the Union (...) where such actions are indicative of an intention of a third country to destabilise the Union or a Member State, [and] where the nature of such actions is liable to put at risk essential State functions, including its territorial integrity, the maintenance of law and order or the safeguard of its national security». The proposed remedies include limiting border crossings, extending deadlines, increasing immigration control measures, and facilitating immediate returns at the EU's external and internal borders. As numerous international organisations (ECRE, Amnesty International, among others) have pointed out, such measures could normalise the state of emergency and thus undermine the fundamental rights of migrants, refugees and asylum seekers.

What are the consequences of viewing migration as a hybrid threat? In *After Europe* (2017), Ivan Krastev points out that migration crises may well end up signifying the beginning of the end of European liberalism, not because of what they are but because of what they produce. Since 2015, our fear of another migration crisis has made us willing to accept the unacceptable. That is the real problem. Internally, we could end up accepting the normalisation of states of exception and, therefore, the violation of fundamental rights. In this sense, viewing migrations as hybrid threats orchestrated by third countries has provided the perfect backstory. Even if migrants are perceived as victims, their role as pressure «weapons» in the hands of neighbouring states' governments simultaneously makes them the main «enemy». The number of migrants is not the important part. As long as they are perceived as a national security threat – more for what they represent than for what they are – few question that the response should be as forceful as possible.

Externally, the instrumentalisation of migration, first by Europe and now from abroad, has left us hostage (and therefore mute) in the face of pressure from third countries. This, above all, is the source of the surprise and fear. This is perhaps what is truly new. Thus, the power asymmetry – or conditionality in the words of Cassarino (2007) – has been reversed: neighbouring countries are now the ones imposing their conditions. Simply put, this is because the number of irregular arrivals depends on them. The most recent example of this subordination is the Spanish government's recognition of Moroccan sovereignty over Western Sahara. It is worth asking to what degree this was the ultimate goal of Moroccan cooperation. In complex regional settings an added problem is that responding to the demands of some may mean raising the suspicions of others. This is why Algeria issued a response to the Spanish government's changed position without delay. Not only is it difficult to decide upon the order of priority – Morocco or Algeria, migration or the price of gas – but also migrations are fluid and those who do not reach one shore will surely end up reaching another.

This does not mean there is no alternative. There is, but the baseline conditions must be altered. This means that the habitual overreaction must cease. The Ukraine refugee crisis is a good example in this regard. It also means that the process of outsourcing migration control should be reversed, so that migration ceases to be a bargaining chip in international relations. We need a foreign policy that is not purely transactional, that does not impose the interests of some upon others and that works towards achieving common goals in the medium and long term. We also need migration policies that address causes and regulate flows, beyond mere containment measures. If not, the policies will always be doomed to fail, because containment only reduces arrivals for a given time and space. When the push and pull factors that drive migration remain in place, a route always emerges. Finally, the alternative solution cannot be to reduce the rights of those who, despite everything, end up arriving. This is for two fundamental reasons: because compliance with the rule of law is a *sine qua non* condition for any democracy; and because today's exclusion is tomorrow's conflict. Contrary to the arguments of the far right, «our» security depends on «their» rights.

References

Cassarino, J. P. «Informalising Readmission Agreements in the EU Neighbourhood». *The International Spectator*, vol. 42, n. 2, (2007), 179–196 (online). [Accessed 09 August 2018]: https://halshs.archives-ouvertes.fr/hal-01232695/document

Greenhill, Kelly M. *Weapons of Mass Migration: Forced Displacement, Coercion, and Foreign Policy*. New York: Cornell University Press, 2010.

Krastev, Ivan. *After Europe*. Filadelfia: University of Pennsylvania Press, 2017.

HOW DEMOCRACIES CAN OVERCOME THE CHALLENGES OF HYBRID WARFARE AND DISINFORMATION

Disinformation has become a daily threat in an interconnected world, even if its effects can be broadly misunderstood due to a lack of tools with which to measure its impact. Central to the challenge is that, as our world has changed, many of the institutions we rely on to keep us protected have stayed the same. In this chapter we will consider how the notion of «democracy» can survive in this new digital world and offer recommendations on how institutions can adapt and grow. In addition, we seek to define new ideas around the measurement of both the spread and impact of disinformation.

John
Kelly
Visiting Fellow,
The German
Marshall Fund

CIDOB REPORT
# 08- 2022

The new war is everywhere

Over the past handful of years, new terms have appeared to describe the sense of a constant state of conflict across the world: hybrid warfare, cyber war, grey-zone conflict, misinformation, disinformation, malinformation, influence operations and malicious actors. They are just a few of the new phrases that have worked their way into the lexicon of conflict conversation in an attempt to define the new, relatively nebulous conceptions of confrontation between states that has begun to be the norm in times of peace. Most fall within the idea of «hybrid warfare».

Peace, as we know it, may be described as an absence of war. At the same time, war, in our traditional conception, is a conflict that becomes kinetic in nature, involving weapon strikes, troop commitments and armed conflict; but hybrid war has been changing our idea of peace time. According to NATO, hybrid war obscures «the line between war and peacetime» while increasing ambiguity and vagueness on where possible hybrid attacks originate from by fusing unconventional as well as conventional tools of power, blurring the threshold of war (see Bargués & Bourekba, this volume).

Though not defined in such terms, the idea of hybrid war is as old as the well-worn pages of Sunzi, who wrote that the skills of warfighting could be encompassed in the idea of subduing «the enemy without fighting» (see Arco Escriche, this volume). Though this passage tends to be interpreted as suggesting that politics and other means should avert war, the idea of continuing or beginning a conflict outside of a kinetic battle has persisted throughout time.

In *The Road to Unfreedom*, Timothy Snyder (2018) noted that a risk with categorising hybrid warfare is that, due to its unconventional and non-kinetic nature, the confrontation can be perceived as «war minus» or less than a *normal* war. Snyder argues that this should really be seen as a «war plus» as it creates an environment of ongoing fight even without a kinetic element (Snyder, 2018: 157).

All these different notions of hybrid warfare give strong places to start on defining a purposely vague concept. In simple terms, hybrid warfare could be considered as the aggression from one entity (be it a state or faction) toward another with the use of non-kinetic tools of power with the intention of creating a strategic outcome. However, more work is needed to comprehend what hybrid war is in its current state. In particular, it should be important to delve into the factors defining when a state can consider itself *in* a hybrid war, what form the response should take, and if there are certain parameters that escalate conventional statecraft or power exertion between states into a hybrid war.

Disinformation as a threat

Hybrid warfare is like an octopus where every tentacle is a new, unconventional warfare tactic. But this octopus' strongest tentacle is harnessing information as a weapon. As hybrid warfare has become more common, there has been a marked increase in the spread of what is categorised as misinformation, disinformation and malinformation (MDM). According to the United States Cybersecurity & Infrastructure Security Agency (CISA), the differences between these terms are slight but important to understand. *Disinformation* is information created deliberately to «harm, or manipulate a person, social group, organization, or country», while *misinformation* is false information created without intent to harm. Finally, *malinformation* is using truthful information out of context in order to mislead. But the star of these tactics is disinformation.

Disinformation has been a growing threat in the past decade, as social media platforms continue to expand largely unchecked and dominate the news. But as disinformation grows, so do our strategies to quantify and battle it, and there are steps that can be taken to mitigate its effects.

Traditionally, we have identified and measured disinformation by focusing on the «production» side of disinformation; or on how much content has been created, «published, shared, or viewed»; or on metrics such as how many bots can be identified on Twitter. While these measures are effective for identifying sources of disinformation, they do not measure the impact of the information being pushed. While both metrics are important to measure, it is crucial to understand the efficacy of these campaigns.

DISINFORMATION HAS BEEN A GROWING THREAT IN THE PAST DECADE, AS SOCIAL MEDIA PLATFORMS CONTINUE TO EXPAND LARGELY UNCHECKED AND DOMINATE THE NEWS. BUT AS DISINFORMATION GROWS, SO DO OUR STRATEGIES TO QUANTIFY AND BATTLE IT, AND THERE ARE STEPS THAT CAN BE TAKEN TO MITIGATE ITS EFFECTS.

On the production side of disinformation, the European Union approved in April 2022 a new legislative package to strengthen EU's response to disinformation: the Digital Markets Act (DMA) and the Digital Services Act (DSA), that includes an updated Code of Practice on Disinformation which aims to tackle the spread of disinformation across technology platforms by making the platform owner (such as Meta, Twitter, etc.) liable for not curbing the spread of disinformation at its root. The Code approaches this by increasing reporting requirements by «very large online platforms» on their work countering disinformation, promoting fact-checking, increasing transparency in political advertising, and more. The penalties for not abiding by these rules may lead to fines of up to 6% of yearly global revenues.

Beyond this effort to create a regulatory framework that places certain limits on the phenomenon, new analytical measures are also advancing to increase knowledge about how disinformation spreads, as well as its social and political effects. One effective proposal for analysing the impact of a disinformation campaign is to measure whether, in the long run, this misleading content eventually leads to action, or if the content breakouts from the platform where it originates to be disseminated through other channels. Ben Nimmo, in a report for Brookings, has worked to create a «breakout scale», which measures the impact of a piece of disinformation. This scale ranges from one to six, measuring if the disinformation leaves a single platform, if it jumps between different media sources, if it becomes amplified by celebrities and, finally, if it calls for action, violence, or policy measures. Working in concert with metrics to measure the root source of disinformation, this scale can help researchers understand the what, where, who and how by which disinformation takes root and spreads. But, all of these measures are for naught if they do not rebuild confidence in our democracies. The problem with disinformation is its potential for the erosion of democracies, but there are ways to combat this.

How does democracy survive in a world of hybrid threats?

Hybrid warfare and disinformation weaken the bases on which our democracies stand and violate the principles and rights upon which they were founded. That is the point of these tactics. But the threats have become so complicated that a fundamental question arises: Does democracy need to be rethought as a concept? Simply put: no, it doesn't. However, democracy, institutions and regulations do need to be revised to be still relevant in the digital era. Just as religious texts are interpreted for modern days, democracies must be interpreted and grown if they are to remain powerful enough entities to protect those inside of them. When it comes to regulating the tech industry to protect from disinformation campaigns, there are multiple steps that can easily be taken to create change right now.

Until 2014, Mark Zuckerberg's mantra for Facebook was the well-known «move fast and break things». This saying meant to give Facebook's developers and managers free reign to try, build and fail, and it was appropriated across Silicon Valley. Many tech companies like Uber and WeWork attempted to replace things like taxis and offices, and the results were mixed at best. What moving quickly and breaking things often lacked was oversight or thought about how new solutions could be misused.

Even if Zuckerberg's mantra might have worked as a mindset for the tech industry, it could not be more antithetical to the slow, methodical and deliberative ideals of democracy. Democracies were designed from the outset to incorporate checks and balances meant to moderate their actions in order to make well-informed decisions to serve the people. This process was not meant to be fast or destructive. Faced with competition from an industry which can build totally new technologies in days, democracy finds itself unevenly matched.

Democracies are as relevant today as they were when the first democracy was born in Athens thousands of years ago. But many are still working under the strict precepts of their founding documents, having not thought to update themselves for a totally different world. In the United States, for example, the country was founded with what was seen as a «Living Constitution», meaning that it should be updated as the world changes – other states have also included this idea in their founding documents. But practice has proven to be a different matter in both the United States and other countries. As Walter Lippman wrote in 1919, democracies are influenced by the information available to them and must work to «control their environment» – this includes new information environments.

However, democratic regimes tend to be reactive instead of proactive, and it has taken nearly three decades to see strong regulations created to rein in this new tech world. Generally, democracies step in when a new sphere of influence becomes dangerous. In the United States, when the automotive industry began to grow unchecked, the National Highway Safety and Traffic Administration was created in 1970; and when pollution began to spread unrestricted across the country with the creation of the Environmental Protection Agency, also in 1970. When we look at the spread of disinformation, it is clear that the tech industry has become dangerous, and it is high time to take measures to make sense of the situation.

Nowadays, given the disruptive capacity of disinformation, amplified by the technology industry, the time has come to take measures to counter risks. Today, Mark Zuckerberg, the original advocate of moving fast and breaking things (who has since updated his motto to "move fast with stable infrastructure"), says that the government needs a more active role in regulating the internet and has put forth four simple regulations that could make social media and the internet a safer place: a) regulating harmful content, b) ensuring election integrity, c) privacy controls and d) data portability. Adopting these concepts would create a safer online environment.

The European Union is blazing a path ahead on creating a safer environment online with the above mentioned Digital Markets Act and Digital Services Act. The adoption of the DMA and DSA frameworks by major allies of the European Union would ensure consistent global regulation that helps prevent online pockets where bad actors can operate. Finally, 61 nations have signed the Declaration for the Future of the Internet proposed by the Biden administration, which sets out a global vision for the internet in which human rights are protected, competition is moderated, infrastructure is secured, and universal access is granted, among other topics. This document could be a strong first step towards achieving these goals if the signatories would ensure that they abide by these rules, and if this document were created as an agreed-upon legal framework instead of its current state as a nonbinding agreement.

As discussed, there are numerous ways democratic institutions can survive and grow in the current environment. First, stronger definitions of hybrid warfare and parameters on what constitutes *being* in a hybrid conflict would cut through the vagueness that these tactics seek to create. Next, using data to measure the effectiveness of acts within conflicts, such as the spread of disinformation, can help gauge risk and reaction. Finally, implementing updated rules and regulations can help safeguard the public and give institutions the latitude they need to work in a new world of threats. Democracies were created to grow and adapt, and it is high time they do.

References

Bilal, Arsalan. «Hybrid Warfare – New Threats, Complexity, And 'Trust' As The Antidote». *NATO Review*, November 30 2021 (online). [Accessed on 28.07.2022]: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Engler, Alex. «The Declaration For The Future Of The Internet Is For Wavering Democracies, Not China And Russia». *Brookings*, May 6 2022 (online). [Accessed on 28.07.2022]: https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/

Lippmann, Walter. «The Basic Problem Of Democracy». *The Atlantic*, November 1919 (online). [Accessed on 28.07.2022]: https://www.theatlantic.com/magazine/archive/1919/11/the-basic-problem-of-democracy/569095/

Nimmo, Ben. «The Breakout Scale: Measuring the Impact of Influence Operations». *Brookings Foreign Policy*, September 2020 (online). [Accessed on 28.07.2022]: https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf

Snyder, Timothy. *The Road to Unfreedom*. United States: Crown, 2018.

Sunzi. *The Art of War*. Capstone Publishing, 2010.

HYBRID ATTACKS ON CRITICAL INFRASTRUCTURE

Cyberspace is the latest battlefield for exploiting a supposed enemy or rival's known and, above all, unknown vulnerabilities. Cyber weapons are malicious computer programmes designed to attack an essential cyber-physical system in order to disrupt its normal operation or destroy it. Unlike manufacturing conventional weapons of war, these types of attack on critical infrastructure do not require multimillion dollar investments and their ability to be replicated is highly effective. But how are they produced? Who makes them and how are they distributed? Who do they serve? And how can we defend ourselves?

Manel Medina Llinàs
Director of the Master's in Cybersecurity Management at UPC-School, and Coordinator of the Technical Training Office of the Catalan Cybersecurity Agency

Some years ago, orbital space joined the traditional battlefields of land, sea and air; more recently, the talk is of cyberspace. In traditional settings, weapons can be seen from planes and satellites, and states and large coalitions like NATO have a good handle on what the other side possesses. But cyberweapons are almost intangible and data networks have removed the need even for a memory chip to cross a border. In the event of a cyber war, this makes establishing an opponent's destructive capacity tricky.

Let's start by establishing what a cyberweapon is. Until less than a decade ago, any malicious computer programme capable of attacking our enemy at any time was considered a cyberweapon. In order to avoid detection and being rendered useless before being deployed, the attack is normally based on one or more methods of exploiting a vulnerability in a programme installed on the victim's computer systems, known as a zero-day vulnerability. Purists would say that for something to be considered a cyberweapon it must be «destructive», in other words, it must cause material damage to critical infrastructure and/or people. Hidden cyberweapons must therefore be sought out in so-called cyber-physical or internet of things (IoT) apparatus like industrial control systems (ICS), railways, telecommunications, essential utilities (water, electricity, gas) and health infrastructure, among others. Along with the fact that many of these systems are not properly updated, this means they can even be attacked via known vulnerabilities.

An accessible and persistent threat

Many cyberweapons aim to remain hidden and unnoticeable as they await the order to destroy the target. This is what is called an advanced persistent threat (APT). In many cases, it is even difficult to identify the development team. The most powerful include military and government cyber-intelligence units, but, as with their physical equivalents, cyberweapon manufacturers exist – criminal organisations that sell them on more or less hidden markets. The Israeli company NSO, which has recently become more widely known, sells cyberweapons like its Pegasus spyware to states, theoretically to support the fight against terrorism.

To identify cyberweapons, we must look beyond cyber warfare and search in surveillance and biometric identification tools, for example, which can impact the supply chain and potentially collect user and citizen data.

This is an «affordable» type of threat that does not need the multi-million dollar investment required to manufacture war equipment and weapons. Discovering new vulnerabilities and developing tools to exploit them is much cheaper. Above all, these weapons can be replicated hundreds or thousands of times at hardly any additional cost. They can be developed by *grey* organisations, which then market them to governments, openly, and to criminal groups in a more covert way.

But, the catalogue of cyberweapons may also include an apparently less bellicose tool: disinformation, which can also be used to attack critical infrastructure. Using conventional information channels (social networks, media, etc.) disinformation selectively targets people with infrastructure management capacity and may be complemented by cyber-(counter) intelligence. The spy software used by intelligence departments may also be attacked, leading it to generate false information about the enemy and prompting decisions that can lead to a trap that is difficult to escape, blocking the infrastructure or causing control of it to be lost. But the most common use of disinformation as a form of attack in cyber-physical environments is altering the data provided by physical systems sensors. The aim is to provoke erroneous reaction decisions in infrastructure management systems, such as, for example, attempting to correct a non-existent problem and thereby creating another, inverse, problem that goes undetected. This is what happened in the Stuxnet attack, where a virus (cyberweapon) destroyed Iranian uranium centrifuges, while avoiding detection by changing the revolutions per minute data recorded to show normal levels. There are several ways to achieve this sensor data modification: a) by substituting or introducing a fraudulent sensor; b) by altering the sensor's software to make it give false readings; or, c) by modifying the data stored in a server or cloud. If the data transmission, storage or processing is not adequately protected, it is very easy to alter it without it being noticed, until the damage is irreparable or unavoidable.

Cyber weapons can be hidden anywhere: a chip, a programme, a memory card, or stored in the cloud. A cyberweapon is made up of «bits» that can be hidden in multiple ways and are therefore undetectable. They may remain dormant for years in an energy production plant, a railway or air traffic control centre, or in the office of a government official or manager without anyone noticing. The 2014 Mandiant report warned of this, revealing dozens of organisations that APT1, a Chinese cyber espionage software development team, had targeted and entered, remaining hidden from its victims for an average of 229 days, and in some cases being installed for years (McWhorter, 2021).

In a cyber war, the computers or devices that control a country's infrastructure are invaded. But we are unaware of them until someone «presses the button» that wakes up the agents (malicious programmes) asleep in their hideouts, which then begin to act, bringing the infrastructure that keeps the country running to a halt.

CYBER WEAPONS CAN BE HIDDEN ANYWHERE: A CHIP, A PROGRAMME, A MEMORY CARD, OR STORED IN THE CLOUD. A CYBERWEAPON IS MADE UP OF «BITS» THAT CAN BE HIDDEN IN MULTIPLE WAYS AND ARE THEREFORE UNDETECTABLE. THEY MAY REMAIN DORMANT FOR YEARS IN AN ENERGY PRODUCTION PLANT, A RAILWAY OR AIR TRAFFIC CONTROL CENTRE, OR IN THE OFFICE OF A GOVERNMENT OFFICIAL OR MANAGER WITHOUT ANYONE NOTICING.

Hybrid conflict is warfare with an added layer of remote operations. Unlike conventional warfare, where the invading army can be seen on the streets, preparations for a cyberattack are imperceptible because there are no troop movements across any borders. In cyberspace there are no borders.

The danger of cyberweapon proliferation

Having established the scenario and the weapons, we shall now look at the dangers these new cyber threats pose and the factors that make them attractive and dangerous.

The cyber war is already underway: cyberweapons are being deployed on the internet even if we cannot see them. Weapons more powerful than missile launchers and tanks are being marketed, inadvertently to most citizens and countries because they are just data bits. As with traditional weapons, there are «legal» purchases made by governments and other «illegal» purchases made by individuals or criminal groups with an interest in spying on a commercial or strategic rival in order to supplant them, or to take control of infrastructure or destroy it, as BlackEnergy did on December 23rd 2015, when it shut down and destroyed the control programmes of Ukrainian power plants.

Cyber weapons can be produced by cyber-mafias, by the cyber units of conventional armies or governments, or by companies working on their behalf. Of particular concern to states is that designing and building a cyberweapon is within the reach of any small country or organisation, as the production requires no expensive raw materials. Hybrid warfare is thus preferable to traditional warfare because it is more profitable. Russia and other European countries distribute this type of cyberweapon, which is often produced in public–private collaboration projects. The tools are often produced by governments and large multinational organisations, although the supply chain has not yet been analysed.

In general, when a hybrid cyberattack takes place, we don't know who ordered it, who perpetrated it or when preparation for the attack began. In some cases, however, it is very clear who is responsible. Following the presentation at the 2016 Berlinale of Zero Days, a documentary on the Stuxnet attack, the United States and Israel were condemned for coordinating the cyberattack to destroy Iranian uranium enrichment centrifuges – although neither country accepts responsibility. In other cases, allocating blame is more difficult. The war in Ukraine has also been waged in cyberspace and both sides have accused the other of false flag attacks. For example, in the attacks on Ukrainian government web services in January 2022, the attackers left false leads that framed Ukrainian and Polish dissidents as a way to divert attention from Russia as the attacker. Determining the origin of an attack is therefore essential.

In order to establish the perpetrator of a cyberattack, the cyberweapon's code is analysed for comments or names that may indicate the country or language used by the developer. But the developer may know about this technique and leave false clues in the target's language in order to simulate a false flag attack. To further complicate matters, the developer may not attempt to hide their identity or ideology, but the actual attacker may be a different entity to the developer if the tool has been sold on the black market. Another technique for detecting the attacker is to examine the origin of the attack. But these clues may not be conclusive either, as intermediate servers can be used to conceal the origin of the attack, such as those on the Tor network. Everything discussed so far opens up a multitude of attack strategies at various levels and requires the deployment of defence strategies based on «mistrusting everything».

Defence strategies against hybrid attacks

Two main types of hybrid attack can be identified: a) those related to (dis) information, which aim to provoke decision-making errors; and b) those that directly affect physical systems.

Analysing public disinformation activities like the fake news that circulates on the internet and influences public perceptions and opinions may lead us to conclude that their success in sowing social destabilisation can be more effective than even attacks on infrastructure control databases. Disinformation can provoke violence, and is another way of starting conflicts or attacks on infrastructure.

HYBRID WARFARE IS PREFERABLE TO TRADITIONAL WARFARE BECAUSE IT IS MORE PROFITABLE.

Disinformation attack strategies are based on the creation and subsequent distribution of news through networks of influential or fake users (social bots) in order to increase their spread among bubbles of like-minded users. In order to defend against this type of attack the distributors of fake news must be identified and blocked; however, social network administrators are not always willing to collaborate, due to the potential advertising revenues associated with these types of dissemination campaigns.

Meanwhile, direct hybrid attacks against critical infrastructure from cyber-space raise the problem of a lack of experience among those responsible for physical security, a lack of collaboration among employees, and managers' lack of conviction about conceiving, planning and implementing appropriate cyber protection measures.

NATO countries declared their readiness to respond to cyberattacks in July 2021, but they are failing to properly take Russia's hybrid attack activities into consideration. For example, the disruptions to the Colonial Pipeline, the largest fuel pipeline in the US, the 2020 hacking of SolarWinds, the provider of widely used infrastructure system management tools, and widespread ransomware attacks on other NATO countries were all orchestrated by Russia, either directly or through cyber-mercenaries, and yet the Atlantic Alliance has yet to react. One reason may be the European Union's new NIS 2.0 Directive, which describes how to deal with cyberattacks, clearly differentiating between critical and essential services, and emphasising that only the latter should be considered a defence matter.

In short, governments are taking administrative and legal steps to promote cyber protection, above all in relation to essential and critical infrastructure and its providers, and throughout the supply chain of essential components for their service. Those managing this infrastructure must identify which services and assets are most valuable and which are most vulnerable, in order to protect them as efficiently as possible. And, finally, it will also be necessary to plan the operational maintenance of the installed protection mechanisms and properly train all the personnel involved. The proper functioning of states depends on it. Rebuilding after a wide-ranging cyber-attack (cyber war) may be relatively quick, but a hybrid attack can be more difficult to recover from, especially if damage to infrastructure is irreparable and rebuilding requires components that are expensive or hard to find on the market.

Reference

McWhorter, Dan. «APT1: Exposing One of China's Cyber Espionage Units». *The Mandiant Intelligence Center* (2021) (online) https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

HYBRID RESILIENCE IN INSECURE TIMES: RUSSIA'S WAR AND UKRAINIAN SOCIETY

Two broad conclusions may be drawn from the ongoing war in Ukraine: on the one hand, Russia's abilities to wage a hybrid war were overrated and most of the non-military components of Russian power turned out to be deficient; on the other hand, the scale and scope of Ukraine's ability to resist the aggression was underestimated. This resistance is built through a combination of multiple forms and practices of resilience as societal characteristics of self-help, self-reliance and self-organisation, which are distinct from the top-down emergency governance response. This «hybrid resilience» is grounded in a decentralised form of governance, sustainability of societal networks, reliable information policy and strong public adherence to the idea of a «just war».

Yulia Kurnyshova
Postdoctoral Researcher, Austrian Institute for International Affairs

Andrey Makarychev
Associate Researcher, CIDOB; Political Science Professor, University of Tartu (Estonia)

CIDOB REPORT
# 08- 2022

Since 2014, Moscow has attempted to integrate hybrid tools into its anti-Ukrainian policy. Yet, the military invasion of Ukraine has ended up with a rather traditional type of warfare aimed at the physical destruction of Ukrainian military and non-military infrastructure, rather than at diversifying policy tools to minimise the hard power component of Russia's overall strategy. The two core elements of the hybrid war concept – «non-linear warfare» and «reflexive control» – were integrated into the initial stage of the war, when Crimea was annexed and the war-by-proxies in Donbas started, but faded away in 2022. The Kremlin failed to effectively use institutional and communicative power: its wartime propaganda has only limited purchase in the Western information space; and its cyberattacks were not a game-changer and its soft power potential was destroyed by the brutality of the invasion.

At the same time the scale and scope of Ukrainian resilience was underestimated. Ukraine, which has often been perceived in the West as a weak, Russia-dependent and peripheral country that did not do much to resist the annexation of Crimea and the occupation of Donbas in 2014, has regained its subjectivity through the capacity to survive and strikeback against its more resourceful invader. We argue that hybrid resilience is the crux of Ukraine's survival as a nation via the political subjectivity and agency of its civil society, and we single out the key components of the Ukrainian model of resilience.

Resilience: The pedigree of the concept

The extant literature generally understands resilience as a process of societal adaptation to complex shocks. By and large, resilience implies adaptation, partnership and self-reliance of individuals and communities. It envisages «shifting of responsibility onto communities and promotion of reflexive self-governance through strategies of awareness, risk management and adaptability» (Humbert & Joseph, 2019: 216). «Resilient people do not look to governments to secure and improve their well-being because they have been disciplined into believing in the necessity to secure and improve it for themselves» (Reid, 2018: 648). Consequently, individuals and groups are ultimately responsible for their own adaptability vis-à-vis external transgressions, including foreign interventions.

However, we contest the opinion of authors who believe that in exceptional times resilience «discourages active citizenship» and even puts «into jeopardy the concept of public space» (Juntunen and Hyvönen, 2014: 196). On the contrary, the Ukrainian experience proves that resilience is deeply political, since it «seeks to empower people to be agents of their own vulnerability reduction in order to make the proper choices and avoid maladaptation in an emergent environment» (Grove, 2014: 244). Therefore, everyday resilience practices «create subjects» (Cavelty et al., 2015: 9): civil society organisations, grassroots groups and networks are key sources of a strategy for survival and human security.

Hybrid resilience: Ukrainian experience

Sociological data from a recent survey indicates a high level of resilience among Ukrainians[1] – 3.9 points out of a possible 5. In this rating, resilience

[1] https://ratinggroup.ua/research/ukraine/b29c8b7d5de3de02ef3a697573281953.html

consists of two indicators: physical health and psychological well-being and comfort, including interest in life, feeling of usefulness, ability to make decisions and plans for the future and lack of regret for the past. However, in thissection we look at resilience from a broader perspective and single out six key characteristics that make the Ukrainian experience of resilience during the war a hybrid phenomenon.

First, the need for resilience emerged from the sense of vulnerability vis-à-vis Russian aggression, which the country's leadership translated into a vision of self-reliance. The war in Ukraine began not on February 24th 2022, but in 2014 with the annexation of Crimea and the beginning of the Russian military infiltration of Donbas. After fighting for Ilovaisk, Donetsk airport and Debaltseve in 2014, Ukraine realized its weaknesses, creating a kind of collective trauma that was even more painful as Western countries had not yet introduced strong punitive sanctions against Russia. The restrictions imposed have neither stopped the war in Donbas nor prevented the Kremlin from further offensives, but they have in the meantime fuelled a sense of frustration with Western allies in Ukraine. The EU welcomed Ukraine's «European aspirations», yet without clear prospects of granting full membership, raising questions about the most feasible formula of partnership and the most plausible scenario of European integration in Ukraine.

Volodymyr Zelensky won the presidency because he managed to capture these widespread sentiments better than his predecessor Petro Poroshenko. Having stated that Ukraine, as a «European country», «begins with each of us», Zelensky addressed the issues of values and policy reforms without making the EU the major reference point. Much less emphasis was put on divisive issues of ethnic and linguistic identity. Zelensky's practical and pragmatic agenda found broad support across the country and clearly captured public demands for self-help and resilience.

UKRAINIAN PUBLIC INSTITUTIONS HAVE LARGELY REMAINED FUNCTIONAL DURING THE CURRENT WAR, INCLUDING IN THE REGIONS MOST AFFECTED BY RUSSIA'S MILITARY ACTIVITIES. THEIR RESILIENCE WOULD NOT HAVE BEEN POSSIBLE WITHOUT PROLONGED SUPPORT FROM THE EU, INCLUDING THE TRANSFER OF EUROPEAN GOOD GOVERNANCE PRACTICES TO UKRAINE.

Second, Ukrainian public institutions have largely remained functional during the current war, including in the regions most affected by Russia's military activities. Their resilience would not have been possible without prolonged support from the EU, including the transfer of European good governance practices to Ukraine. Decentralisation and self-governance reforms have been fundamental elements of Ukraine's engagement with foreign political and civil actors (non-governmental and educational organisations, think tanks and the media), which have had a visible impact on Ukrainian decision-makers. In particular, the COVID-19 pandemic has added a great deal to Ukraine's preparedness for future challenges, including the growing ability of regional and municipal public authorities to perform their functions remotely under the strict conditions of supervision and control.

SOCIAL NETWORKS AND CIVIL SOCIETY HAVE BEEN ESSENTIAL TO RESILIENCE AT THE LOCAL LEVEL. IN THE EARLY STAGES OF THE RUSSIA INVASION, THERE WAS A HEAVY RELIANCE ON NGOS AND FIRST-TIME RELIEF ACTORS, SUCH AS VOLUNTEERS, RATHER THAN ON THE CENTRAL GOVERNMENT. MOREOVER, UKRAINIAN NGOS HAVE OFTEN SUBSTITUTED FOR INTERNATIONAL ORGANISATIONS AND HAVE DELIVERED AID TO THE BESIEGED CITIES OR FACILITATED THE EVACUATION OF CIVILIANS.

Third, the war displayed mechanisms through which social capital and family networks become helpful elements of hybrid resilience. These mechanisms include the elimination of barriers to collective action, as well as the provision of informal assurance and mutual aid. Ties between relatives, neighbours and communities serve as a critical engine in resilience-building and, according to a survey, 94% of respondents claim to have peaceful relations within their families, 89% with neighbours and 67% with strangers. Members of large families from the war-torn regions have found refuge in the western part of Ukraine. Neighbourhoods where residents relied on mutual help and assistance were better able to overcome shared problems (such as looting) and the likelihood was higher of displaced persons' eventual return to their homes. These practices of grass-roots resilience are substantial components of Ukraine's development as a modern networked open society where the middle class has proven capable of taking social and financial responsibility in previous crises, including the Maidan revolution, and nowadays in the war with Russia.

Fourth, social networks and civil society have been essential to resilience at the local level. In the early stages of the Russia invasion, there was a heavy reliance on NGOs and first-time relief actors, such as volunteers, rather than on the central government. Moreover, Ukrainian NGOs have often substituted for international organisations and have delivered aid to the besieged cities or facilitated the evacuation of civilians. Most national and local NGOs, religious networks, civil society organisations and a considerable number of newly emerged volunteer networks are providing vital humanitarian aid in most cities affected by the war.

Fifth, information resilience matters too. The fact that the full-scale Russian invasion was preceded by a hybrid war has helped Ukraine gain some experience in countering Russian propaganda. In contrast to Russia, before the war Ukrainian media were characterised by diversity and pluralism of opinions, and since the full-scale invasion Ukraine has not introduced military censorship, although coverage sometimes suffers from over-optimism. Free online media creates opportunities for volunteers, human rights defenders and journalists to record war crimes. The high level of emotional support to – and symbolic identification with – Ukraine in many Western media serves as an additional mobilising force for domestic resistance.

Sixth, the ethical and value-based dimensions of resilience are of utmost importance: the fundamental difference is that Ukraine is waging a war of self-defence (for its survival and future), while Russia is waging an aggressive war (for expansion and to recover the past). For Ukraine, it is first and foremost a liberating and just war that mobilises and unites the nation for the sake of defending the independence of the country. For Russia, this is a neo-imperialist war aimed at restoring a bygone empire, drawing on ideas of zones of influence and great power management.

The EU's role

The EU played a crucial role in all the six mentioned factors contributing to Ukraine's hybrid resilience after the war restarted in February 2022. This is unsurprising given that it was largely the EU that produced and promoted resilience discourses and practices towards the eastern and southern neighbourhoods. Since 2014, Western assistance programmes have been instrumental in facilitating reforms in Ukraine and creating favourable conditions for economic and social integration. The EU–Ukraine Association Agreement concluded in 2014 is the EU's most comprehensive with any third country. Ukraine has received €14 billion from the EU, an unprecedented level of financial support, which made an important contribution to the reification of resilience practices, as defined by the EU in its Global Strategy as the ability of «states and societies to reform thus withstanding and recovering from internal and external crises».

On March 18th 2020, the European Commission presented the «Eastern Partnership beyond 2020: Reinforcing Resilience – an Eastern Partnership that delivers for all», which emphasised the positive results achieved in three out of four priority areas (stronger economy, stronger connectivity and stronger society) in the work plan «20 Deliverables for 2020». As regards the stronger governance priority area, the document advocated «the need to significantly improve results» in the governance sphere connected with anti-corruption efforts and empowerment of civil society. Decentralisation and self-governance reforms in Ukraine have been among the pillars of this process. Beyond that, EU assistance is instrumental in supporting civil society, free media and grassroot activism in Ukraine. Should the EU keep prioritising the strengthening of resilience through facilitating local ownership and bottom-up engagements that encompass the whole of society, Ukraine will be on the right track for prompt post-conflict recovery based on European norms of democracy, transparency and good governance.

Resilience has become a backbone for a new Ukrainian subjectivity in Europe as a nation capable of fighting not only for its own independence and territorial integrity, but also for broader European security.

References

Cavelty, Myriam Dunn; Mareile Kaufmann and Kristian Søby Kristensen. «Resilience and (in)security: Practices, subjects, temporalities», *Security Dialogue* 46 (1), 3–14, 2015.

Grove, Kevin. «Agency, affect, and the immunological politics of disaster resilience», *Environment and Planning D: Society and Space* 32, 240–256, 2014.

Humbert, Clemence & Jonathan Joseph. «Introduction: the politics of resilience: problematising current approaches», *Resilience*, 7 (3), 215–223, 2019.

Juntunen, Tapio and Ari-Elmeri Hyvönen. «Resilience, Security, and the Politics of Processes», in *Resilience: International Policies, Practices, and Discourses* 2 (3), 195–209, 2014. DOI: 10.1080/21693293.2014.948323

Reid, Julian. «Neoliberalism, Development and Resilience», in *The SAGE Handbook on Neoliberalism*. Edited by Martijn Konings, David Primrose, Damien Cahill and Melinda Cooper, 2018.

NATO'S STRATEGIES FOR RESPONDING TO HYBRID CONFLICTS

The North Atlantic Treaty Organization (NATO) has a long relationship with the hybrid. Initially used to describe a form of warfare that incorporates both conventional and irregular elements, NATO's current conception is based on the coordinated and synchronised use of different kinds of power that remain below the threshold of conflict. Hybrid threats are now established as a danger to the allies' security. The Strategic Concept approved at the Madrid Summit in 2022 warns of China and Russia's use of hybrid threats and their effects, even to the point of potentially leading Article 5 of the Washington Treaty to be invoked.

Guillem
Colom Piella
Full Professor of Political Science, Pablo de Olavide University

CIDOB REPORT
# 08- 2022

The origins

Influenced by hybrid warfare's rising popularity as a concept in the US strategic community following the 2006 Israel–Hezbollah war, and the appointment of General James Mattis to lead the Allied Command Transformation, NATO first showed an interest in hybrid warfare in 2007. Understanding that this form of warfare, in which «adversaries integrate conventional, irregular, terrorist, and criminal assets operationally and tactically», was likely to characterise conflict in the 21st century, the allies' means and capabilities needed adapting in order to operate effectively in these more ambiguous and diffuse settings. Unsurprisingly, then, hybrid tactics were included in the 12th capabilities planning review, were introduced into military testing campaigns, and figured among the Multiple Futures Project's recommendations for long-term transformation among the allies. While NATO military command did publish a basic concept to clarify the term and guide this development of capabilities, the hybrid remained somewhat limited to the military field. This explains why, despite the «Albright Report» mentioning the hybrid on one occasion, it did not appear in the 2010 Strategic Concept. Other risks were mentioned, like terrorism, extremism, transnational crime and cyber-attacks, which had gained enormous prominence after the events in Estonia in 2007 and which would end up closely linked to the hybrid. The threat was not mentioned at the 2012 Chicago Summit either.

Despite the military interest in the hybrid, no consensus existed on the concept. In fact, the organisation's documents used war, threat, strategy and tactics interchangeably to refer to the complexity of 21st century conflicts. A political–military organisation like NATO was unprepared for such conflicts and had to address them via a «comprehensive approach» that would increase coherence between allied military actions and the civilian work of other actors in crisis management operations. In fact, many saw the intervention in Libya (2011) as an example of a conflict taking place outside the regular/irregular dichotomy (with government forces, guerrillas and mercenaries operating on ambiguous fronts), whose satisfactory resolution could only be achieved through a comprehensive approach with better crisis management tools and increased capacity to provide military support for post-conflict stabilisation and reconstruction.

The hybrid emerges

It was not until Russia's annexation of Crimea (2014) that public opinion and the political classes in NATO countries began to pay attention to hybrid threats. An astonished international community watched on as unmarked military units and local actors took the peninsula. Exploiting the region's sociopolitical divisions and launching a multi-channel disinformation campaign inside and outside Ukraine, Moscow managed to conceal its objectives and plausibly deny responsibility until the invasion was complete. The Russian incursion in Donbas (2014–) confirmed this blurring of the boundaries between peace and war into a large grey zone that was a natural habitat for misinformation and cyber-attacks. Since that time, these asymmetric, ambiguous tools, which are difficult to attribute and can impact society as a whole, have been observed by both NATO and the European Union.

Events in Ukraine helped the hybrid reach the top of the allied agenda. Described by NATO Secretary General Jens Stoltenberg as «the dark reflection of our comprehensive approach» these new challenges, which employ «a wide range of overt and covert military, paramilitary, and civilian measures … in a highly integrated design», featured prominently at the Wales Summit (2014). At the meeting, it was agreed that tools should be developed to deter and respond to so-called «hybrid war threats» and to strengthen national capacities. Several of the initiatives set out there – reinforcing strategic communication, conducting exercises with hybrid scenarios, improving coordination with other organisations and drawing up a plan to counteract them – would be consolidated later. NATO's Strategic Communications Centre of Excellence, established in Riga in January 2014, became one of the organisation's pillars for combating disinformation and propaganda. Some months later, the first exercise began with a scenario that included hybrid threats in order to train allied politicians, officials and military personnel in these ambiguous situations that have the potential to paralyse decision-making. Many of those will end up benefitting from EU participation and this will become a key area of cooperation between the two organisations.

LIKE CYBER-ATTACKS, HYBRID STRATEGIES ARE AMBIGUOUS IN ORDER TO HINDER DETECTION AND ATTRIBUTION. THEY OPERATE BELOW THE VICTIM'S RESPONSE THRESHOLD. THE AFFECTED COUNTRY MUST ALLOCATE RESPONSIBILITY (ALTHOUGH IT CAN BE COMMUNICATED JOINTLY) AND ASSESSMENT IS MADE ON A CASE-BY-CASE BASIS. IT MAY THEREFORE BE DIFFICULT TO REACH THE CONSENSUS REQUIRED TO INVOKE ARTICLE 5.

In 2015, NATO presented its strategy for countering hybrid threats. Intended to guide its political and military efforts to combat hybrid threats, it was articulated around preparedness (identify, assess, communicate and attribute any activity in the grey zone), deterrence (strengthening allied societies' resilience, adapting the decision-making process and improving enlistment to reduce the impact of these threats, and increasing allied response options), and defence (increasing allied response capacity).

These initiatives were ratified and expanded at the Warsaw Summit in 2016. Describing hybrid warfare as «a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary and civilian measures … employed in an integrated manner by states and non-state actors to achieve their objectives», several agreements were reached. First, that the resilience of members' societies and infrastructure must be improved in order to reduce areas of exposure to hybrid strategies and to increase deterrence by denial. As with cyber defence, this is the member states' responsibility, with NATO's role to provide the necessary support. This is logical, because every society has specific vulnerabilities that each grey zone is tailor-made to exploit, and a number of these hybrid tools (information-based, economic, cultural, legal, environmental, etc.) lie beyond the scope of NATO action. In any case, in 2018 anti-hybrid support groups were formed to provide technical assistance to countries – like Montenegro in 2019 – that need to prepare for or respond to hybrid threats.

Second, it was declared that a hybrid act may prompt the invocation of Article 5 of the Washington Treaty, under which an attack against any member of NATO is an attack against all. While this decision strengthens mutual defence, enables deterrence via punishment and increases the credibility of the process by altering the adversary's strategic calculations, implementing it may be more complicated than seems at first glance. Like cyber-attacks, hybrid strategies are ambiguous in order to hinder detection and attribution. They operate below the victim's response threshold. The affected country must allocate responsibility (although it can be communicated jointly) and assessment is made on a case-by-case basis. It may therefore be difficult to reach the consensus required to invoke Article 5. Instead, the consultation mechanism in Article 4 may be used, which allows any NATO member that believes its territorial integrity, political independence or security to be under threat to initiate a round of consultations with the other allies. Another factor is that NATO lacks the non-military tools to be able to give a gradual response, reducing its range of responses to hybrid attacks.

PREPARATION, DETERRENCE AND DEFENCE AGAINST THE COERCIVE USE OF POLITICAL, ECONOMIC, ENERGY OR INFORMATION TOOLS BY STATE ACTORS LIKE CHINA AND RUSSIA, OR BY NON-STATE ACTORS AND PROXIES, WHICH COULD PROMPT THE INVOCATION OF ARTICLE 5 OF THE WASHINGTON TREATY, HAVE BECOME ONE OF NATO'S FUTURE LINES OF ACTION.

Third on the list is collaboration with other actors facing similar problems. Since 2016, NATO has strengthened relations with Finland and Sweden (both have extensive experience countering hybrid threats using a comprehensive approach), Ukraine and Georgia (both are familiar with Russian activities that remain below the threshold of conflict), and several Indo-Pacific countries affected by China's grey zone activities. However, NATO's closest and most fruitful collaboration has been with the EU. The joint declaration signed between the organisations in Warsaw identified seven areas of cooperation, including the fight against hybrid threats, or cybersecurity and cyber defence. Since then, the two organisations have collaborated to improve issues such as situational awareness, strategic communication, crisis response, resilience and cybersecurity. While the disparity in membership, organisational cultures and available tools makes closer cooperation difficult, both bilaterally and through the European Centre of Excellence for Countering Hybrid Threats, NATO and the EU have made significant progress in detection, attribution, response and resilience in this area.

Looking towards the future

In short, between the Wales and Warsaw summits, NATO laid the foundations for counteracting these strategies. Building on previous studies on hybrid warfare, since the 2014–16 period the organisation has made significant progress in combating this threat. Detection and early warning capabilities, threat intelligence, collaboration with other actors, exchange of sensitive information between members and with the EU, flexibility of decision-making processes, crisis response, strategic communication, cyber defence, support for national resilience and adapting deterrence to these more ambiguous environments in order to monitor escalation are just a few. While the invasion of Ukraine has shown that NATO's main *raison d'être* remains the deterrence and defence of its members against conventional or nuclear threats, the protection and resilience of its societies against these much more ambiguous threats will also be a key line of future NATO action. As the comprehensive approach and the lack of specific capabilities for civilian purposes show, NATO is a politico-military organisation with a much more limited catalogue of tools than the EU. However, its ability to deliver credible deterrence and response across the high threat spectrum makes it a good complement to an EU that is able to deploy a wide range of civilian tools.

Hybrid threats were barely mentioned in the final declaration of the London Summit (2019), while the Madrid Summit in June 2022 was monopolised by the invasion of Ukraine and the Russian threat to Euro-Atlantic stability. Nevertheless, these threats and the need to counteract them also played a prominent role at the meeting and in the Strategic Concept approved. Preparation, deterrence and defence against the coercive use of political, economic, energy or information tools by state actors like China and Russia, or by non-state actors and proxies, which could prompt the invocation of Article 5 of the Washington Treaty, have become one of NATO's future lines of action. This should come as no surprise, as the coming decade is likely to bring a rise in strategic revisionism and the proliferation of grey zones in which the hybrid will continue to play a fundamental role.

References

OTAN-Allied Command Transformation. *Multiple Futures Project. Navigating Towards 2030*. Norfolk: OTAN, 2009, p. 55.

OTAN. «Assured Security, Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO» (17 May 2010a) (online) https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf

OTAN. «BI-SC Input to a New Capstone Project for The Military Contribution to Countering Hybrid Threats» (25 August 2010b) (online) https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

OTAN. «Wales Summit Declaration» (5 September 2014) (online) https://www.nato.int/cps/en/natohq/official_texts_112964.htm

OTAN. «Jens Stoltenberg Keynote speech at the opening of the NATO Transformation Seminar» (25 March 2015) (online) https://www.nato.int/cps/en/natohq/opinions_118435.htm

OTAN. «Warsaw Summit Communiqué» (9 July 2016) (online) https://www.nato.int/cps/en/natohq/official_texts_133169.htm

WINNING WITHOUT FIGHTING: CHINA'S GREY ZONE STRATEGIES IN EAST ASIA

The hybrid nature of China's actions in the conflicts in East Asia is nothing new. It is an updating of a historical tradition based on the philosophy of Sunzi and the revolutionary past of the Chinese Communist Party (CCP) to adapt to a reality defined by competition between major powers, technological revolutions and the rise of computerised contexts. By acting in the grey zone, where the boundaries of peace and conflict blur, China pursues its interests while avoiding open conflict with the United States (US) and other regional actors.

Inés
Arco Escriche
Research Fellow,
CIDOB

CIDOB REPORT
# 08- 2022

In *Unrestricted Warfare*, published in 1999, Qiao Liang and Wang Xiangsui, two colonels in China's People's Liberation Army, analysed US strategy during the first Gulf War and concluded that the age of using military force to induce the enemy to submit had come to an end. Instead, contemporary warfare was characterised by an amalgamation of political, economic, cultural, diplomatic and military tactics used alongside armed and unconventional forces to bring the enemy to heel – a definition similar to the Western concept of hybrid warfare.

That book and its analysis have been seen as the Chinese conceptualisation of hybrid conflict, but some of the principles that govern contemporary hybrid threats were described by Sun Tsu in *The Art of War* (2019) over 2,000 years ago. For the ancient philosopher, wars are characterised by constant mutation and victory requires adaptive responses to each situation in order to neutralise the adversary through the constant search for relative advantage. This vision calls for an asymmetrical approach through the unlimited use of tactics that are at once predictable and unpredictable – for example, regular and irregular troops – with the aim of confusing, demoralising and ultimately dissuading the enemy from going to war. For Sunzi, «supreme excellence consists of breaking the enemy's resistance without fighting».

The implementation of those teachings is clearly visible in China's history and responses to conflicts. In the Imperial Era, the strategy to combat external threats consisted of employing multiple unconventional tactics, from using mercenaries of enemy origin against their own people in order to divide them, to making offerings, tributes and bribes to the adversary, and building fortifications, like the Great Wall, to deter attacks by northern nomadic peoples. Only if these prior strategies failed was military action deployed. More recently, the CCP achieved victory in the Chinese Civil War (1945–1949) through a combination of propaganda, revolutionary militias and information warfare aimed at exploiting the weaknesses of the nationalist Kuomintang (KMT) forces. The equivalent of these tactics today might be cyber warfare, using militias, supporting local insurgencies, signing lucrative business contracts and development aid packages, or building artificial islands in the South China Sea (SCS) for – theoretically – «defensive» reasons (Baker, 2015). So if the hybrid strategy is ancient, what's new?

First, China's growing regional and international rivalry and competition with the US, its military inferiority, and the need to maintain its «peaceful development» narrative favour the proliferation of hybrid tactics. These are assessed very precisely to stay short of open aggression, achieving small victories while avoiding a head-on conflict with the US and its allies in the region (Mazarr et al., 2018). Second, new technological advances have allowed new information and cyber tactics to emerge, like disinformation and cyber-attacks and, in the near future, innovative forms of AI-led warfare. Third, the emerging need to respond to hybrid wars given the certainty of this new type of conflict in which public opinion, institutions and legal systems can be used as weapons. The Chinese army has been preparing for this since 2003 in its «three warfares» doctrine, which is based upon psychological, media and legal warfare tactics that complement existing diplomatic, economic and military measures – including the deployment of military force in times of peace. The aim is to cultivate a favourable strategic environment in its neighbourhood, and to promote and defend its fundamental interests of sovereignty and territorial integrity in times of peace while preparing for possible war (PLA Daily, 2004).

In other settings, the rise of these methods is categorised as «hybrid conflict» (see chapter by Bargués and Bourekba). Nevertheless, the absence, thus far, of violence and direct military force places these operations in the grey zone, although this is not a popular concept in China. The key difference is that China feels comfortable testing the limits of peace and challenging the status quo in grey zones in which the conflict drags on for years without crossing the line into direct aggression – but it also implies no clear victory.

Geopolitics in the grey zone: from the South China Sea to Taiwan

Asia's geography and the centrality of the seas for security and relations between regional actors have allowed certain indigenous forms of grey zone tactics to emerge. In this light, China favours unconventional strategies in sovereignty disputes in areas where the US casts its shadow, but projects military superiority to deter regional powers. Such is the example of the SCS conflict and relations with Taiwan.

DESPITE THE WIDE RANGE OF TACTICS DEPLOYED TO PURSUE ITS GOALS, CHINA'S STRATEGY IN THE GREY ZONE HAS ACHIEVED MIXED RESULTS. IT HAS PROGRESSIVELY ADVANCED ITS TERRITORIAL AIMS IN THE SOUTH CHINA SEA, BUT IT HAS ALSO ERODED ITS LEGITIMACY IN THE REGION WHILE INCREASING THE RISK OF CONFLICT WITH THE US.

China claims control of maritime territories delimited by the «nine-dash line», which total around 90% of the South China Sea – including the Paracel Islands, Spratly Islands and the Scarborough Shoal, which are disputed by Vietnam, Malaysia, Indonesia, Brunei and the Philippines. In order to establish its historical claims over the last decade, Beijing has rolled out a carefully designed grey zone strategy based on using civil forces and maritime militias, the construction of dual-use infrastructure – civil engineering works that can be re-purposed for military enclaves such as ports and airfields – information tactics and the reinterpretation of international laws.

First, by deploying civilian forces like the coast guard and oceanographic vessels, as well as maritime militias made up of fishermen, alongside the navy, China gradually surrounds islets to occupy territory in *faits accomplis*, exemplified by the Scarborough Shoal standoff of 2012, or the Ayungin Shoal in the Spratlys in 2013. Specifically, these Chinese fishermen, ostensibly unlinked to the government or armed forces, have been involved in harassing foreign vessels and preventing access to territorial waters and commercial activities under the pretext that they are acting on their own initiative to «enforce the law» (Lendon, 2021). These actions also serve to exert psychological pressure and progressively test the limits and responses of rivals, as in March 2021, when 220 fishing vessels anchored near Whitsun Reef, which belongs to the Philippines, citing «rough weather». Once under its control, China has implemented an Anti-Access/Area Denial strategy in the first chain of islands in the SCS, pumping sand to construct artificial islands and dual use civil engineering and military works in the occupied islets, which have allowed it to extend its control in the region. This aims to deter access by rival military forces and to increase the projection of Chinese power, while offering its armed forces greater room for manoeuvre in the event of a military conflict (CSIS, 2017). For instance, by installing anti-ship and surface-to-air missiles on three reefs – Fiery Cross, Subi and Mischief – China has exercised de facto control over the Spratly Islands by being able to oppose all aerial or maritime movements in the archipelago since 2018.

At the same time, China has sought to legitimise some of these claims via information strategies, conducting campaigns supporting its territorial claims by disseminating the map with the nine-dash line, including in children's movies (Reuters, 2019); and using international and national jurisdiction in its favour. Although Beijing vigorously advocates compliance with the United Nations Convention on the Law of the Sea (UNCLOS), its actions suggest that these rules are not fully enforced in the region. In 2016, China rejected the Hague Tribunal's ruling in favour of the Philippines, citing inconsistency with the principle of sovereignty and contesting part of UNCLOS, defending the right to regulate, oppose or prevent navigation in the waters under its jurisdiction. In the same vein, in 2021 China approved two new national laws – the Coast Guard Law and a new maritime safety law – that set out vessel control measures and the conditions under which the Chinese coast guard may use force against foreign vessels in «waters under Chinese jurisdiction». The lack of specificity about which territory falls within Chinese jurisdiction, along with the other coercive and psychological measures, has achieved the strategy's primary objective of deterring other regional players from acting in the area – although not the US, which systematically carries out «free navigation operations» – and securing effective control of the territory without using force.

Its contested sovereignty, complex identity issues, US support and its history and ties to mainland China make Taiwan a unique case. This translates into the deployment of other tactics to exploit specific weaknesses. Beijing uses economics, diplomacy, the press and disinformation to attract, coerce and unsettle Taiwanese society thus fuelling further polarisation in regards to its future and relations with the mainland.

In the economic field, China has introduced a package of measures to attract Taiwanese citizens to study, invest and work in mainland China, with the specific aim of garnering support from sections of society, as well as from politicians, businesspeople and prominent public figures. However, during electoral periods or times of heightened tension, China does not hesitate to resort to tactics of trade coercion to influence the island's politics and foment the rivalry between the two main parties, the Democratic Progressive Party (DPP) and the KMT. The most recent case was the import ban on Taiwanese pineapples in 2021 for «food safety» reasons. A familiar tactic for Lithuania, on whom Beijing imposed similar trade restrictions after Taiwan was allowed to open a de facto embassy in Vilnius in November 2021.

These tactics have been complemented by information warfare strategies ongoing since the 1950s. Via propaganda, financing Taiwanese media outlets to publish news favourable to China. More recently, the spread of fake news and disinformation campaigns over social networks even managed to tip the balance in favour of pro-China candidates like the populist Han Kuo-yu in 2018 (Huang, 2020).

The best possible strategy is to continue using the grey zone as a «a better alternative to a military strike», according to Cui Lei (2021). Nonetheless, the rise to power of Tsai Ing-wen (DPP) in 2016 has brought a more assertive position by the mainland, with threats of «reunification by force», military drills around Fujian and incursions into Taiwan's air defence zone aimed at discouraging any secessionist moves.

CHINA FAVOURS UNCONVENTIONAL STRATEGIES IN SOVEREIGNTY DISPUTES IN AREAS WHERE THE US CASTS ITS SHADOW, BUT PROJECTS MILITARY SUPERIORITY TO DETER REGIONAL POWERS.

Where grey may become black

Despite the wide range of tactics deployed to pursue its goals, China's strategy in the grey zone has achieved mixed results. It has progressively advanced its territorial aims in the SCS, but it has also eroded its legitimacy in the region while increasing the risk of conflict with the US. In Taiwan, success also remains elusive: at the end of 2021, over 62% of Taiwan's population defined themselves as Taiwanese, compared to 2% as Chinese; while more than 80% opposed reunification (NCCU, 2022). This shows that the results remain nuanced, even if hybrid tactics and grey zone conflicts have been considered especially effective in advancing certain actors' interests and goals.

Hence, it is necessary to consider the circumstances under which China could take the leap into the "black zone" and embark on a conventional war. One would be China voluntarily raising tensions and using military force, for example, by invading Taiwan – a case with parallels with the Russian invasion of Ukraine. This remains unlikely at present. A more realistic possibility is an increase in strategic tensions in either of the two conflicts that brings a simple miscalculation and ends up provoking a direct confrontation or an open conflict due to the accumulation of activities that skirt the boundaries between peace and war, as we saw in the tensions on the border with India in the summer of 2020. For the time being, Sunzi's influence continues to guide China's strategy.

References

Aspinwall, Nick. «Taiwan Rebukes Beijing's New 26 Measures for Cross-Strait exchanges». *The Diplomat*, 2019 (online). [Accessed on 19.07.2022]: https://thediplomat.com/2019/11/taiwan-rebukes-beijings-new-26-measures-for-cross-strait-exchanges/

Baker, Benjamin D. «Hybrid warfare with Chinese characteristics». *The Diplomat*, 2015. (online). [Accessed on 19.07.2022]: https://thediplomat.com/2015/09/hybrid-warfare-with-chinese-characteristics/

CSIS. «Chinese Power Projection Capabilities in the South China Sea». CSIS, 2017 (online). [Accessed on 19.07.2022]: https://amti.csis.org/chinese-power-projection/

Cui Lei. «Mainland China is in no position to take Taiwan by force». *EastAsiaForum*, 2021 (online). [Accessed on 19.07.2022]: https://www.eastasiaforum.org/2021/02/26/mainland-china-is-in-no-position-to-take-taiwan-by-force/

Huang, Paul. «Chinese cyber-operatives boosted Taiwan's insurgent candidate». *Foreign Policy*, 2020 (online). [Accessed on 19.07.2022]: https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/

Lendon, Brad. «Beijing has a navy it doesn't even admit exists, experts say. And it's swarming parts of the South China Sea» CNN, 2021 (online). [Accessed on 19.07.2022]: https://edition.cnn.com/2021/04/12/china/china-maritime-militia-explainer-intl-hnk-ml-dst/index.html

Mazarr, Michael J., Heath, T. R., & Cevallos, A. *China and the International Order*. Santa Monica, CA: RAND Corporation, 2018.

National Chengchi University (NCCU). «Taiwanese/Chinese Identity (1992/06~2021/12)». Election Study Center, NCCU, 2022 (online). [Accessed on 19.07.2022]: https://esc.nccu.edu.tw/PageDoc/Detail?fid=7800&id=6961

PLA Daily. «El ejército popular de liberación de China empieza el estudio y el entrenamiento de las 'Tres Guerras'». Sina.cn, 2004 (online). [Accessed on 19.07.2022]: http://mil.news.sina.com.cn/2004-07-16/1738210714.html

Qiao, L., & Wang, X. *Unrestricted warfare*. Brattleboro: Echo Point Books & Media, 2015.

Reuters. «Abominable: Anger grows over controversial map in Chinese children's film». *The Guardian*, 2019 (online). [Accessed on 19.07.2022]: https://www.theguardian.com/world/2019/oct/18/abominable-anger-grows-over-controversial-map-in-chinese-childrens-film

Sunzi (Sun Tsu). *L'Art de la guerra*. Barcelona: Publicacions de l'Abadia de Montserrat, 2019.

INSECURITY IN THE MAGHREB: A GROWING CATALOGUE OF THREATS

With a frozen conflict now thawing, the rivalry between the leading regional powers increasingly evident and domestic and international factors piling up that heighten the ruling elites' perceptions of insecurity, the prospects appear bleak for intra-Maghrebi relations and the security of the countries in the region – which also has implications for their neighbours.

Eduard
Soler i Lecha
Senior Research Fellow,
CIDOB

CIDOB REPORT
# 08- 2022

A small window of hope opened in the late 1980s and early 1990s. Coinciding with the end of the Cold War, the leaders of Morocco and Algeria reached out to one another, an Arab Maghreb Union (AMU) was created in the image of the European Union and, soon after, in Western Sahara a ceasefire was declared between Morocco and the Polisario Front and MINURSO was launched – the United Nations mission meant to help resolve the conflict.

However, hopes of peace in the region were short-lived. A bloody decade in Algeria, the closure of the border between the two countries in 1994, the impasse in the negotiations over the Sahara as two plans championed by James Baker, personal envoy of the UN Secretary-General, failed, and the manifest dysfunctionality of the AMU made Maghrebi integration little more than a mirage.

At the time of writing, there is concern over rising violence in the Sahara and the rapid deterioration of relations between Morocco and

Algeria. Added to the border closure in place since 1994 are the diplomatic breakdown and the closing of Algerian airspace in August and September 2021, respectively. Morocco has been blamed for the attack on an Algerian convoy as it transited through an area controlled by the Polisario Front on the route between Mauritania and Algeria on November 1st 2021, as reported by Menadefense. The attack set off various alarms. It is not a good sign that publications like the *Atlas Stratégique de la Méditerranée et su Moyen-Orient* of the French Fondation Méditerranéenne d'Etudes Stratégiques are devoting attention to the military capabilities of Morocco and Algeria and the potential scenario of an armed confrontation between them.

Further east, to complicate matters, Libya is struggling to escape the spiral of conflict in which it has been immersed since 2011. Meanwhile, to the south, the Sahel has for some time been a key area of concern for regional security. That both Morocco and Algeria are projecting their influence in these spaces, whether by offering mediation or to coordinate regional dialogue forums or bilateral cooperation initiatives, is significant. Algerian–Moroccan competition is not responsible for the high levels of instability in Libya and the Sahel, but it does not help find ways to reduce tensions either.

A key feature of the insecurity in the Maghreb is that hybrid threats are used alongside shows of force more typical of a conventional confrontation. The Maghreb exemplifies how rather than replacing conventional threats, the hybrid can precede or even encourage them. The conflict in Western Sahara, the links with other conflict spaces and the attempts to delegitimise or weaken the regime of a rival country will help us better understand this interrelation.

The Sahara conflict: guess who?

Who are the opposing parties in this conflict? The lack of a unanimous answer to this question is a clear sign of the hybrid nature of the conflict and the differing perceptions of the threats. Algeria maintains that the clash is between Morocco and the Polisario Front. Rabat, meanwhile, argues that Polisario is a proxy for Algeria. In other words, in the Moroccan narrative, Algeria is one of the parties in the conflict, while the Algerian narrative rejects that outright.

The 50th anniversary of the Sahara conflict approaches. From 1991 to November 2020 it fit squarely within the frozen conflict category. Hostilities had ceased. The conflict had not been resolved, but continued through non-military means and modalities. The troops were still deployed, but the diplomatic competition to kickstart or reverse recognition of the Sahrawi Arab Democratic Republic (SADR) played a larger role.

The lack of progress and growing frustration among Polisario's supporters made it a matter of time before the situation worsened, and in November 2020 the conflict was definitively removed from the freezer. In response to Morocco's operation to retake control of the Guerguerat border crossing with Mauritania, Polisario announced the end of the ceasefire. Shortly after, US President Donald Trump recognised Moroccan sovereignty over Western Sahara, encouraging a more assertive Moroccan policy that fuelled diplomatic crises with Germany and Spain in 2021. On the ground, a Moroccan drone killed the head of the Polisario gendarmerie in April 2021, as confirmed by Sahrawi sources. Meanwhile, occasional episodes of hostility have occurred in the area separating the territories controlled by the two parties without any talk of a return to war. But the situation could change if the Polisario Front follows through on its threat to launch attacks against the Sahrawi cities under Moroccan control.

The confusion around who the parties are in the conflict – is Algeria one? – as well as the arms race in which the two Maghrebi powers have become embroiled increase the risks of the conflict in the Sahara thawing. If the Polisario Front acts on its threats, will Morocco see it as a form of hybrid attack directed from Algiers? And if so, how will it react? And how will Algeria respond if its nationals suffer new attacks in Polisario-controlled areas, especially, if the confrontation reaches Tindouf? Such scenarios are highly delicate but not insignificant and strengthen the argument that the hybrid is spreading: the conventional and the unconventional feed off each other.

Porous borders and theatres of conflict

Among the most worrying security dynamics in the Maghreb is the growing interconnection with other theatres of conflict. After Muammar Gaddafi was toppled in 2011, the nexus of insecurity between the Maghreb and the Sahel became especially visible as criminal gangs, arms and people traffickers, militias and terrorist groups took advantage of porous borders. The conflict in northern Mali in 2012 provided definitive proof. A decade ago, change in the Maghreb contributed to destabilising the Sahel. Now, the insecurity also flows the other way. Well aware of this situation, both Morocco and Algeria have used the tools at their disposal to show the Sahel countries – as well as the global powers with interests in the region – that they are essential actors. In doing so, Rabat and Algiers have added a further dimension to this relationship of competition and open hostility.

The other nexus links the Maghreb with the Middle East. Over the last decade, the Maghreb has become a sphere of competition between Middle Eastern regional powers. This competition involves both traditional powers like Egypt and Turkey and smaller countries with resources and ambition, like the United Arab Emirates and Qatar. Libya has become the setting par excellence for this regional competition, with these five countries supporting either the Tripoli government or Field Marshal Khalifa Haftar. Often they justify their political, financial and military support by citing national security. However, they have also occasionally shown that their support for rival groups in Libya aligns with opposing views on the region's future and, specifically, the role the groups related to the Muslim Brotherhood can play.

A KEY FEATURE OF THE INSECURITY IN THE MAGHREB IS THAT HYBRID THREATS ARE USED ALONGSIDE SHOWS OF FORCE MORE TYPICAL OF A CONVENTIONAL CONFRONTATION. THE MAGHREB EXEMPLIFIES HOW RATHER THAN REPLACING CONVENTIONAL THREATS, THE HYBRID CAN PRECEDE OR EVEN ENCOURAGE THEM.

The most striking change, however, and perhaps the most significant, is the normalisation of relations between Morocco and Israel. This rapprochement has occurred within the framework of the so-called «Abraham Accords» promoted by the US administration. In December 2020, despite having already lost the elections, in consecutive tweets Donald Trump welcomed the announcement of normalisation and at the same time recognised Moroccan sovereignty over Western Sahara.

Joe Biden reaching power has not affected this process, and the rapprochement between Morocco and Israel was sealed with visits to Rabat by then Israeli foreign minister and now prime minister, Yair Lapid, as well as by defence minister Benny Gantz, which brought the signing of the first security and defence agreement between the two countries. The Algerian authorities have made their opposition to Morocco's cooperation with Israel clear.

Whenever handling their complex neighbourly relations, the Algerian authorities have always trusted in their military superiority. But Israel's arrival on the scene in areas as diverse as drone building and intelligence has aroused major concern in Algeria, especially when it comes to unconventional confrontations.

To further complicate matters, it is worth noting that Morocco has for years been accusing Iran of providing support to the Polisario Front through

Hezbollah. Most recently, Israeli officials have argued that Algeria and Iran are part of the same regional bloc. The Maghreb is not only more divided, more and more actors from outside the region see it as a space in which to project their rivalries.

The battle for legitimacy and the catalogue of retaliation

Since their respective independences, Morocco and Algeria have built very different political models, both in their internal organisation and their international support. Morocco set itself up as a conservative monarchy with good relations with the West, while republican Algeria aspired to be a model for revolutionaries around the world. This is neither the only nor perhaps even the main reason for the mistrust and poor relations between the countries' ruling elites, but it must be taken into account. What is more, as Tilila Sara Bakrim makes clear, it is not only the ruling elites who participate in the battle of narratives, but also media allies on each side.

Despite this, Miguel Hernando de Larramendi has described how the Arab Springs generated a feeling of shared vulnerability that temporarily reactivated bilateral relations between Algeria and Morocco. But, as the fears of weakness in the face of their respective people's protests eased, the rivalry resurfaced.

In the run-up to the pandemic, both Morocco and Algeria saw protests revive. In Morocco they were highly localised in the north of the country and specifically the Rif region. In Algeria, they spread further and the Hirak movement that began in 2019 forced the resignation of President Abdelaziz Bouteflika. Nevertheless, far from generating conditions for rapprochement, these types of protests increased suspicions and even accusations that the neighbouring country was meddling in internal affairs and seeking to contribute to the destabilisation.

The situation peaked in summer 2021. Morocco's Permanent Representative to the United Nations, Omar Hilale, issued a document in which he dismissed Polisario and the SADR as a «chimerical republic self-proclaimed in the Algerian capital» and criticised Algeria for setting itself up as a fervent defender of the right to self-determination while denying «this same right to the Kabyle people, one of the oldest peoples in Africa». The «valiant Kabyle people», he went on, «deserve, more than any other, to fully enjoy their right to self-determination». The support for the Kabyle independence movement, articulated around the Mouvement pour l'autodetermination de la Kabylie (MAK), whom Hilale proposed inviting to the meetings of the United Nations Special Committee on Decolonization, generated a strong rejection by the Algerian authorities and was, ultimately, the argument used to justify severing diplomatic relations. Before making this decision, Algiers accused the MAK – and therefore indirectly Morocco – of having encouraged the forest fires that affected Kabylia in August 2021. It is difficult to think of a more hybrid threat than this.

Shortly afterwards, in October 2021, the Algerian government closed one of the two gas pipelines that connect Algeria with the Iberian Peninsula, specifically the Maghreb-Europe whose construction began during the brief thaw in relations between Algiers and Rabat in the early 1990s, and which runs through northern Morocco before flowing into Andalusia. In exchange for the rights of passage, Morocco received a kind of toll in the form of gas at prices below market rates. The gas played an important role in electricity production. Algeria has not gone as far as saying that closing the gas pipeline is part of an attempt to weaken Morocco and, formally, no contract has been broken – rather, it has expired. Nevertheless, the effects and perceptions are not much different and they therefore reinforce the hybrid aspects of the tools deployed in the intra-Maghrebi competition.

THE GROWING HOSTILITY BETWEEN MOROCCO AND ALGERIA AND THE THAWING OF THE CONFLICT IN WESTERN SAHARA ARE HAVING A SIGNIFICANT IMPACT ON SPAIN. FOR NOW, THIS HAS MATERIALISED IN DIPLOMATIC CRISES, LEGAL PROCEEDINGS AGAINST FORMER MEMBERS OF THE GOVERNMENT, SUSPICIONS OF ESPIONAGE, THE USE OF ENERGY AND MIGRATION AS A POLITICAL WEAPON, AND REPRISALS IN THE FIELDS OF TRADE AND MOBILITY.

The proliferation and diversification of threats are rarely confined to one geographical space. Neighbours tend to be dragged along, and they also end up suffering the repercussions of any escalation of the conflict. The growing hostility between Morocco and Algeria and the thawing of the conflict in Western Sahara are having a significant impact on Spain. For now, this has materialised in diplomatic crises, legal proceedings against former members of the government, suspicions of espionage, the use of energy and migration as a political weapon, and reprisals in the fields of trade and mobility. Authors like Javier Jordán say that Morocco employs hybrid strategies in its relations with Spain. The catalogue of threats is mainly used among the Maghreb countries themselves, but neighbours like Spain can also end up suffering. Normalising the threats would pose a risk to all European partners.

References

Fondation Méditerranéenne d'Etudes Stratégiques, *Atlas stratégique de la Méditerranée et du Moyen-Orient* (édition 2022), Paris: Institut FMES, 2022 (online). [Accessed on 06.07.2022]: https://fmes-france.org/atlas-strategique-de-la-mediterranee-et-du-moyen-orient-edition-2022/

Hernando de Larramendi, Miguel. «Doomed regionalism in a redrawn Maghreb? The changing shape of the rivalry between Algeria and Morocco in the post-2011 era», *The Journal of North African Studie*s, vol. 24, no. 3 (2019), pp. 506–531, DOI: 10.1080/13629387.2018.1454657.

Jordán, Javier. «Ceuta y Melilla: ¿emplea Marruecos estrategias híbridas contra España?» *Global Stategy* (24th March 2021) (online). [Accessed on 06.07.2022]: https://global-strategy.org/ceuta-y-melilla-emplea-marruecos-estrategias-hibridas-contra-espana/

Sara Bakrim, Tilila. «Rivalité Maroc-Algérie: la guerre des récits». Note de la FRS no.18/2022 (April 2022), (online). [Accessed on 06.07.2022]: https://www.frstrategie.org/publications/notes/rivalite-maroc-algerie-guerre-recits-2022

Soler i Lecha, Eduard. «La otra África: rivalidades superpuestas en el Magreb», *IDEES*, no. 56 (January 2022), (online). [Accessed on 06.07.2022]: https://revistaidees.cat/es/la-otra-africa-rivalidades-superpuestas-en-el-magreb/

CIDOB

BARCELONA
CENTRE FOR
INTERNATIONAL
AFFAIRS

Con el apoyo de:

U.S. Consulate General
Barcelona

At a time of uncertainty and contestation of international norms, conflicts are becoming increasingly diffuse, as is the space between war and peace. Tactics are diversifying. Greater dependency and connectivity between actors is used to exploit the vulnerabilities of others. Concern is growing about hybrid threats like cyber-attacks, disinformation, electoral interference and the mobilisation of migrants, which are being deployed in many parts of the world. Unconventional threats fuel uncertainty, erode values and norms, and strain international relations.

This *CIDOB Report* analyses the rise of hybrid threats. It aims to study their different forms and tactics, as well as the various scenarios in which they are deployed, in order to examine their impact, and analyse the responses that seek to address the multiple challenges they pose.