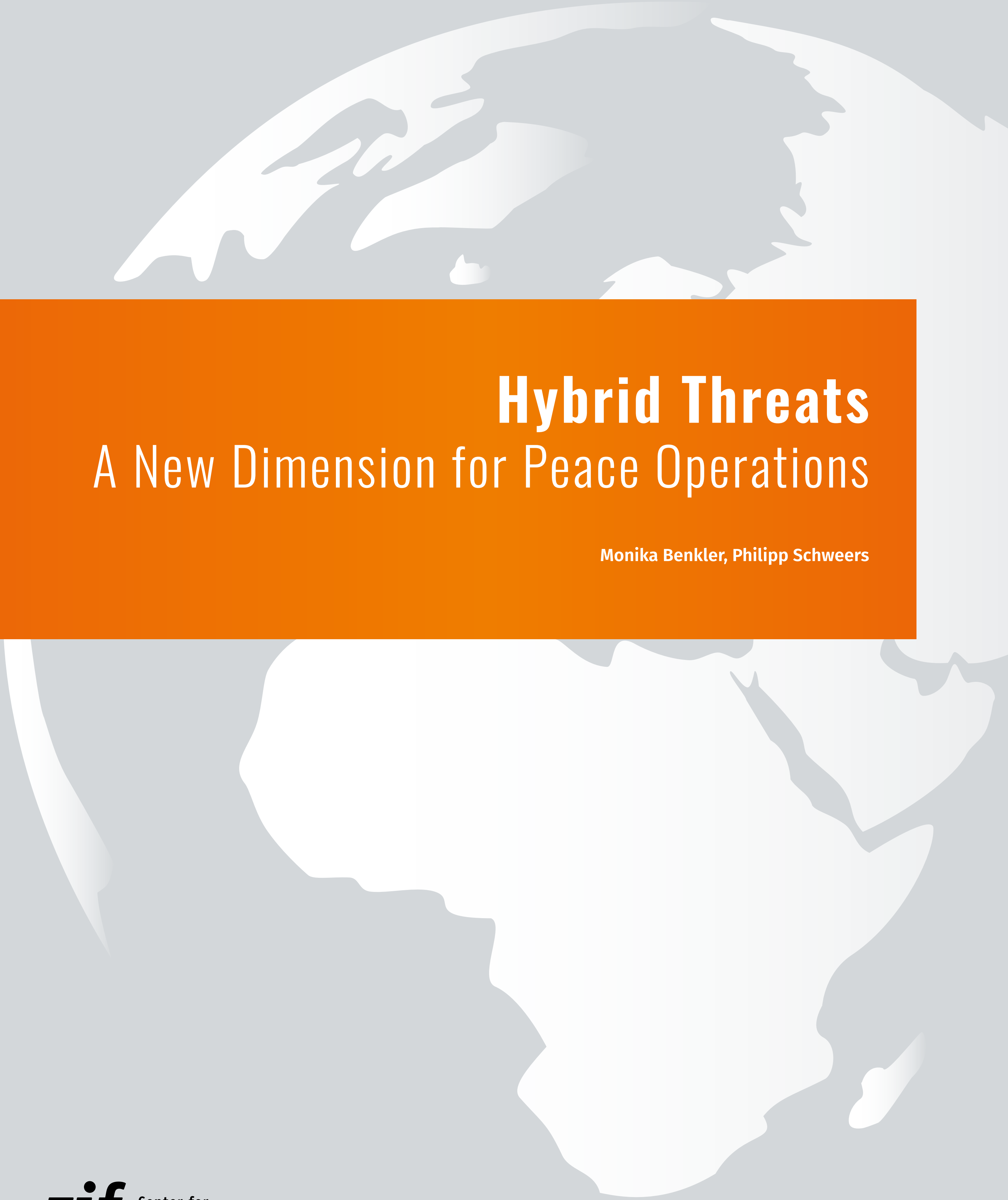
**STUDY** | OCTOBER 2025



# Hybrid Threats
## A New Dimension for Peace Operations

**Monika Benkler, Philipp Schweers**

Center for
International
Peace Operations

## Publication details

Publisher: Center for International Peace Operations –
Zentrum für Internationale Friedenseinsätze (ZIF) gGmbH
Ludwigkirchplatz 3 – 4
10719 Berlin
Fon +49 (0)30 / 52 00 565 – 0
Fax +49 (0)30 / 52 00 565 – 90

Executive Director: Dr. Astrid Irrgang
Chairperson of the Supervisory Board: Minister of State Florian Hahn

www.zif-berlin.org

Authors: Monika Benkler, ZIF Team Policy, Partnerships & Innovation (PPI).
Philipp Schweers, Head of Hybrid Threats & Cyber Security in the first year of the EUPM Moldova; currently seconded expert at the International Criminal Court.

All our publications incorporate the practitioners' perspective of ZIF's seconded experts.

The study is funded by the Federal Foreign Office.

Layout: finedesign, Berlin

**STUDY** | OCTOBER 2025

# Hybrid Threats

## A New Dimension for Peace Operations

**Monika Benkler, Philipp Schweers**

zif
Center for
International
Peace Operations

# Executive Summary

**Highly dynamic in the landscape of hybrid threats:** Although hybrid threats are as old as warfare itself, the combination of geopolitical shifts and recent accelerated technological innovation has led to a significant increase in their quality, intensity and reach, particularly on the part of autocratic states. The easy accessibility of digital technologies has also significantly expanded the range of non-state actors operating autonomously or on behalf of third parties. This directly impacts international peace operations.

**Peace operations increasingly targeted by hybrid activities:** In recent years, peace operations have increasingly become the target of hybrid activities – not least with the intention of delegitimising international engagement and undermining peacebuilding measures. Unlike states, which engage in hybrid activities in numerous different sectors, peace operations have so far been most clearly targeted in the cyber and information space.

**Peace operations as actors – new approaches:** As actors dealing with hybrid conflict activities, peace operations have implemented new approaches. This includes integrating relevant tasks into existing missions, establishing explicit, focused missions such as the EU Partnership Mission in Moldova (EUPM Moldova), and using *ad hoc* instruments such as Rapid Response Teams. These approaches must now be further refined against the backdrop of a global increase and intensification of hybrid threats. Given the polarised Security Council, expanding the mandates of UN peace operations into the cyber and information space appears unlikely at best. Nevertheless, proposals to e.g. establish a hybrid model or consider increased cooperation with the private tech sector are being put forward at the right time.

**Lessons learned for peace operations and *ad hoc* interventions in a hybrid context:** The experiences of the EUPM Moldova are helpful both for peace operations and for future *ad hoc* interventions in a hybrid context: (1) The spectrum of hybrid threats is not limited to the cyber and information space, even though this remains the main arena for destabilising operations. In both Ukraine and Moldova, hybrid attack strategies continue to identify and hit systemic vulnerabilities. (2) Successfully countering such activities requires (a) rapidly deployable expertise to counter an active threat and intervene, provide operational support to national institutions, and prevent further destabilisation; and (b) bespoke strategic advisory expertise that can permanently address the exploited systemic vulnerabilities in the aftermath of a threat.

**Recommendations for German policymakers:** The need for resilience-building missions and short-term interventions will increase. Germany should play a key, if not leading, role in the further development and implementation of peace operations and short-term interventions to counter hybrid threats. Germany should continue to participate actively in further developing instruments such as the EU Hybrid Rapid Response Teams – politically, conceptually and in terms of personnel – as well as maintain its own expertise. Due to the growing need for dedicated capacities from analysts and cyber security experts to communications specialists and financial flow analysts, Germany should further bolster its operational capability in the civilian sector and make targeted use of the expertise that already exists in the ZIF Expert Pool.

# Introduction

Against a backdrop of geopolitical tensions, global interconnectedness and easily accessible innovative digital technologies, hybrid threats are constantly on the rise and are being used by a growing range of primarily autocratic state and non-state actors to advance their own interests. The war in Ukraine since 2022 is a clear example of how the rapid implementation of hybrid activities such as cyber and information campaigns, social disruption manoeuvres and attacks on critical infrastructure is increasingly relevant in conventional warfare as well.

These developments have direct consequences for international peace operations.[1] On the one hand, they have of late increasingly become the target of hybrid activities, particularly in the cyber and information space – not least with the intention of delegitimising international engagement and undermining peacebuilding measures. On the other hand, the global increase and intensification of hybrid threats challenges international organisations and peace operations as actors to (further) develop approaches for dealing with hybrid conflict activities. This includes, in particular, integrating relevant tasks or structures into existing or future missions, establishing explicit, focused missions, deploying rapid response teams or partnering with companies in the tech industry.

This study analyses the challenges posed by an increasingly complex landscape of hybrid threats to international peace operations as well as resulting conceptual and personnel measures and offers recommendations for German policy.

**Table of contents**

1. Definition of terms 6

2. New qualities in new technologies 8

3. Peace operations as a target of hybrid activities 9

3.1 Harmful information 9
3.2 Cyberattacks 10
3.3 Expanded range of actors 11

4. International organisations and their peace operations as actors: Approaches to dealing with hybrid conflict activities 13

4.1 Integration into existing mandates 13
4.2 Explicit, focused missions: EUPM Moldova as a blueprint 15
4.3 Multinational rapid response capabilities 17
4.4 Cooperation with the private sector 18

5. Future challenges for operations in the context of hybrid threats – recommendations for German policymakers 19

List of abbreviations 22

[1] In this publication, we use the term "peace operations" to refer to the entire spectrum from smaller field-based missions to large multidimensional operations.

# 1. Definition of terms

Russia's annexation of the Crimean Peninsula in 2014 was a wake-up call for the international community to take the threat of hybrid activities seriously. Since 2015, international organisations have launched approaches for dealing with hybrid threats and hybrid warfare. In December, NATO adopted its first formal Strategy on NATO's Role in Countering Hybrid Warfare (2015). [2] A few months later, in April 2016, the EU followed suit with its Joint Framework on Countering Hybrid Threats: A European Union Response.[3] The UN Security Council discussed hybrid wars as a threat to international peace and security for the first time in March 2017 within the framework of an informal Arria formula meeting.[4]

Hybrid warfare is a type of activity involving the possible use of hybrid threats and is at the end of the escalation spectrum.

Despite their inclusion in strategy documents and their continued presence in the security policy debate, no universally accepted definition has emerged for the terms "hybrid threats" and "hybrid warfare" since their introduction.[5] They are often used synonymously but must be distinguished from one another. This study follows the understanding of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), founded in 2017 by EU and NATO member states:[6]

### Hybrid threats, hybrid warfare

- **Hybrid threats** are harmful activities by an opponent that are planned with malicious intent and carried out in a targeted and covert manner to prevent attribution. They seek to undermine, destabilise or delegitimise a target, such as a state or an institution, through a variety of means, often combined, in order to achieve their own political goals. These means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvres, election manipulation, coercive diplomacy or the threat of military force. Hybrid threats cover a wide range of harmful activities with different objectives, ranging from interference, influence and operations to hybrid warfare.
- **Hybrid warfare** is a type of activity involving the possible use of hybrid threats and is at the end of the escalation spectrum. Unlike other variations, its key feature is the use of military means (covert or overt). The "little green men" – Russian soldiers without insignia – who occupied Crimea in 2014 are one example. Not every form of undesirable action using the hybrid toolbox can therefore be declared hybrid warfare.

[2] The strategy is based on the three pillars of preparedness, deterrence and defence and has formed the basis for NATO's approach to hybrid activities since 2015. For further information, see Davide Genini, Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine, in: New Perspectives, Volume 33, Issue 2, June 2025, pp. 122- 149.

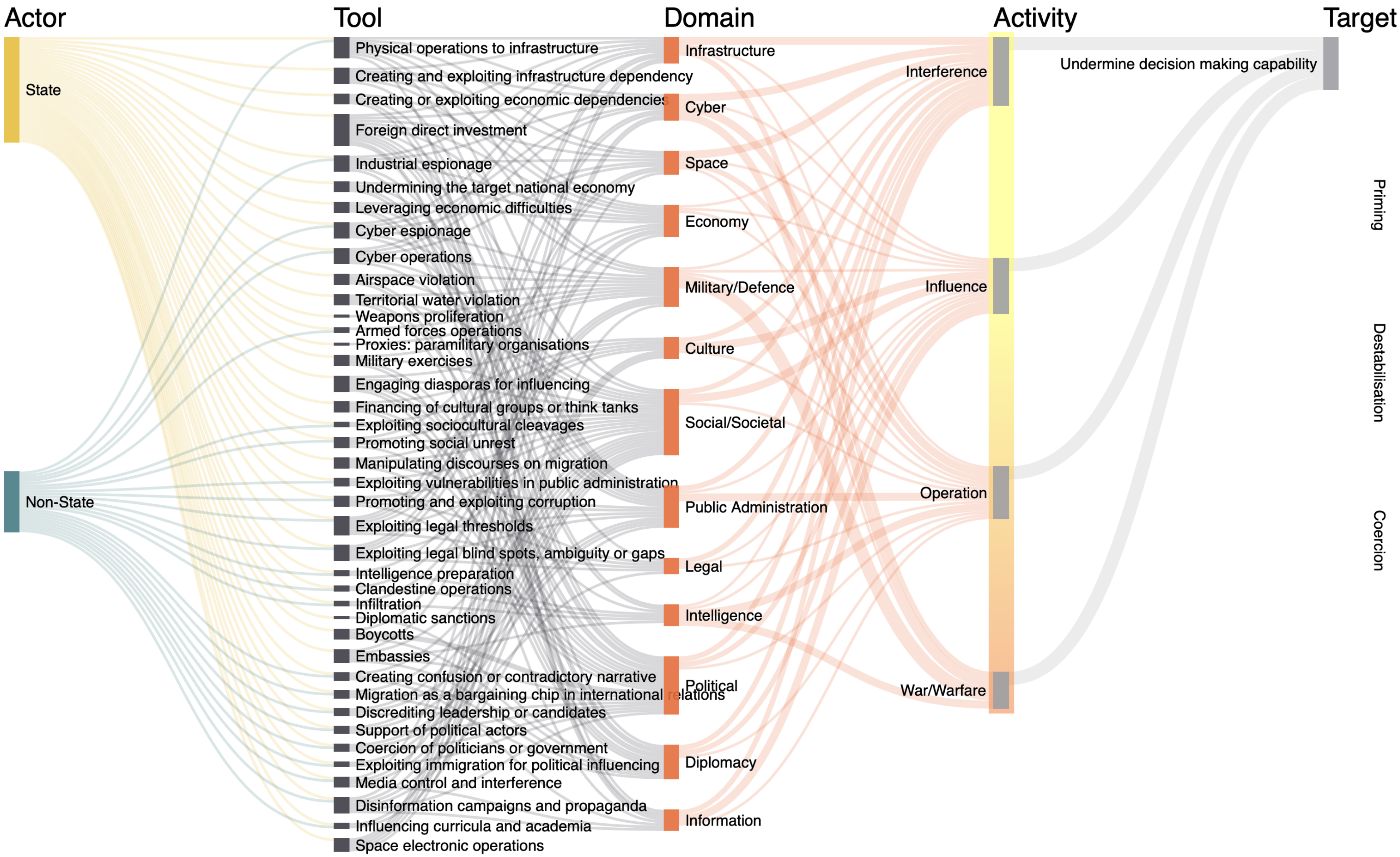
[3] See Joint Framework on Countering Hybrid Threats: A European Union Response. Since 2016, the EU has continuously developed its response to hybrid activities. See: European Council and Council of the European Union, A coordinated EU response to hybrid threats, Last review: 20 May 2025.

[4] The meeting, entitled "Hybrid Wars as a Threat to International Peace and Security," was initiated by Ukraine and aimed to discuss the concept of hybrid warfare and its impact on international peace and security.

[5] After the term "hybrid war" had already been used sporadically in literature in the 1990s, a publication by American military theorist Frank G. Hoffman in 2007 sparked a broader discussion on the topic. With regard to Hezbollah's actions against Israel in the Second Lebanon War in 2006, he described the tactics of mostly non-state armed groups that use conventional and irregular methods of warfare to fight technologically superior opponents. See Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, December 2007.

[6] See European Centre of Excellence for Countering Hybrid Threats, accessed on 29 June 2025, and Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou (Eds.), The Landscape of Hybrid Threats: A Conceptual Model, Public Version, European Commission and Hybrid CoE, 2021, p. 11.

**The landscape of Hybrid Threats: Visualization of the conceptual model**


Actor
Tool
Domain
Activity
Target
State
Non-State
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Interference
Influence
Operation
War/Warfare
Undermine decision making capability
Priming
Destabilisation
Coercion

Quelle: Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305, p. 13.

## 2. New qualities in new technologies

Over the past decade, the analytical usefulness of the terms “hybrid threats” and “hybrid warfare” has been hotly debated, as has the novelty of the concept.[7] In fact, hybrid forms of conflict are as old as the history of war and conflict itself.[8] And still, modern technologies – and in particular the resulting emergence of the cyber and information space as an additional “battlefield” – have opened up unprecedented new opportunities for asserting interests. In short, the scope and reach of hybrid activities have expanded and the range of actors diversified.

The exponential pace with which generative artificial intelligence is evolving will further strengthen the hybrid toolbox.

Over the past ten years, it has been the increasing technological automation in the cyber and information space that has especially contributed to the damage potential of hybrid activities. The manipulation of social media by so-called bot networks or attacks on critical infrastructure and cyber infrastructure by progressively specialised malware (so-called Advanced Persistent Threats/APT) are a case in point.[9] New scenarios that revealed the expanded damage potential caused by accelerated technological innovation prompted NATO at its 2021 Brussels summit to define malicious cumulative cyber activities against a member under certain circumstances as a hostile military attack, that could trigger Article 5 of the North Atlantic Treaty.[10]

The exponential pace with which generative artificial intelligence (AI) is evolving will further strengthen the hybrid toolbox.[11] The same applies, however, to possible new defence strategies against hybrid attacks, which, with the appropriate use of AI, can more quickly identify and counter harmful activities in the information and cyber space – whether they pertain to monitoring social media activity, tracking suspicious financial flows or protecting networked critical infrastructure.[12]

[7] See, among others, Michael Rühle, Aufstieg und Fall des hybriden Krieges (The Rise and Fall of Hybrid Warfare), in: Internationale Politik 5/2023, pp. 87–91; Lennart Maschmeyer, Assessing Hybrid War: Separating Fact from Fiction, CSS Analyses in Security Policy, No. 332, November 2023, ETH Zurich; Libiseller Chiara, “Hybrid warfare” as an academic fashion, Journal of Strategic Studies, 2023, Vol. 46, No. 4, pp. 858–880.

[8] See Johann Schmid, Hybride Kriegführung – Erklärstück (Hybrid Warfare - Explanatory Piece), Bundeswehr, 14 December 2022.

[9] See, among others, The Evolution of Cyber Operations in Armed Conflict, in: FP Analytics / Microsoft, Digital Front Lines. A sharpened focus on the risks of, and responses to, hybrid warfare, Fall 2023, pp. 4-10; John Nagl and Michael Posey, Botnets, Battlefields, and Blurred Lines: Optimizing an Information Strategy for Modern War, Modern War Institute, September 12, 2022; Manel Medina Llinàs, Hybrid Attacks on Critical Infrastructure, CIDOB, September 2022.

[10] See NATO, Brussels Summit Communiqué, 14 June 2021. See also: Sarah Wiedemar, NATO and Article 5 in Cyberspace, CSS Security Policy Analyses, No. 323, May 2023, ETH Zurich.

[11] See, among others, Eleonore Pauwels, Preparing for Next Generation Information Warfare with Generative AI, CIGI Paper No. 310, December 2024; Mikael Weissmann, Future threat landscapes: The impact on intelligence and security services, Security and Defence Quarterly 2025, 49 (1), pp. 40-57; Katja Muñoz, Maria Pericàs Riera, The Influence Evolution. Harnessing AI Innovation While Preserving Human Connection in Social Media, DGAP Policy Brief, 27 May 2025.

[12] See Wesley R. Moy, Kacper T. Gradon, Artificial intelligence in hybrid and information warfare. A double-edged sword, in: Fabio Cristiano, Dennis Broeders, François Delerue, Frédérick Douzet, Aude Géry (Eds.), Artificial Intelligence and International Conflict in Cyberspace, London 2023, pp. 47-74.

# 3. Peace operations as a target of hybrid activities

## 3.1 Harmful information

Unlike states, which engage in hybrid activities in numerous different sectors, peace operations have so far been most clearly targeted in the cyber and information space. Malicious actors use Harmful Information (in the parlance of the UN), Foreign Information Manipulation and Interference/FIMI (EU) or Information Threats (NATO) to promote broader strategic goals in countries and regions where they seek to expand their influence. In Africa, the region with the largest UN missions, the number of disinformation campaigns has almost quadrupled from 50 (2022) to 189 (2024). Sixty percent of these originated from external state actors, with Russia topping the list at around 40 percent.[13] In other regions, such as the South Caucasus or the Western Balkans, a similar picture emerges with regard to the extent and actors involved.[14]

Hybrid activities have so far most clearly attacked peace operations in the cyber and information space.

For peace operations such as the UN Mission MONUSCO in the Democratic Republic of Congo (DRC) or the EU Mission in Armenia (EUMA), harmful information is a persistent challenge. At times, it has massively damaged their reputation, undermined popular trust in their work – the foundation for successful mandate implementation – and threatened the safety of the personnel deployed. According to a recent study by the UN Department of Peace Operations (DPO) that looked at harmful online information and narratives during MINUSMA's withdrawal phase from Mali (June to December 2023), "disinformation can serve as a sign of a strategic and existential threat to missions."[15] In the case of MINUSMA, it helped "to reinforce and justify its removal."[16]

The investigation into MINUSMA also highlights the transnational nature of the threat. The report argues that linking negative narratives about MINUSMA with supposed similarities to other 'malicious' missions in the region – in particular MONUSCO in the DRC and MINUSCA in the Central African Republic (CAR) – points to a wider intent of "broadening the perspective and delegitimising the UN peacekeeping enterprise."[17] The latest FIMI report by the European External Action Service (EEAS) also notes that, given Russia's FIMI infrastructure in Africa, a "long-term, multi-layered strategy [has] developed over recent years"[18] that challenges Western and European engagement.

[13] See South Africa Center for Strategic Studies, Mapping a Surge of Disinformation in Africa, 13 March 2024.

[14] See Digital Forensic Research Lab, In Europe and the South Caucasus, the Kremlin leans on energy blackmail and scare tactics, Issue Brief, 29 February 2024, Atlantic Council; Bojana Zorić, The Western Balkans. The power of connection, in: Ondrej Ditrych and Steven Everts (Eds.), Unpowering Russia. How the EU can counter and undermine the Kremlin, EUISS, Chaillot Paper 186, May 2025, pp. 40-46; Leonardo De Agostini, Ondrej Ditrych, Digital Echoes. Countering adversarial narratives in Georgia and Armenia, EUISS, Brief 19, July 2025.

[15] UN DPO Information Integrity Unit, Digital Information Harms Targeting MINUSMA During the Drawdown, Retrospective Analytical Report, 01 June-31 December 2023, 2024, p. 34.

[16] Ibid., p. 3.

[17] Ibid., p. 33.

[18] EEAS, 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the architecture of FIMI operations, March 2025, p. 32.

**Strategies in the fight against harmful information**[19]

The spread of attacks in the digital space requires peace operations to strengthen their defences against harmful information and external influence. They are doing so more and more systematically.[20] In addition to (1) monitoring and analysis (situational awareness), the focus is on (2) reactive, proactive and preventive measures such as strategic communication or community engagement and, related to this, (3) fortifying the mission's own resilience and (4) cooperating with partners. Given the close connection between harmful activities in the information space and cyberattacks, missions' resilience building must include their own cybersecurity.

## 3.2 Cyberattacks

The United Nations International Computing Centre (UNICC), a specialised agency within the UN system, noted in its latest Cyber Threat Landscape Report that "malicious activities of interest"[21] – including cyberattacks – against UN organisations are increasing in frequency and severity. In 2023, 46 UN organisations supported by UNICC were attacked. Compared to the previous year, the report records a 170 percent increase in the number of incidents with the primary goal of obtaining sensitive information and data (48 percent), followed by financial gain (42 percent).[22]

For peacekeeping missions, the threat posed by cyber attacks has increased significantly in recent years.

Peace operations are significantly threatened by cyberattacks. In 2023, UN Secretary-General António Guterres pointed out to the Security Council that AI-supported cyberattacks were being used against peace operations.[23] In 2021, the EEAS stated that the (military) missions of the Common Security and Defence Policy (CSDP) were increasingly exposed to threats from cyberspace.[24] Concrete figures and cases of cyberattacks in the context of peace operations are difficult to verify with open sources, but enhanced digitalisation of peace operations is clearly rendering them more vulnerable – despite other positive effects on the efficiency of mandate implementation.

The use of more sophisticated tools for gathering and managing information in peace operations means that new, highly sensitive and highly centralised types of data are stored in mission networks. These can be useful to conflict actors and are therefore potential targets for cyberattacks.[25] Were this data used, for example, for a physical attack on ethnic groups or individuals, it might cause significant damage to popular trust in the mission, in addition to the harm done to those groups or individuals. At the same time, mission staff themselves are at risk, for instance, when operational data about patrols is extracted, access to information is denied or communication channels disrupted. Moreover, they are increasingly exposed to hacking attempts aimed at undermining them personally.[26]

International organisations have established various measures to bolster their peace operations against cyber threats. This includes establishing Computer Emergency Response Teams (CERT), systematically integrating and monitoring their own IT infrastructure, and deploying rapid response teams both preventively and reactively to support member states and partner countries (see below).

[19] See Monika Benkler, Annika S. Hansen, Lilian Reichert, Protecting the Truth: Peace Operations and Disinformation, ZIF Study, September 2022.

[20] See UN DPO, Policy on Information Integrity in Peacekeeping Settings, 16 December 202; EEAS, Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI), 14 March 2025; NATO, NATO's approach to counter information threats, 23 June 2025.

[21] UNICC uses the term "malicious activities of interest" to classify all cyber threats, security incidents and events that target UN organisations and are relevant to improving proactive cyber defence. UNICC, Cyber Threat Landscape Report 2023, May 2024, p. 4.

[22] Ibid., p. 9.

[23] See Secretary-General Urges Security Council to Ensure Transparency, Accountability, Oversight, in First Debate on Artificial Intelligence, 18 July 2023.

[24] See EEAS, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations, 15 September 2021, p. 5.

[25] See Dirk Druet, Cybersecurity and Peace Operations: Evolving Risks and Opportunities, IPI Issue Brief, March 2024; Eleonore Pauwels, Peacekeeping in an Era of Converging Technological & Security Threats. Preventing Collective AI & Data Harms, Learning to Save Lives with Dual-Use Technologies, UN DPO Paper, April 2021.

[26] See Allison Pytlak, Protecting Civilians in Cyberspace: A UN Security Council Imperative, Commentary, The Henry L. Stimson Centre, 13 June 2025.

## 3.3 Expanded range of actors

The range of actors who use hybrid threats to hinder peace operations in implementing their mandates has expanded significantly in recent years. Among states, major powers such as Russia and China, both permanent members of the UN Security Council, but also emerging middle powers, are using hybrid activities to influence political processes in countries where peace operations are deployed, and to undermine the credibility and legitimacy of those operations.[27] Even though hybrid tools are mostly used below the military threshold, the activities of several actors – in particular the Russian approach[28] – show that the entire spectrum of hybrid activities is increasingly being used by state military and secret services, using military planning and allocating the corresponding resources.[29]

In addition to state actors, armed and unarmed non-state actors play an important role, acting autonomously or on behalf of third parties.

Using military and security companies (Private Military Companies, Private Security Companies) such as the Russian Wagner Group (and its successor organisation, Africa Corps) or Chinese security companies[30] is also part of the toolbox. These operate in countries such as the CAR and South Sudan in parallel with peace operations, influencing conflict dynamics with covert activities and hindering peace operations in the implementation of their mandates.[31] In the CAR, media outlets affiliated with Russia and Wagner, in collaboration with local networks of journalists and influencers, spread rumours about links between peacekeeping forces and non-state armed groups and terrorists. Following specific allegations that MINUSCA surveillance drones were being used to drop bombs on Russian camps, the government banned the use of drones, which severely limited the mission's observation capabilities, especially in areas with no physical access.[32]

In addition, armed and unarmed non-state actors (NSAs) play an important role. They act autonomously (e.g., local rebel groups in the Central African Republic, extremist groups such as the jihadist group JNIM in the Sahel) or on behalf of third parties. Attacks in which NSAs are used as proxies are increasing in number and intensity globally: "It is cost-effective, deniable, and risk averse. It allows the sponsor to benefit from the proxy's local or specialist knowledge, while minimising the risk of retribution."[33] For NSAs, this 'relationship' not only offers the opportunity to maximise resources, but also increases the chance of achieving their own strategic goals.[34] Organised crime structures, hackers for-hire, cyber mercenaries, state-affiliated companies or non-governmental cultural institutions are used as proxies, as are official media, diplomatic missions or influencers.[35]

Available data indicates that a complex network of actors was involved in the production and distribution of harmful information against MINUSMA in Mali – the mission was ultimately withdrawn in late 2023. The campaign primarily aimed at damaging the mission's reputation and praised its expulsion. Local and international social media influencers, who were reportedly financed by national and external actors, played a prominent role.[36]

[27] See Giovanni Faleg, Nad'a Kovalčíková, Rising Hybrid Threats in Africa. Challenges and Implications for the EU, EUISS Brief 3, March 2022; Chris Kremidas-Courtney, Hybrid storm rising: Russia and China's axis against democracy, European Policy Centre, 02 May 2025.

[28] This is also referred to as the Russian "hybrid playbook," which has been tested in practice in the 2008 war in Georgia, the 2014 Crimea crisis and the current war of aggression against Ukraine, including ongoing regional destabilisation efforts, and is increasingly professionalised. For like-minded countries, like China and Iran, these efforts could suggest examples of 'good practice.' Ofer Friedman, Russian 'Hybrid Warfare': Resurgence and Politicisation, Oxford University Press, 2018.

[29] See Tom Burt, The Face of Modern Hybrid Warfare, in: FP Analytics / Microsoft, Digital Front Lines. A sharpened focus on the risks of, and responses to, hybrid warfare, Fall 2023, pp. 14-15.

[30] See Alessandro Arduino, Chinese private security firms are growing their presence in Africa: why it matters, The Conversation, 08 August 2022.

[31] See Andreas Wittkowsky, Geopolitische Spoiler. „Private" Militär- und Sicherheitsunternehmen und Friedenseinsätze ("Private" Military and Security Companies and Peace Operations), ZIF Briefing 09|2024; Dirk Druet, Knives Out: Evoving Trends in State Interference with UN Peacekeeping Operations, Ethics & International Affairs, Volume 38, Issue 4 (2024), pp. 464-478; Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou (eds.), The Landscape of Hybrid Threats: A Conceptual Model, Public Version, European Commission and Hybrid CoE, 2021, p. 23.

[32] See Dirk Druet, Knives Out: Evoving Trends in State Interference with UN Peacekeeping Operations, p. 472.

[33] Vladimir Rauta, Countering state-sponsored proxies: Designing a robust policy, Hybrid CoE Paper 23, February 2025, pp. 6 f.

[34] Ibid.

[35] EUROPOL's EU Serious and Organized Crime Threat Assessment 2025 states: "Criminal networks are also increasingly operating as proxies in the service of hybrid threat actors, a cooperation which is mutually reinforcing;" see also Janne Jokinen, Magnus Normark, Hybrid threats from non-state actors: A taxonomy, Hybrid CoE Research Report 6, June 2022.

[36] See UN DPO Information Integrity Unit, Digital Information Harms Targeting MINUSMA During the Drawdown, Retrospective Analytical Report, 01 June–31 December 2023, 2024, p. 24 ff.

While no cyberattacks against peace operations have been publicly attributed to NSAs to date, this does not correspond with a low threat level in this security-sensitive area. Given the generally growing number of NSAs attacking cyberspace and their complexity, the threat potential of proliferating NSAs in the cyber domain will likely also increase for international peace operations.

The threat potential of proliferating NSAs in the cyber domain is also expected to increase for peace operations.

### Powerful NSAs in cyberspace

Nationalist, pro-Russian hacktivists such as the KillNet-network have been attacking Ukrainian and European websites and internet services, particularly those of state structures, since 2022.[37] Cybercriminal organisations such as the Russian Evil Corp – known, among other things, for extensive and successful ransomware attacks on the private sector – have reportedly carried out large-scale cyberattacks on Western internet service providers on behalf of the Russian secret service.[38] Research also points to China using numerous NSAs – especially in cyberspace – to make it more difficult to attribute malicious activities.[39]

[37] See Antoaneta Roussi, Meet Killnet, Russia's hacking patriots plaguing Europe, Politico, 09 September 2022; Daryna Antoniuk, Russian hacker group Killnet returns with new identity, The Record, 22 May 2025.

[38] See National Crime Agency, Evil Corp: Behind the Screens, October 2024.

[39] See Jukka Aukia, China as a hybrid influencer: Non-state actors as state proxies, Hybrid CoE Research Report 1, June 2021; Medium, Chinese Cyber Operations targeting Critical Infrastructure, 13 April 2025.

# 4. International organisations and their peace operations as actors: Approaches to dealing with hybrid conflict activities

## 4.1 Integration into existing mandates

As hybrid forms of conflict resolution have become the “new normal,”[40] international organisations and their peace operations, as the most important instruments of international conflict management, are called upon to respond. Since 2016, the UN Security Council has shown growing concern with the impact of digital technologies on international peace and security. Member states have used various formats to address issues such as cyber security and hybrid warfare, the role of social media in inciting discrimination, hostility and violence, and the implications of artificial intelligence for peacekeeping operations and Special Political Missions (SPMs).[41]

The United Nations Security Council should be more actively involved in addressing threats from cyberspace.

How widely perspectives differ among members of the Security Council regarding its role and engagement in these areas was again evident at the High-level Open Debate on Emerging Threats in Cyberspace in June 2024.[42] While some saw a clear role for the Council in addressing threats from cyberspace, Russia instead pointed to the expertise and representativeness of a working group mandated by the UN General Assembly (GA) in 2019 and open to all UN member states: the Open-ended Working Group (OEWG) on security and use of information and communications technologies (ICTs). Like the Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace, established by the GA in 2004, the OEWG is a significant process for the development of rules, norms and principles of responsible state behaviour in cyberspace.

As early as the 2010s, a debate began on “cyber peacekeeping,” which, depending on the context, could take on similar tasks to physical peacekeeping in cyberspace.

During the open debate, Cho Tae-yul, Minister of Foreign Affairs of the Republic of Korea and President of the Security Council, called on the Council not to bury its head in the sand and to intensify its efforts to address threats from cyberspace. Following the Security Council’s annual debate on the Protection of Civilians (POC) in May 2025, the Stimson Center recommended that the Council “leverage the current momentum on cyber issues to more closely consider how to prevent and mitigate the negative impact of cyber operations and ICT misuse on civilian protection and, relatedly, international peace and security.”[43]

[40] Christopher Nehring, Es braucht eine ganzheitliche Strategie gegen hybride Angriffe (A holistic strategy is needed against hybrid attacks), Tagesspiegel Background, 18 June 2025.

[41] See Allison Pytlak and Shreya Lad, Strengthening Global Cyber Resilience Through UN Security Council Initiatives, Issue Brief, The Henry L. Stimson Center, 08 August 2024.

[42] See Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats, Meetings Coverage Security Council, 20 June 2024.

[43] Allison Pytlak, Protecting Civilians in Cyberspace: A UN Security Council Imperative, Commentary, The Henry L. Stimson Center, 13 June 2025.

### Cyber peacekeeping

In order to stabilise states after escalated hybrid activities, restore structures in affected areas of operation (e.g., contaminated cyber infrastructure, polarised information space, damaged critical infrastructure) and contribute to the creation of lasting peace, sectors affected by hybrid activities must be more closely integrated into peace operations than has been the case to date. A debate on "cyber peacekeeping" began as early as the 2010s, which, depending on the context, could take on similar tasks to physical peacekeeping in cyberspace.[44] These include monitoring activities that violate a ceasefire or peace agreement, investigating major attacks, demobilising cyber combatants, protecting the civilian population from cyberattacks such as disinformation campaigns, promoting human rights in cyberspace, and supporting states in rebuilding critical infrastructure.

As part of the current discussion on the future of UN peace operations, existing proposals for deployment models have been taken up.[45] These include integrating a cyber unit into a physical UN peace operation or implementing purely online missions in cyberspace with "digital blue helmets." In the past, the UN's Digital Blue Helmets (DBH) programme, which was established in 2016 to protect its own infrastructure, was seen as a possible starting point.[46]

An expansion of mandates into the cyber and information space is also difficult to imagine at present, given the desire of some UN Security Council members for peace operations to concentrate on core tasks.[47] In recent years, though, new aspects have already been integrated into the mandates of various UN, EU and OSCE missions, particularly with regard to building state and societal resilience. These range from digital literacy to strengthening independent, high-quality media and protecting critical infrastructure to resilient security and defence structures. UN peace operations like UNIFIL, UNMISS and MONUSCO have been given explicit mandates in relation to harmful information and UNAMI in Iraq provides advice on how to deal with harmful information as part of its mandate to support elections (S/2025/323). In the DRC, MONUSCO recently trained 26 leaders of civil society organisations in North Kivu province for two days on fighting disinformation and hate speech.[48]

The EU is committed to strengthening state structures against hybrid activities as part of its Common Security and Defence Policy (CSDP) missions. In 2023, the Civilian CSDP Compact called on EU member states "[to] provide the necessary capabilities to strengthen resilience against and response to hybrid and cyber threats, as well as FIMI, of host countries, wherever relevant, and of civilian CSDP missions, supported by the EEAS [European External Action Service]."[49] EUAM Ukraine (European Union Advisory Mission Ukraine), which has been running since 2014, has adapted to current challenges by integrating strengthening resilience to hybrid activities into its civilian security sector reform mandate. In this way, it supports the Ukrainian National Security and Defence Council (NSDC) in matters of cybersecurity, strategic communication in the context of disinformation and the protection of critical infrastructure.[50]

[44] See, among others: Walter Dorn, Cyberpeacekeeping: A New Role for the United Nations?, Georgetown Journal of International Affairs, Volume 18, Number 3, Fall 2017, pp. 138- 146; Michael Robinson, Kevin Jones, Helge Janicke & Leandros Maglaras, Cyber Peacekeeping from Concept to Implementation, Policy Brief, Global Foundation for Cyber Studies and Research, September 2019; Branka Panic, Cyber Blue Helmets - Can Cyber Peacekeepers Help Sustain Peace in Cyberspace?, NYU, Center on International Cooperation, 02 May 2022.

[45] See El-Ghassim Wane, Professor Paul D. Williams, Professor Ai Kihara-Hunt, The Future of Peacekeeping, New Models, and Related Capabilities, Independent Study commissioned by the United Nations Department of Peace Operations, October 2024, pp. 33 f.

[46] See Nikolay Akatyev, Joshua I. Jame, United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping, November 2017.

[47] During the debate on the UNMISS mandate extension on 08 May 2025, the US clearly formulated its position on the future design of peacekeeping mandates: "Peacekeeping mandates, including this one, should not pursue ideological goals that are difficult to define and even more challenging to implement on the ground, but rather focus on core Chapter VII functions."

[48] See MONUSCO, North Kivu: Civil Society Leaders Trained to Combat Disinformation and Hate Speech, 24 April 2025.

[49] European Union Common Security and Defence Policy, Civilian CSDP Compact, Towards more effective civilian missions, 2023, p. 22, No. 9.

[50] See EUAM Ukraine, EUAM continues its support towards the National Security of Ukraine and EU integration, 20 May 2024.

Through its activities in the field of media (promoting media pluralism and information literacy in civil society), the OSCE has long contributed to strengthening societies' resilience against harmful information. Eleven of its current 12 field operations have a corresponding mandate. In the field of cybersecurity, the Transnational Threats Department (TNTD) of the OSCE Secretariat has been doing pioneering work since 2012: TNTD organises a range of activities to build national capacities for dealing with cybersecurity threats and to promote regional cooperation and resilience.[51] Established in 1995, the OSCE Mission to Bosnia and Herzegovina, has an explicit mandate in the field of cyber/ICT security. Among other things, it supports the development of a strategic cybersecurity framework and the establishment and strengthening of national Computer Emergency Response Teams.[52]

In recent years, new aspects have been incorporated into mandates for various missions at the UN, the EU and the OSCE.

## 4.2 Explicit, focused missions: EUPM Moldova as a blueprint

Similar to the situation in Ukraine before 2022, aspiring EU-member Moldova is exposed to intense Russian-led hybrid activities aimed at destabilising the country politically and economically and preventing it from moving closer to the EU and the West.[53] Using a synchronised combination of hybrid tools that were gradually positioned in the Republic of Moldova over the past 30 years, Russia has been attempting to sabotage the country's European integration since at least 2020. Tools include manipulating the energy supply (by suspending Russian-dominated gas and electricity supplies and destabilising the power grid), military threats by Russian military contingents stationed in breakaway Transnistria, paying and equipping anti-government protests, using organised crime structures to illegally establish and finance pro-Russian parties, conducting disinformation campaigns with deep fakes against pro-European politicians, cyberattacks against security agencies, hack-to-leak operations, and attempting to manipulate elections.

The EU is scaling up its engagement through the additional use of so-called specialised teams and highly specialised visiting experts.

Building on lessons learned during the massive intensification of hybrid activities in the run-up to Russia's attack on Ukraine in 2022, the EU established a small civilian partnership mission in Moldova, which focuses exclusively on hybrid threats.[54] Acting as an experimental spearhead in dealing with hybrid attacks, the EU Partnership Mission in Moldova (EUPM Moldova) supports efforts to build the resilience of Moldovan security authorities against destabilising hybrid activities, with a particular focus on FIMI, cybersecurity and crisis management. Among other things, it contributes to building the capacities of the recently established National Cyber Security Authority within the Ministry of the Interior, as well as the government's Strategic Communications Team.[55]

Although comparatively small, with a mandated mission size of up to 49 international experts, the EU is scaling up its engagement by additionally deploying temporary experts seconded from member states in the form of so-called "Specialised Teams" and highly specialised "Visiting Experts." With the Brussels-based Hybrid Rapid Response Teams established in 2024, the EUPM Moldova can draw on additional personnel support (see below).[56]

[51] See OSCE Transnational Threats Department, Cyber/ICT Security.

[52] See OSCE Mission to Bosnia and Herzegovina, Cyber/ITC Security.

[53] See Lucjan Kubica, Moldova's struggle against Russia's hybrid threats: from countering the energy leverage to becoming more sovereign overall, Hybrid CoE Working Paper 28, January 2024.

[54] See Monika Benkler, Ringen um Stabilität: Die neue EU-Mission in der Republik Moldova (Struggling for stability: The new EU mission in the Republic of Moldova), ZIF kompakt, 15 May 2023.

[55] See EU Partnership Mission in the Republic of Moldova (EUPM).

[56] See RTA, EU to Set Up Rapid Response Team to Support Moldova in Combating Hybrid Threats, 25 April 2025.

## Lessons Learned

The lessons learned from the EUPM Moldova are particularly helpful – both for peace operations and for future *ad hoc* interventions in hybrid contexts.

The lessons learned from the EUPM Moldova are relevant both for peace operations for future *ad hoc* interventions in hybrid context.

1. Even though destabilising operations are the current focus, the spectrum of hybrid threats goes beyond the cyber and information space. In both Ukraine and Moldova, hybrid attack strategies continue to target systemic vulnerabilities in particular (a) in critical infrastructure (e.g., disrupting telecommunications networks and power supply), (b) in financial flow monitoring (e.g., financing anti-constitutional parties, recruiting saboteurs, or equipping and paying demonstrators) and (c) in the area of the rule of law (e.g., exploiting legal loopholes or attempting to corrupt particularly under-resourced parts of the government).

2. Successfully countering such activities requires two elements, as seen in Ukraine and experimentally implemented by the EU in Moldova using specialised task forces: (a) in the event of an active threat, rapidly deployable expertise in key areas of national security for intervention, operational support and prevention of further destabilisation; and (b) following hybrid attacks, strategic advisory expertise to permanently remedy the systemic vulnerabilities that have been exploited (e.g., Ukraine after a ceasefire/EUAM Ukraine).

### Dynamic development of support structures and expertise clusters

With the increase in hybrid conflict activities, international organisations have established various clusters of expertise, training programmes and support structures in the hybrid field, particularly in the last decade. Since 2017, the Hybrid CoE, founded by EU and NATO member states, has served as a specialised research, advisory and training facility for partner countries, supporting EU CSDP missions and conducting extensive groundwork in the field of hybrid threats.

The EU has also established centres of excellence, research structures and support mechanisms on hybrid issues at various levels. At the Commission level, experts at the EU Joint Research Centre conduct research and provide advice on hybrid threats and FIMI, while both the Foreign Policy Instruments (FPI) and various Directorates General of the Commission – DG HOME (Home Affairs) and DG DEFIS (Defence Industry and Space), as well as DG NEAR (European Neighbourhood and Enlargement Negotiations) and DG CONNECT (Communications Networks, Content and Technology) – support activities and provide project funding in the fields of FIMI, cyber and critical infrastructure. In addition, several StratCom (Strategic Communication) Task Forces[57] have been created within the EEAS to specifically analyse FIMI dynamics and to support and train CSDP missions in the field of disinformation, while the EEAS Hybrid Fusion Cell prepares broader analyses and conducts training.

NATO also supports its member states and selected partners in dealing with hybrid threats through knowledge sharing, training and joint exercises and has developed and adapted strategies for this purpose.[58] In the areas of disinformation, cyber and energy security, the Alliance has created three centres

[57] See EEAS Strategic Communication Task Forces.

[58] See FN 2.

of excellence to promote and expand training and knowledge sharing among Alliance partners: the Strategic Communications Centre of Excellence in Riga, Latvia, the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, and the Energy Security Centre of Excellence in Vilnius, Lithuania.

At the OSCE, the topics of hybrid threats and cybersecurity are handled primarily by the Secretariat in the TNTD, while hybrid threat dynamics are monitored and analysed by the OSCE Conflict Prevention Centre (CPC). At the UN, a two-year work stream established in 2022 has, among other things, been supporting peace operations with training, tools and expertise in the areas of misinformation, disinformation, malinformation and hate speech. In 2023, this was structurally anchored in the Department of Peace Operations (DPO) in the shape of the Information Integrity Unit.

## 4.3 Multinational rapid response capabilities

The ability to detect hybrid activities at an early stage, counter them swiftly and, if necessary, repair any damage quickly is crucial for a state's national security – as well as for peace operations. The EU Rapid Response Teams can be deployed to support both their member states, CSDP operations and partner countries.[59]

In 2018, the EU Cyber Rapid Response Team (CRRT)[60] was established under Lithuanian leadership within the Permanent Structured Cooperation (PESCO), with the aim of "responding to cyber incidents and ensuring a higher level of cyber resilience." To assess vulnerabilities and assist in improving cyber defence, it was deployed first to Moldova in 2022, then as part of the European Union Training Mission in Mozambique (EUTM Mozambique) in 2023, and then again to Moldova in 2023. To date, the instrument has not been used in an actual crisis because the EU CRRT process has not been able to "reach decisions and deployments in reasonable time frames."[61]

Given the diverse attack modes of hybrid threats, rapid and integrated intervention concepts such as the EU Hybrid Rapid Response Team appear promising and groundbreaking.

The EU Hybrid Rapid Response Team was then established in 2024 as an instrument of the EU Hybrid Toolbox and serves to prevent and counter hybrid threats. As one of the key outcomes of the Strategic Compass for Security and Defence 2022, the teams are intended to provide short-term, tailored and targeted support to member states, CSDP operations and partner countries.[62] From 28 April to 09 May 2025, such a team assisted the Republic of Moldova for the first time in its fight against external interference in the run-up to the parliamentary elections (September 2025).[63]

Due to the diverse attack modes of hybrid threats, which are not limited to individual sectors such as cyberspace but align with systemic vulnerabilities, rapid and integrated intervention concepts such as the EU Hybrid Rapid Response Team appear promising and groundbreaking.

[59] NATO also has rapid response capabilities – the NATO Cyber Rapid Reaction Team (since 2012) and the NATO Counter Hybrid Support Team (since 2018) – but these are primarily available to NATO institutions and allies.

[60] See Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT).

[61] Taylor Grossman, Cyber Rapid Response Teams. Structure, Organization and Use Cases, Centre for Security Studies (CSS), ETH Zurich, November 2023, p. 33.

[62] See Council of the European Union, Hybrid threats: Council paves the way for the deployment of rapid response teams to address hybrid threats, 21 May 2024.

[63] See EEAS, Moldova: Remarks by High Representative Kaja Kallas at the joint press conference following the Association Council meeting, 04 June 2025.

## 4.4 Cooperation with the private sector

For tech companies, preventive and reactive activities in cyberspace and the information space are part of their business model. In the wake of Russia's war of aggression against Ukraine, actors such as Google's Threat Analysis Group (TAG) and Microsoft's Threat Intelligence Centre (MSTIC) are using their technical capabilities specifically to defend the country under attack.[64] In view of the spread of modern conflicts into cyberspace and the lower capabilities and capacities of international organisations to manage them compared to private tech actors, the former UN Under-Secretary-General for Peace Operations, Jean-Marie Guéhenno (et. al.), recently advocated for a new multi-stakeholder model from "traditional peace enforcers (to handle military and diplomatic tasks) and technology companies (to disrupt cyber or disinformation operations)."[65] Guéhenno proposes a hybrid model that combines the capabilities of the private sector with the legitimacy of states and multilateral institutions.

The involvement of tech companies in international crisis management undoubtedly offers opportunities. At the same time, it entails a number of problematic issues and risks. These include a lack of democratic control and accountability, commercial conflicts of interest and the associated unpredictability of engagement, as well as security and espionage concerns, particularly when dealing with sensitive data.[66]

The involvement of tech companies in international crisis management undoubtedly offers opportunities, but at the same time entails problematic issues and risks.

Apart from institutionalised cooperation with private sector actors in international crisis management, the rapidly developing analytical tools of various tech companies are already playing an increasing role in peace operations and in dealing with hybrid threats. In the past, AI-supported monitoring and analysis tools were expensive, complicated and mostly reserved for intelligence services. Today, they are increasingly affordable and allow for comprehensive monitoring of the cyber and information space, aggregation of a wide variety of information channels, and rapid reinforcement of partners threatened by hybrid activities through cost-effective off-the-shelf solutions.

### Cooperative stress test in Moldova

In the run-up to Moldova's September 2025 parliamentary elections, a Digital Hybrid Threats Simulation took place in Chișinău in June. In addition to Moldovan authorities, civil society organisations, fact checkers, independent media and international partners, representatives from Google, Meta and TikTok participated in the simulation. The aim was to raise awareness of potential disinformation campaigns and cyberattacks designed to disrupt the upcoming elections and to enable an effective response from all relevant actors.[67]

[64] See Shane Huntley, Fog of war: how the Ukraine conflict transformed the cyber threat landscape, Google Threat Analysis Group (TAG), 16 February 2023. Between January 2022 and September 2023, Ukraine was subjected to 2,776 cyberattacks. Cyber Peace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, 2023, p. 3.

[65] Jean-Marie Guéhenno, Olivia Grinberg, Jason Healey, A Multistakeholder Model of Cyber Peace, Lawfare, 07 February 2025.

[66] See Troy Smith, The Role of Private Entities in Hybrid Warfare. Navigating policy, legal frameworks, and cybersecurity challenges, EU Cyber direct, 14 October 2024.

[67] See European Commission, Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova's parliamentary elections, 12 June 2025; see also NIS Cooperation Group, Compendium on Election Cybersecurity and Resilience, Updated Version, 06 March 2024.

# 5. Future challenges for operations in the context of hybrid threats – recommendations for German policymakers

International peace operations are often deployed in geopolitically contested areas and must protect themselves and their personnel from hybrid activities by state and non-state actors. Unlike states, they cannot employ credible deterrence, instead they must further bolster their resilience to attacks and proactively pursue an approach that does not focus on a singular phenomenon but rather shields their own information infrastructure as holistically as possible, controls internal communication channels and strategies, monitors the surrounding information space, and maintains close contact with national and international security actors. Personnel rotation in peace operations – a significant weak point in the shielding and control of internal processes, information and structures – can be countered by harmonising the system and the infrastructure, and tightening process control.

Hybrid dynamics require mission mandates to be highly adaptable and mission personnel to have technical expertise.

Having had to handle hybrid conflict activities, peace operations have implemented new approaches in recent years. These must now be further developed in view of the growing use of the hybrid toolbox by state and non-state actors. Hybrid dynamics require mission mandates to be highly adaptable and mission personnel to have technical expertise that has so far been limited, ranging from experts in strategic communication and intelligence analysis to specialised cyber defence. Against this backdrop, the experimental EUPM Moldova model is groundbreaking. It combines medium-term resilience building as a key measure for strengthening states with the short-term deployment of a team of experts for special needs – supplemented by the new EU Hybrid Rapid Response Team.

In the future, it will probably be impossible to ignore the capabilities of large tech companies when it comes to securing peace.

Given the polarised Security Council, in which some member states prefer UN peace operations to focus on core tasks, it is currently difficult to imagine expanding mandates into the cyber and information space. For the time being, the UN will therefore continue to focus on building resilience in host countries. Nevertheless, proposals such as establishing a hybrid model or expanding cooperation with the private tech sector are being put forward at the right time. In the future, the capabilities of large tech companies to contribute to securing peace cannot be ignored, making it necessary to establish new partnerships and expand existing ones.

## Recommendations

In view of the global rise in hybrid conflict activities, there will be a growing need for resilience-building missions and short-term interventions. For German policymakers, recommendations emerge along three central lines of action:

### → Promoting and strengthening multilateral approaches and capabilities in the field of hybrid threats

In view of multidimensional challenges, it is essential that German civilian crisis management remains firmly embedded in existing multilateral efforts. National security policy priorities may be shifting toward national and alliance defence. But given the destabilising effect of hybrid activities on Germany's own security, as well as on EU partner countries and its neighbourhood, and given its expertise on hybrid security issues, Germany is well-placed to play a lead role in further developing and implementing peace operations and short-term interventions to ward off hybrid threats.

Germany should play a leading role in further developing and implementing peace operations and short-term interventions to counter hybrid threats.

Strong and sustained participation in experimental, resilience-building, multilateral initiatives such as the EUPM Moldova, and partially also the EUAM Ukraine, is advisable for two reasons: First, German support strengthens important multilateral approaches to tackling new hybrid challenges in a targeted manner, especially when finite resources limit the effectiveness of bilateral solo efforts. Second, the operational knowledge that German experts gained from contexts involving active hybrid threats or even hybrid warfare can (a) directly feed into the further development of German capabilities and expertise in the hybrid domain and (b) provide insights and experience relevant to the German national context.

To counter acute hybrid activities, rapid, time-bound interventions with lean, specialised task forces are particularly useful. Germany should continue to participate actively in further promoting and supporting suitable instruments such as the EU Hybrid Rapid Response Team – politically, conceptually and in terms of personnel – as well as maintain its own expertise.

### → Creating synergies among structures and measures, and bundling them efficiently

Multilateral and national defence approaches have multiplied in a dynamically developing field of hybrid threats, at least since the annexation of Crimea in 2014. A deeper understanding of the threat in Germany, and especially within its alliances and partnerships, has led – over a short period of time – to the emergence of new, bespoke structures and instruments, which could at times benefit from better coordination. Issues such as disinformation have generated a momentum of their own and are being addressed in silos.  The presence of peace operations, bilateral project financing, international organisations and non-governmental organisations, as for instance in Moldova, can threaten to overload national partners with a limited absorption capacity. In this context, Germany should support holistic approaches to the issue of hybrid threats, closely follow how structures are evolving, and focus its resources – both human and financial – in a way that minimises redundancy.

## → Efficient use of specialised expertise in the ZIF pool

Defending against hybrid threats in the context of peace operations requires a broad, networked approach, not least because aggressors operate covertly and target vulnerabilities through a wide variety of entry points. Germany has extensive expertise in the relevant ministries on the subject of hybrid threats and has proven experts working in various peace operations and institutions (EU, UN, OSCE and NATO). The secondment of personnel in leadership positions from both the Federal Foreign Office/ZIF and the Federal Ministry of the Interior enabled, for example, the rapid and successful launch of EUPM Moldova. EUPM Moldova has also shown in the course of its work that there is a high demand for expert profiles in the hybrid field that can be mobilised quickly.

Due to the growing demand for dedicated expertise in various areas of national security – from analysts and cybersecurity experts to communications specialists and financial flow analysts – Germany should further expand its operational capabilities in the civilian sector and make targeted use of the existing expertise of the ZIF Expert Pool. In this way, Germany not only strengthens its ability to respond to hybrid threats at the international level, but also defends its values, interests and security.

Given the dynamic development of the hybrid toolbox, agility is an important factor when it comes to increasing Germany’s operational capability in the civilian sector.

# List of abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| CAR | Central African Republic |
| CERT | Computer Emergency Response Team |
| CSDP | Common Security and Defence Policy |
| DRC | Democratic Republic of the Congo |
| EEAS | European External Action Service |
| EU | European Union |
| EU CRRT | European Union Cyber Rapid Response Team |
| EUAM Ukraine | European Union Advisory Mission Ukraine |
| EUMA | European Union Mission in Armenia |
| EUPM Moldova | European Union Partnership Mission in Moldova |
| EUTM Mozambique | European Union Training Mission in Mozambique |
| FIMI | Foreign Information Manipulation and Interference |
| GA | General Assembly |
| GGE | Group of Governmental Experts |
| Hybrid CoE | European Centre of Excellence for Countering Hybrid Threats |
| ICTs | Information and Communications Technologies |
| IT | Information Technology |
| JNIM | Jama‘a Nusrat ul-Islam wa al-Muslimin |
| MINUSCA | United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic |
| MINUSMA | United Nations Multidimensional Integrated Stabilization Mission in Mali |
| MONUSCO | United Nations Organization Stabilization Mission in the Democratic Republic of the Congo |
| NATO | North Atlantic Treaty Organisation |
| NSA | Non-State Actor |
| OEWG | Open-ended Working Group |
| OSCE | Organisation for Security and Cooperation in Europe |
| POC | Protection of Civilians |
| SPM | Special Political Mission |
| StratCom | Strategic Communication |

| | |
|---|---|
| TNTD | Transnational Threats Department |
| UN | United Nations |
| UNAMI | United Nations Assistance Mission for Iraq |
| UN DPO | United Nations Department of Peace Operations |
| UNICC | United Nations International Computing Centre |
| UNIFIL | United Nations Interim Force in Lebanon |
| UNMISS | United Nations Mission in South |

www.zif-berlin.org