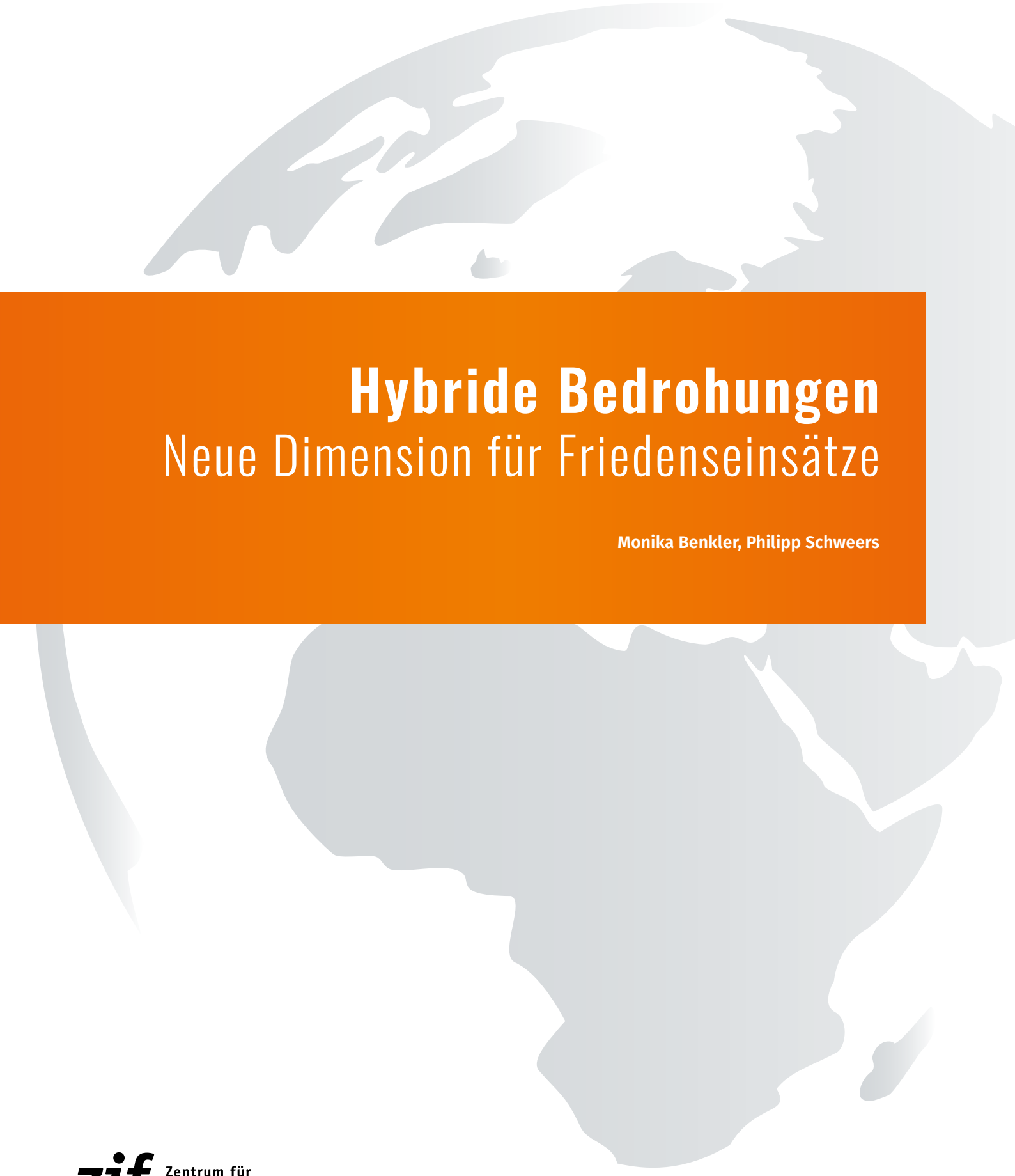
STUDIE | SEPTEMBER 2025



Hybride Bedrohungen
Neue Dimension für Friedenseinsätze

Monika Benkler, Philipp Schweers

zif Zentrum für Internationale Friedenseinsätze

Impressum

Herausgeber: 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

Geschäftsführerin: Dr. Astrid Irrgang
Aufsichtsratsvorsitzender: Staatsminister Florian Hahn

www.zif-berlin.org

Autor:innen: Monika Benkler, ZIF Team Policy, Partnerships & Innovation (PPI).
Philipp Schweers leitete im ersten Missionsjahr die Komponente *Hybrid Threats & Cyber Security* der EUPM Moldau und ist aktuell als Fachexperte an den Internationalen Strafgerichtshof sekundiert.

Unsere Publikationen beziehen regelmäßig das Einsatzwissen von ZIF-Sekundierten ein.

Die Studie ist gefördert durch das Auswärtige Amt.

Grafik & Layout: finedesign, Berlin

STUDIE | SEPTEMBER 2025

Hybride Bedrohungen

Neue Dimension für Friedenseinsätze

Monika Benkler, Philipp Schweers

zif Zentrum für Internationale Friedenseinsätze

Executive Summary

Hohe Dynamik in der Landschaft hybrider Bedrohungen: Zwar sind hybride Bedrohungen konzeptionell so alt wie die Kriegführung, doch hat die Kombination aus geopolitischen Systemverschiebungen und beschleunigter technologischer Innovation in den vergangenen Jahren zu einer deutlichen Zunahme im Hinblick auf Qualität, Intensität und Reichweite insbesondere von Seiten autokratischer Staaten geführt. Die leichte Zugänglichkeit digitaler Technologien hat zudem das Feld nichtstaatlicher Akteure deutlich erweitert, die autonom oder im Auftrag Dritter agieren. Diese Entwicklung hat unmittelbare Folgen für internationale Friedenseinsätze.

Friedenseinsätze zunehmend Ziel hybrider Aktivitäten: Zum einen sind Friedenseinsätze in den vergangenen Jahren verstärkt zum Ziel hybrider Aktivitäten geworden – nicht zuletzt mit der Absicht, internationales Engagement zu delegitimieren und friedensfördernde Maßnahmen zu unterwandern. Dabei sehen sie sich – im Unterschied zu Staaten, die in zahlreichen verschiedenen Sektoren hybride Aktivitäten verzeichnen – bisher am deutlichsten im Cyber- und Informationsraum angegriffen.

Friedenseinsätze als Akteur – neue Ansätze: Als Akteur in der Bearbeitung hybrider Konfliktaktivitäten haben Friedenseinsätze in den vergangenen Jahren neue Ansätze umgesetzt. Dazu gehören die Integration entsprechender Aufgaben in bestehende Einsätze, die Etablierung expliziter, fokussierter Missionen wie die *EU Partnership Mission in Moldova* (EUPM Moldova) oder der Einsatz von ad-hoc Instrumenten wie *Rapid Response Teams*. Diese Ansätze müssen nun angesichts der globalen Zunahme und Intensivierung hybrider Bedrohungen im sicherheitspolitischen Kontext weiterentwickelt werden. Eine Ausweitung der Mandate von UN-Friedenseinsätzen in den Cyber- und Informationsraum ist angesichts eines polarisierten Sicherheitsrats aktuell nur schwer denkbar. Dennoch kommen Vorschläge wie die Etablierung eines hybriden Modells bzw. Überlegungen zur verstärkten Zusammenarbeit mit dem privaten Tech-Sektor zum richtigen Zeitpunkt.

***Lessons learned* für Einsätze und ad-hoc-Interventionen im hybriden Kontext:** Die Erfahrungen der EUPM Moldau sind sowohl für Friedenseinsätze als auch für zukünftige ad-hoc-Interventionen im hybriden Kontext hilfreich: (1) Das Spektrum hybrider Bedrohungen beschränkt sich nicht auf den Informations- und Cyberraum, auch wenn dieser derzeitig einen Schwerpunkt destabilisierender Operationen bildet. Sowohl in der Ukraine als auch in Moldau haben hybride Angriffsstrategien insbesondere auf systemische Schwachstellen gezielt und tun dies weiterhin. (2) Die erfolgreiche Abwehr derartiger Aktivitäten erfordert (a) in einer aktiven Gefährdung zügig entsendbare Fachexpertise zur Intervention, operativen Unterstützung von nationalen Institutionen und darauf aufbauend Prävention weiterer Destabilisierung; und (b) im Nachgang strategische Beratungsexpertise in ebendiesen Themenfeldern, um die ausgenutzten systemischen Schwachstellen nachhaltig zu beheben.

Empfehlungen an die deutsche Politik: Der Bedarf an resilienzstärkenden Einsätzen und kurzfristigen Interventionen wird steigen. Deutschland sollte eine tragende, wenn nicht führende Rolle bei der weiteren Konzeptentwicklung und Umsetzung von Friedenseinsätzen und kurzfristigen Interventionen zur Abwehr hybrider Bedrohungen übernehmen. Eine anhaltend aktive, deutsche Beteiligung an der Weiterentwicklung von Instrumenten wie dem *EU Hybrid Rapid Response Team* – politisch, konzeptionell und personell – sowie das strukturierte Vorhalten eigener deutscher Expertise ist dringend anzuraten. Aufgrund steigenden Bedarfs an dezidierter Fachexpertise in den unterschiedlichen Themenfeldern der nationalen Sicherheit – von Analytiker:innen über *Cyber Security*-Expert:innen zu Kommunikationsspezialist:innen und Analyst:innen für Finanzströme – ist es empfehlenswert, die deutsche Einsatzfähigkeit im zivilen Bereich weiter zu erhöhen und die vorhandene Expertise des ZIF *Expert Pool* gezielt zu nutzen.

Einleitung

Vor dem Hintergrund geopolitischer Spannungen, globaler Vernetzung und leicht zugänglicher innovativer digitaler Technologien nehmen hybride Bedrohungen kontinuierlich zu und werden von einer wachsenden Palette vorrangig autokratischer staatlicher sowie nichtstaatlicher Akteure für die eigene Interessendurchsetzung genutzt. Am Beispiel des Konfliktgeschehens seit 2022 in der Ukraine ist erkennbar, dass die flankierende Durchführung hybrider Aktivitäten wie Informations- und Cyberkampagnen sowie gesellschaftliche Störmanöver und Angriffe auf kritische Infrastruktur eine steigende Relevanz auch in der konventionellen Kriegführung hat.

Diese Entwicklungen haben für internationale Friedenseinsätze[1] unmittelbare Folgen. Zum einen sind sie in den vergangenen Jahren vermehrt zum Ziel hybrider Aktivitäten insbesondere im Cyber- und Informationsraum geworden – nicht zuletzt mit der Absicht, internationales Engagement zu delegitimieren und friedensfördernde Maßnahmen zu unterwandern. Zum anderen stellen die globale Zunahme und Intensivierung von hybriden Bedrohungen im sicherheitspolitischen Kontext internationale Organisationen und Friedenseinsätze vor die Herausforderung, als Akteur Ansätze zur Bearbeitung hybrider Konfliktaktivitäten (weiter) zu entwickeln. Dazu gehören insbesondere die Integration entsprechender Aufgaben oder Strukturen in bestehende oder künftige Einsätze, die Etablierung expliziter, fokussierter Missionen, der Einsatz von *Rapid Response Teams* oder Partnerschaften mit Unternehmen der Tech-Industrie.

Diese Studie analysiert die Herausforderungen einer zunehmend komplexen Landschaft hybrider Bedrohungen für internationale Friedenseinsätze und erarbeitet daraus resultierende konzeptionelle und personelle Handlungsfelder sowie Empfehlungen für die deutsche Politik.

Inhalt

1 In dieser Veröffentlichung verstehen wir unter dem Begriff „Friedenseinsätze" das gesamte Spektrum von kleineren feldbasierten Missionen bis hin zu großen multidimensionalen Einsätzen.

1. Begriffsklärung

Die Einnahme der Halbinsel Krim durch Russland 2014 war ein Weckruf für die internationale Gemeinschaft, die Bedrohung durch hybride Aktivitäten ernst zu nehmen. In der Folge legten internationale Organisationen seit 2015 Ansätze zum Umgang mit hybriden Bedrohungen (*hybrid threats*) und hybrider Kriegführung (*hybrid war/warfare*) vor. Die NATO verabschiedete im Dezember 2015 ihre erste formale *Strategy on NATO's Role in Countering Hybrid Warfare*.[2] Wenige Monate später, im April 2016, folgte die Europäische Union (EU) mit ihrem *Joint Framework on Countering Hybrid Threats: A European Union Response*.[3] Der Sicherheitsrat der Vereinten Nationen (UN) diskutierte hybride Kriege als Bedrohung für den internationalen Frieden und die internationale Sicherheit erstmals im März 2017 im Rahmen eines informellen *Arria-formula-Meeting*.[4]

Hybrider Krieg ist eine Art von Aktivität im möglichen Einsatz hybrider Bedrohungen und steht am Ende des Eskalationsspektrums.

Trotz ihrer Verankerung in Strategiedokumenten und der fortdauernden Präsenz in der sicherheitspolitischen Debatte, hat sich für die Begriffe „Hybride Bedrohungen" und „Hybrider Krieg / Hybride Kriegführung" seit ihrer Einführung[5] keine allgemeingültige Definition herausgebildet. Oft werden sie synonym verwendet – sind aber voneinander abzugrenzen. In dieser Studie wird dem Verständnis des 2017 von EU- und NATO-Mitgliedstaaten gegründeten *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE) gefolgt:[6]

Hybride Bedrohungen, Hybrider Krieg/Hybride Kriegführung

- **Hybride Bedrohungen** sind schädliche Aktivitäten eines Opponenten, die mit bösartiger Absicht geplant und gezielt verdeckt durchgeführt werden, um eine Zuordnung (*attribution*) zu verhindern. Sie wollen ein Ziel, z. B. einen Staat oder eine Institution, durch eine Vielzahl von Mitteln, die häufig kombiniert werden, untergraben, destabilisieren oder delegitimieren, um eigene politische Einflussziele durchzusetzen. Zu diesen Mitteln gehören Informationsmanipulation, Cyberangriffe, wirtschaftliche Einflussnahme oder Nötigung, verdeckte politische Manöver, Wahlmanipulation, Zwangsdiplomatie oder die Androhung militärischer Gewalt. Hybride Bedrohungen beschreiben eine breite Palette schädlicher Aktivitäten mit unterschiedlichen Zielen, die von der Einmischung (*Interference*), Einflussnahme (*Influence*), Operation (*Operation*) bis hin zur hybriden Kriegführung (*War/Warfare*) reichen.
- **Hybrider Krieg/Hybride Kriegführung** ist *eine* Art von Aktivität im möglichen Einsatz hybrider Bedrohungen und steht am Ende des Eskalationsspektrums. Diese ist – im Unterschied zu den anderen Varianten – durch den Einsatz *auch* militärischer Mittel (verdeckt oder offen) definiert. Ein Beispiel dafür sind die „grünen Männchen" – russische Soldaten ohne Hoheitsabzeichen –, die 2014 die Krim besetzten. Nicht jede Form unerwünschten Vorgehens unter Einsatz des hybriden Instrumentenkastens ist demnach als hybrider Krieg zu deklarieren.

2 Die Strategie basiert auf den drei Pfeilern Vorbereitung (*preparedness*), Abschreckung (*deterrence*) und Verteidigung (*defence*) und bildet seit 2015 die Grundlage für den Umgang der NATO mit hybriden Aktivitäten. Zur Entwicklung s. 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.

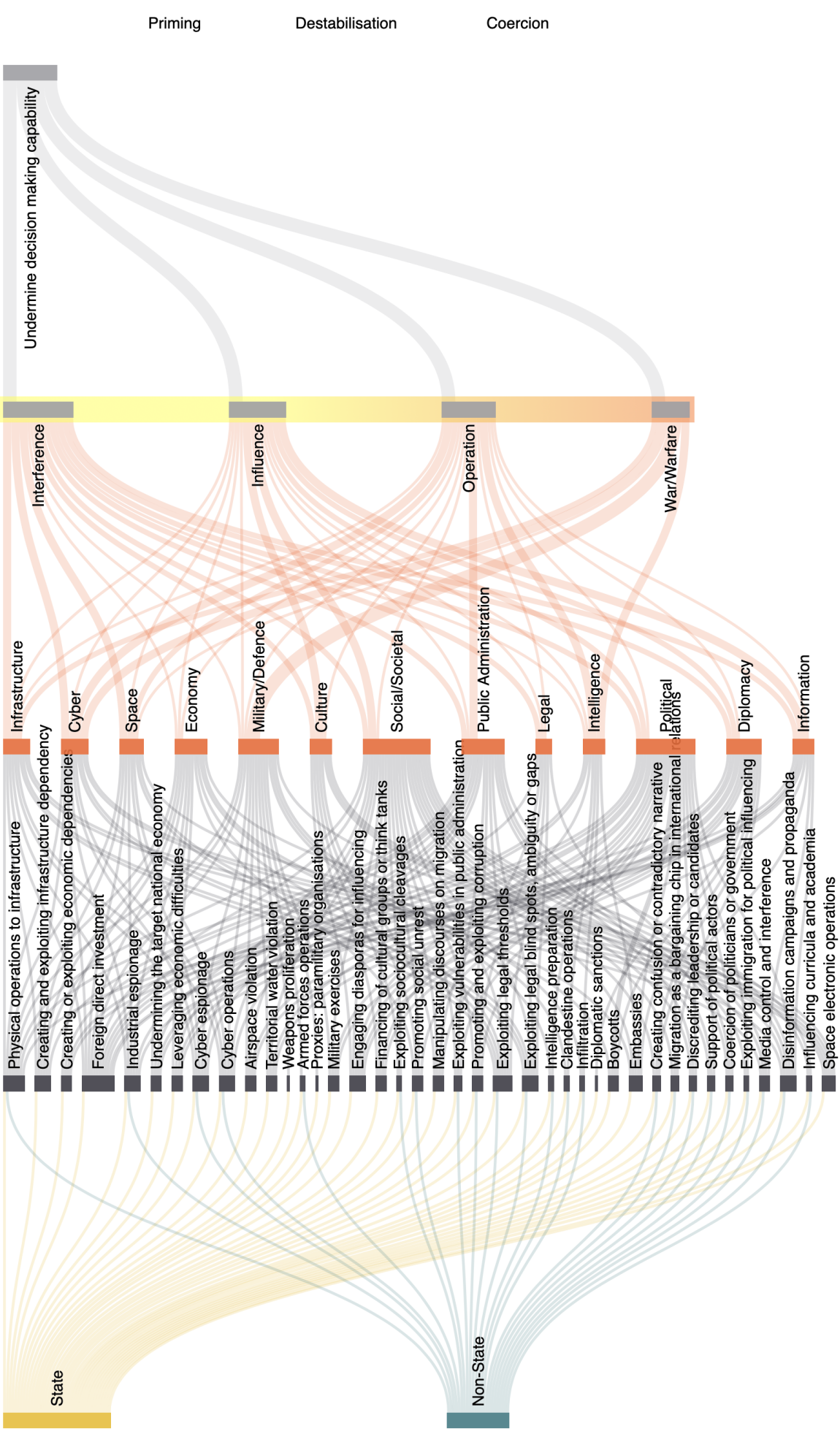
3 S. Joint Framework on Countering Hybrid Threats: A European Union Response. Seit 2016 hat die EU ihre Antwort auf hybride Aktivitäten kontinuierlich weiterentwickelt. S. dazu: European Council and Council of the European Union, A coordinated EU response to hybrid threats, Last review: 20 May, 2025.

4 Das Treffen mit dem Titel „Hybrid Wars as a Threat to International Peace and Security", initiiert von der Ukraine, zielte darauf ab, das Konzept der hybriden Kriegsführung und deren Auswirkungen auf den internationalen Frieden und die internationale Sicherheit zu diskutieren.

5 Nachdem der Begriff „Hybrid War" bereits in den 1990er Jahren vereinzelt in der Literatur verwendet worden war, setzte eine Veröffentlichung des amerikanischen Militärtheoretikers Frank G. Hoffman im Jahr 2007 eine breitere Diskussion dazu in Gang. Mit Blick auf das Vorgehen der Hisbollah gegen Israel im zweiten Libanonkrieg 2006 beschrieb er die Vorgehensweise zumeist nichtstaatlicher bewaffneter Gruppen, die sich konventioneller und irregulärer Methoden der Operationsführung bedienen, um technologisch übermächtige Gegner zu bekämpfen. S. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, December 2007.

6 Vgl. European Centre of Excellence for Countering Hybrid Threats, abgerufen am 29.06.2025 sowie Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou (Eds.), The Landscape of Hybrid Threats: A Conceptual Model, Public Version, European Commission and Hybrid CoE, 2021, S. 11.

The landscape of Hybrid Threats: Visualization of the conceptual model



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, S. 13.

2. Neue Technologien – neue Qualität

In einer kontrovers geführten Debatte wurden in der vergangenen Dekade der analytische Nutzen der Begriffe Hybride Bedrohungen und Hybrider Krieg ebenso in Frage gestellt wie die Neuheit des Konzeptes.[7] Tatsächlich sind hybride Formen der Konfliktführung so alt wie die Geschichte von Krieg und Konflikt.[8] Dabei ist allerdings zu berücksichtigen, wie sehr moderne Technologien – und insbesondere die dadurch beförderte Entwicklung des Cyber- und Informationsraums als weiteres „Gefechtsfeld" – neue Möglichkeiten der Interessendurchsetzung eröffnet, sich Umfang und Reichweite hybrider Aktivitäten daher erhöht und Akteure diversifiziert haben.

Das exponentielle Entwicklungstempo generativer künstliche Intelligenz wird den hybriden Instrumentenkasten weiter verstärken.

So hat die zunehmende technologische Automatisierung im Cyber- und Informationsraum Reichweite und Schadenspotential hybrider Aktivitäten in den vergangenen zehn Jahren deutlich vergrößert – zum Beispiel in Form von Manipulation sozialer Medien durch sogenannte Bot-Netzwerke oder von Angriffen auf kritische Infrastruktur (KRITIS) und Cyberinfrastruktur durch zunehmend spezialisierte Schadprogramme (sog. *Advanced Persistent Threats* / APT).[9] Die erweiterten möglichen Schadensszenarien auf Grund beschleunigter technologischer Innovation haben die NATO auf ihrem Brüsseler Gipfel 2021 dazu veranlasst, böswillige kumulative Cyberaktivitäten gegen ein Mitglied unter bestimmten Umständen als feindlichen militärischen Angriff zu definieren, der die Aktivierung von Art. 5 des Nordatlantikvertrages erlaubt.[10]

Das exponentielle Entwicklungstempo generativer künstliche Intelligenz (KI) wird den hybriden Instrumentenkasten weiter verstärken.[11] Gleiches gilt aber auch für mögliche neue Abwehrstrategien von hybriden Angriffen, die bei entsprechender Nutzung von KI schädliche Aktivitäten im Informations- und Cyberraum – sei es bei der Aktivitätsüberwachung sozialer Medien, dem Monitoring auffälliger Finanzströme oder dem Schutz vernetzter kritischer Infrastruktur – schneller identifizieren und abwehren können.[12]

7 S. u.a. Michael Rühle, Aufstieg und Fall des hybriden Krieges, in: Internationale Politik 5/2023, S. 87-91; Lennart Maschmeyer, Assessing Hybrid War: Separating Fact from Fiction, CSS Analyses in Security Policy, Nr. 332, November 2023, ETH Zürich; Libiseller Chiara, "Hybrid warfare" as an academic fashion, Journal of Strategic Studies, 2023, Vol. 46, No. 4, pp. 858–880.

8 S. Johann Schmid, Hybride Kriegführung – Erklärstück, Bundeswehr, 14.12.2022.

9 S. u.a. 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, 12.09.2022; Manel Medina Llinàs, Hybrid Attacks on Critical Infrastructure, CIDOB, 09/2022.

10 S. NATO, Brussels Summit Communiqué, 14 June 2021. S. dazu auch: Sarah Wiedemar, Die NATO und Artikel 5 im Cyberraum, CSS-Analysen zur Sicherheitspolitik, Nr. 323, Mai 2023, ETH Zürich.

11 S. u.a. 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, May 27, 2025.

12 S. 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. Friedenseinsätze als Ziel hybrider Aktivitäten

3.1 Schädliche Informationen

Im Unterschied zu Staaten, die in zahlreichen verschiedenen Sektoren hybride Aktivitäten verzeichnen, sehen sich Friedenseinsätze bisher am deutlichsten im Cyber- und Informationsraum angegriffen. *Harmful Information* (UN), *Foreign Information Manipulation and Interference* / FIMI (EU) oder *Information Threats* (NATO) dienen böswilligen Akteuren oft als Instrument zur Förderung umfassender strategischer Ziele in Ländern und Regionen, in denen sie ihren Einfluss ausweiten wollen. In Afrika, der Region mit den umfangreichsten UN-Einsätzen, hat sich die Zahl der Desinformationskampagnen von 50 (2022) auf 189 (2024) fast vervierfacht. 60 Prozent davon gingen von externen staatlichen Akteuren aus – mit Russland an der Spitze (rund 40 Prozent).[13] In anderen Regionen, etwa dem Südkaukasus oder Westlichen Balkan, zeigt sich ein ähnliches Bild im Hinblick auf Ausmaß und Akteure.[14]

Friedenseinsätze sehen sich bisher am deutlichsten im Informations- und Cyberraum durch hybride Aktivitäten angegriffen.

Für Friedenseinsätze wie die UN-Mission MONUSCO in der Demokratischen Republik Kongo (DRC) oder die *EU Mission in Armenia* (EUMA) sind schädliche Informationen eine permanente Herausforderung. Sie werden dadurch zum Teil massiv in ihrem Ansehen beschädigt, das Vertrauen der Bevölkerung in ihre Arbeit – Basis für eine erfolgreiche Mandatsumsetzung – geht verloren, die Sicherheit der Einsatzkräfte ist bedroht. Eine aktuelle Untersuchung von schädlichen Online-Informationen und -Narrativen in der Phase des Abzugs von MINUSMA aus Mali (Juni bis Dezember 2023) zeigt laut UN DPO, „*that disinformation can serve as a sign of a strategic and existential threat to missions*“[15]. Im Falle MINUSMAs half sie dabei, „*to reinforce and justify its removal*“[16].

Die Untersuchung zu MINUSMA macht zudem den transnationalen Charakter der Bedrohung deutlich. Die Verknüpfung negativer MINUSMA-Narrative mit vermeintlichen Gemeinsamkeiten anderer „böswilliger“ Missionen in der Region – insbesondere MONUSCO in der DRC und MINUSCA in der Zentralafrikanischen Republik (ZAR) – weist, so der Bericht, auf das Ziel, „*to broaden the perspective and delegitimise the UN Peacekeeping enterprise*“[17]. Auch der jüngste FIMI-Report des Europäischen Auswärtigen Dienstes (EAD) konstatiert angesichts der russischen FIMI-Infrastruktur in Afrika eine „*long-term, multi-layered strategy developed over recent years*“[18], die das westliche und europäische Engagement herausfordere.

13 S. Africa Center for Strategic Studies, Mapping a Surge of Disinformation in Africa, March 13, 2024.

14 S. Digital Forensic Research Lab, In Europe and the South Caucasus, the Kremlin leans on energy blackmail and scare tactics, Issue Brief, February 29, 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, 1 June - 31 December 2023, 2024, S. 34.

16 Ebd., S. 3.

17 Ebd. S. 33.

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

Strategien im Kampf gegen schädliche Informationen[19]

Die Ausbreitung von Angriffen gegen Friedenseinsätze in den digitalen Raum führt zu der Notwendigkeit, die Abwehr von Einsätzen gegen schädliche Informationen und externe Einflussnahme zu stärken. Dies geschieht im Rahmen von internationalen Friedenseinsätzen zunehmend systematisch.[20] Neben (1) Monitoring/Analyse (*Situational Awareness*) stehen (2) reaktive sowie proaktive und präventive Maßnahmen wie Strategische Kommunikation oder *Community Engagement* und damit zusammenhängend (3) der Aufbau eigener Resilienz und (4) die Zusammenarbeit mit Partnern als Handlungsfelder im Fokus. Da der Zusammenhang zwischen schädlichen Aktivitäten im Informationsraum und Cyberangriffen häufig eng ist, muss der Resilienzaufbau die Cybersicherheit von Missionen einschließen.

3.2 Cyberangriffe

Das *United Nations International Computing Centre* (UNICC), eine spezialisierte Organisation innerhalb des UN-Systems, stellte in seinem jüngsten *Cyber Threat Landscape Report* fest, dass „*Malicious Activities of Interest*"[21] – dazu gehören auch Cyberangriffe – gegen UN-Organisationen an Häufigkeit und Schwere zunehmen. 2023 seien 46 von UNICC betreute UN-Organisationen angegriffen worden. Im Vergleich zum Vorjahr stieg die Zahl der Vorfälle laut Bericht um 170 Prozent – mit dem vorrangigen Ziel der Beschaffung sensibler Informationen und Daten (48 Prozent), gefolgt von finanziellem Gewinn (42 Prozent).[22] Auch für Friedenseinsätze hat sich die Gefährdungslage durch Cyberangriffe in den vergangenen Jahren erheblich verschärft. UN-Generalsekretär António Guterres wies 2023 vor dem Sicherheitsrat darauf hin, dass KI-gestützte Cyberangriffe gegen Friedenseinsätze eingesetzt würden.[23] Der EAD konstatierte 2021, dass die (militärischen) Missionen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) zunehmend Bedrohungen aus dem Cyberraum ausgesetzt seien.[24] Konkrete Zahlen und Fälle von Cyberattacken im Rahmen von Friedenseinsätzen sind schwer öffentlich nachvollziehbar, eindeutig ist jedoch, dass die zunehmende Digitalisierung von Friedenseinsätzen diese – neben ihren diversen positiven Auswirkungen auf die Effizienz in der Mandatsumsetzung – auch verwundbarer gemacht hat.

Für Friedenseinsätze hat sich die Gefährdungslage durch Cyberangriffe in den vergangenen Jahren erheblich verschärft.

Die Nutzung ausgefeilterer Tools zur Informationsgewinnung und -verwaltung in Friedenseinsätzen bedeutet, dass in den Missionsnetzwerken neue, hochsensible und stark zentralisierte Arten von Daten aufbewahrt werden, die für Konfliktakteure nützlich sein können und damit potenzielle Ziele von Cyberangriffen sind.[25] Die Verwendung dieser Daten etwa für einen physischen Angriff auf ethnische Gruppen oder Einzelpersonen hätte fatale Folgen für das Vertrauen der Bevölkerung in eine Mission. Gefährdet ist aber auch das Einsatzpersonal selbst, etwa wenn operationsrelevante Daten über Patrouillen exfiltriert oder mittels Cyberangriffen der Zugang zu Informationen verhindert bzw. Kommunikationskanäle gestört werden. Darüber hinaus sehen sich Einsatzkräfte zunehmend mit *Hacking*-Versuchen konfrontiert, die darauf abzielen, sie persönlich zu unterminieren.[26]

Internationale Organisationen haben verschiedene Maßnahmen etabliert, um ihre Friedenseinsätze gegen Cyberbedrohungen zu stärken, dazu gehören die Etablierung von *Computer Emergency Response Teams* (CERT), die systematische Integration und Überwachung eigener IT-Infrastruktur, aber auch Teams für die rasche Reaktion, die im Missionskontext und zur Unterstützung von Mitgliedstaaten und Partnerländern präventiv und reaktiv eingesetzt werden können (s. u.).

19 S. Monika Benkler, Annika S. Hansen, Lilian Reichert, Der Schutz der Wahrheit: Friedenseinsätze und Desinformation, ZIF-Studie, September 2022.

20 S. UN DPO, Policy on Information Integrity in Peacekeeping Settings (16 Dezember 2024); EEAS, Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI), 14.03.2025; NATO, NATO's approach to counter information threats, 23.06.2025.

21 UNICC verwendet den Begriff „böswillige Aktivitäten von Interesse", um alle Cyber-Bedrohungen, Sicherheitsvorfälle und Ereignisse zu klassifizieren, die auf UN-Organisationen abzielen und die für die Verbesserung der proaktiven Cyber-Abwehr von Bedeutung sind. UNICC, Cyber Threat Landscape Report 2023, May 2024, S. 4.

22 Ebd., S. 9.

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

24 S. EEAS, European Union Military Vision and Strategy on Cyberspace as a Domain of Operations, 2021, S. 5.

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

3.3 Erweitertes Akteursfeld

Das Feld der Akteure, die mit hybriden Bedrohungen die Mandatsumsetzung von Friedenseinsätzen erschweren, hat sich in den vergangenen Jahren deutlich erweitert. Auf staatlicher Seite versuchen insbesondere Großmächte wie Russland und China, beide ständige Mitglieder im UN-Sicherheitsrat, aber auch aufstrebende Mittelmächte, mit hybriden Aktivitäten Einfluss auf politische Prozesse in Einsatzländern von Friedensmissionen zu nehmen und die Glaubwürdigkeit sowie Legitimität von Einsätzen zu untergraben.[27] Auch wenn hybride Werkzeuge meist unterhalb der militärischen Schwelle angewendet werden, zeigen insbesondere das russische Vorgehen[28], aber auch Aktivitäten anderer Akteure, dass das gesamte Spektrum hybrider Aktivitäten verstärkt von staatlichen Militärapparaten und Geheimdiensten unter Verwendung militärischer Planung und entsprechender Ressourcenbereitstellung eingesetzt wird.[29]

Neben staatlichen, spielen bewaffnete und unbewaffnete nichtstaatliche Akteure eine wichtige Rolle, die autonom oder im Auftrag Dritter agieren.

Zum Instrumentenkasten gehört dabei auch der Einsatz von Militär- und Sicherheitsunternehmen (*Private Military Companies / PMC, Private Security Companies / PSC*) wie die russische Wagner-Gruppe (und ihre Nachfolgeorganisation Afrikakorps) oder chinesische Sicherheitsunternehmen[30], die in Ländern wie der ZAR oder Südsudan parallel zu Friedenseinsätzen arbeiten, Konfliktdynamiken mit verdeckten Aktivitäten beeinflussen und Friedenseinsätze in der Mandatsumsetzung behindern.[31] In der ZAR verbreiteten mit Russland und Wagner verbundene Medien in Zusammenarbeit mit lokalen Netzwerken von Journalist:innen und Influencer:innen Gerüchte über Verbindungen der Friedenstruppen mit nichtstaatlichen bewaffneten Gruppen und Terrorist:innen. Infolge der konkreten Anschuldigung, mit Überwachungsdrohnen Bomben auf russische Lager abzuwerfen, untersagte die Regierung MINUSCA die Nutzung von Drohnen, was ihre Beobachtungsfähigkeiten stark einschränkte – insbesondere in Gebieten, zu denen sie keinen physischen Zugang hatte.[32]

Daneben spielen bewaffnete und unbewaffnete nichtstaatliche Akteure (*Non-State Actors* / NSAs) eine wichtige Rolle. Sie agieren autonom (z. B. lokale Rebellengruppen in der Zentralafrikanischen Republik, extremistische Gruppierungen wie die Dschihadistengruppe JNIM im Sahel) oder im Auftrag Dritter. Angriffe, bei denen NSAs als Stellvertreter (*Proxies*) eingesetzt werden, nehmen global an Zahl und Intensität zu: „*It is cost-effective, deniable, and risk-averse. It allows the sponsor to benefit from the proxy's local or specialist knowledge, while minimizing the risk of retribution.*"[33] Für die NSAs bietet diese „Beziehung" nicht nur die Gelegenheit zur Ressourcenmaximierung, sondern auch die gesteigerte Chance, eigene strategische Ziele zu erreichen.[34] Dabei werden Strukturen der organisierten Kriminalität, *Hackers-for-hire*, *Cyber Mercenaries*, staatsnahe Unternehmen oder nichtstaatliche Kultureinrichtungen als *Proxies* ebenso genutzt wie offizielle Medien, diplomatische Vertretungen oder Influencer:innen.[35]

Verfügbare Daten weisen darauf hin, dass ein komplexes Netz aus Akteuren an der Produktion und Distribution schädlicher Information gegen die Ende 2023 abgezogene UN-Mission MINUSMA in Mali beteiligt war, die sich unter anderem gegen ihre Reputation richteten und ihre Ausweisung priesen. Eine herausragende Rolle spielten dabei lokale und internationale *Social Media Influencer*, die Berichten zufolge von nationalen und externen Akteuren finanziert wurden.[36]

27 S. 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, May 02, 2025.

28 Man spricht hier auch vom sog. russischen „hybrid playbook", das sich durch Praxistests im Georgienkrieg 2008 über die Krim 2014 bis hin zum derzeitigen Angriffskrieg gegen die Ukraine mitsamt flankierenden regionalen Destabilisierungsbemühungen und Einflussoperationen zunehmend professionalisiert hat und möglicherweise bereits als „good practice" für befreundete Regime wie China und Iran fungiert. S. Ofer Friedman, Russian 'Hybrid Warfare': Resurgence and Politicisation, Oxford University Press, 2018.

29 S. 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 S. Alessandro Arduino, Chinese private security firms are growing their presence in Africa: why it matters, The Conversation, August 8, 2022.

31 S. Andreas Wittkowsky, Geopolitische Spoiler. „Private" Militär- und Sicherheitsunternehmen und Friedenseinsätze, ZIF Briefing 09|2024; Dirk Druet, Knives Out: Evolving 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, S. 23.

32 S. Dirk Druet, Knives Out: Evolving Trends in State Interference with UN Peacekeeping Operations, S. 472.

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

34 Ebd..

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

36 S. UN DPO Information Integrity Unit, Digital Information Harms Targeting MINUSMA During the Drawdown, Retrospective Analytical Report, 1 June - 31 December 2023, 2024, S. 24 ff..

Das Bedrohungspotential proliferierender NSAs im Cyberbereich wird voraussichtlich auch für Friedenseinsätze zunehmen.

Eine öffentliche Zuordnung von NSA-initialisierten Cyberangriffen gegen Friedenseinsätze gibt es bisher nicht – was in diesem sicherheitssensiblen Bereich keiner Bestätigung einer niedrigen Gefährdung entspricht. Angesichts einer generell zunehmend komplexen Anzahl von NSAs, die den Cyberraum attackieren, kann davon ausgegangen werden, dass das Bedrohungspotential proliferierender NSAs im Cyberbereich auch für internationale Friedenseinsätze zunehmen wird.

Schlagkräftige NSAs im Cyberraum

Nationalistische, pro-russische *Hacktivists* wie das KillNet-Netzwerk attackieren seit 2022 ukrainische und europäische Webseiten und Internetdienstleistungen insbesondere staatlicher Strukturen.[37] Cyberkriminelle-Organisationen wie die russische Evil Corp – unter anderem bekannt durch umfang- und erfolgreiche *Ransomware*-Angriffe auf den Privatsektor – haben laut unterschiedlichen Ermittlungen großflächige Cyberangriffe auf westliche Internetdienstleister im Auftrag des russischen Geheimdienstes durchgeführt.[38] Untersuchungen zufolge nutzt auch China eine zunehmende Anzahl von NSAs – insbesondere im Cyberraum – um eine Attribution schädlicher Aktivitäten zu erschweren.[39]

37 S. Antoaneta Roussi, Meet Killnet, Russia's hacking patriots plaguing Europe, Politico, September 9, 2022; Daryna Antoniuk, Russian hacker group Killnet returns with new identity, The Record, May 22, 2025.

38 S. National Crime Agency, Evil Corp: Behind the Screens, October 2024.

39 S. 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, April 13, 2025.

4. Internationale Organisationen und ihre Friedenseinsätze als Akteur: Ansätze zur Bearbeitung hybrider Konfliktaktivitäten

4.1 Integration von Aspekten in bestehende Mandate

Da sich hybride Formen des Konfliktaustrags zum „neuen Normal“[40] entwickelt haben, sind internationale Organisationen und ihre Friedenseinsätze als wichtigstes Instrument internationaler Konfliktbearbeitung gefordert, darauf zu reagieren. Der UN-Sicherheitsrat befasst sich seit 2016 zunehmend mit digitalen Technologien und ihren Auswirkungen auf den internationalen Frieden und die internationale Sicherheit. In verschiedenen Formaten wurden unter anderem Fragen der Cybersicherheit und hybriden Kriegführung, die Rolle sozialer Medien bei der Aufstachelung zu Diskriminierung, Feindseligkeit und Gewalt und die Implikationen künstlicher Intelligenz für Friedenseinsätze und *Special Political Missions* (SPMs) diskutiert.[41]

Der Sicherheitsrat der Vereinten Nationen sollte sich stärker für die Bearbeitung von Bedrohungen aus dem Cyberraum einsetzen.

Die unterschiedlichen Perspektiven der Mitglieder des Sicherheitsrats bzgl. seiner Rolle und seines Engagements in diesen Themenfeldern wurde erneut bei der jüngsten *High Level Open Debate* zu sich entwickelnden Bedrohungen im Cyberraum deutlich (Juni 2024).[42] Während einige eine klare Rolle des Rates in der Bearbeitung von Bedrohungen aus dem Cyberraum sahen, hielt Russland ihn nicht für das geeignete Diskussionsforum für Cybersicherheit und verwies auf die Expertise und Repräsentanz einer 2019 von der UN-Generalversammlung (GV) mandatierten und allen UN-Mitgliedstaaten offenen Arbeitsgruppe (*Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs)*). Wie die bereits 2004 ebenfalls von der GV etablierte *Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace*, ist die OEWG ein wichtiger Prozess für die Entwicklung von Regeln, Normen und Prinzipien verantwortungsvollen, staatlichen Verhaltens im Cyberraum.

Bereits in den 2010er Jahren begann eine Debatte über „Cyber Peacekeeping“, das abhängig vom jeweiligen Kontext ähnliche Aufgaben wie das physische Peacekeeping im Cyberraum übernehmen könnte.

Cho Tae-yul, Außenminister der Republik Korea und Präsident des Sicherheitsrats, forderte den Rat im Zuge der o.g. *Open Debate* auf, nicht den Kopf in den Sand zu stecken und sich stärker für die Bearbeitung von Bedrohungen aus dem Cyberspace einzusetzen. Das Gremium sollte, so auch das *Stimson Center* im Nachgang der jährlichen *Protection of Civilians (POC)*-Debatte des UN-Sicherheitsrats im Mai 2025, “*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, Tagesspiegel Background, 18.06.2025.

41 S. Allison Pytlak and Shreya Lad, Strengthening Global Cyber Resilience Through UN Security Council Initiatives, Issue Brief, The Henry L. Stimson Center, August 8, 2024.

42 S. 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, June 13, 2025.

Cyber Peacekeeping

Um Staaten nach eskalierten hybriden Aktivitäten zu stabilisieren, Strukturen in betroffenen Einsatzgebieten wiederherzustellen (z. B. kontaminierte Cyber-Infrastruktur, polarisierter Informationsraum, geschädigte kritische Infrastruktur) und zur Schaffung eines dauerhaften Friedens beizutragen, müssen betroffene Sektoren hybrider Aktivitäten stärker als bisher in die Aktivitäten von Friedenseinsätzen einbezogen werden. Bereits in den 2010er Jahren begann eine Debatte über „*Cyber Peacekeeping*", das abhängig vom jeweiligen Kontext ähnliche Aufgaben wie das physische Peacekeeping im Cyberraum übernehmen könnte.[44] Dazu gehören das *Monitoring* von Aktivitäten, die einem Waffenstillstand oder Friedensabkommen zuwiderlaufen, die Untersuchung von größeren Angriffen, die Demobilisierung von Cyber-Kombattanten, der Schutz der Zivilbevölkerung vor Cyberangriffen wie Desinformationskampagnen, die Förderung von Menschenrechten im Cyberraum oder die Unterstützung von Staaten beim Wiederaufbau von kritischer Infrastruktur.

Im Zuge der aktuellen Diskussion über die Zukunft des UN Peacekeeping wurden existierende Vorschläge für Einsatzmodelle aufgegriffen.[45] Dazu gehören die Integration einer *Cyber Unit* in einen physischen UN-Friedenseinsatz oder die Durchführung reiner online-Einsätze im Cyberraum mit „digitalen Blauhelmen". Als möglicher Startpunkt wurde in der Vergangenheit das *Digital Blue Helmets (DBH) Programme* der UN gesehen, das 2016 zum Schutz der eigenen Infrastruktur etabliert wurde.[46]

Eine Ausweitung von Einsatzmandaten in den Cyber- und Informationsraum ist auch angesichts der von einigen Mitgliedern des UN-Sicherheitsrats gewünschten Konzentration von Friedenseinsätzen auf Kernaufgaben aktuell nur schwer denkbar.[47] Bei verschiedenen Missionen wurden allerdings sowohl bei den UN, wie auch der EU und OSZE, bereits in den vergangenen Jahren neue Aspekte in Mandate integriert – insbesondere im Hinblick auf den staatlichen und gesellschaftlichen Resilienzaufbau. Dieser reicht von digitaler Informationskompetenz über die Stärkung unabhängiger, qualitativer Medien und den Schutz kritischer Infrastrukturen hin zu resilienten Sicherheits- und Verteidigungsstrukturen. So erhielten einige UN-Friedenseinsätze (UNIFIL, UNMISS, MONUSCO) ein explizites Mandat im Zusammenhang mit schädlichen Informationen oder beraten wie die *Special Political Mission* UNAMI im Irak im Rahmen des Mandats zur Wahlunterstützung zum Umgang mit schädlichen Informationen (S/2025/323). In der DRC trainierte MONUSCO jüngst 26 Führungspersonen zivilgesellschaftlicher Organisationen in der Provinz Nord-Kivu zwei Tage lang im Kampf gegen Desinformation und Hassrede.[48]

Die EU engagiert sich im Rahmen ihrer GSVP-Missionen dafür, staatliche Strukturen gegen hybride Aktivitäten zu stärken. 2023 formulierte der *Civilian CSDP (Common Security and Defence Policy) Compact* das Ziel, "*[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]. Die seit 2014 laufende zivile EUAM Ukraine (*European Union Advisory Mission Ukraine*) hat im Rahmen ihres Mandats zur zivilen Sicherheitssektorreform – angepasst an aktuelle Herausforderungen – wichtige Aspekte der Resilienzstärkung gegenüber hybriden Aktivitäten in ihr Engagement integriert. So unterstützt sie das *National Security and Defence Council* (NSDC) der Ukraine in Fragen der Cybersicherheit, der strategischen Kommunikation im Desinformationskontext sowie des Schutzes kritischer Infrastruktur.[50]

44 S. u.a.: 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, May 2, 2022.

45 S. 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, S. 33 f.

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

47 Im Zuge der UNMISS-Mandatsverlängerung am 08. Mai 2025 formulierten die USA deutlich ihre Position zur künftigen Ausgestaltung von Peacekeeping-Mandaten: „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 S. MONUSCO, Nord-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, S. 22, No. 9.

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

Die OSZE trägt mit ihren Aktivitäten im Bereich Medien (Förderung des Medienpluralismus und der Informationskompetenz der (Zivil-) Gesellschaft) schon lange zur Stärkung der Resilienz von Gesellschaften gegen schädliche Informationen bei. Elf ihrer aktuell 12 Feldeinsätze haben ein entsprechendes Mandat. Im Bereich Cybersicherheit hat das *Transnational Threats Department* (TNTD) im OSZE-Sekretariat seit 2012 Pionierarbeit geleistet: TNTD organisiert eine Reihe von Aktivitäten zum Aufbau nationaler Kapazitäten für den Umgang mit Cybersicherheits-Bedrohungen sowie zur Förderung regionaler Zusammenarbeit und Resilienz.[51] Als einziger OSZE-Einsatz hat die 1995 etablierte *OSCE Mission to Bosnia and Herzegovina* ein explizites Mandat im Bereich *Cyber/ICT Security*. Sie unterstützt unter anderem die Entwicklung eines strategischen *Cybersecurity*-Rahmens sowie Aufbau und Stärkung nationaler *Computer Emergency Response Teams*.[52]

Bei verschiedenen Missionen wurden sowohl bei den UN, wie auch der EU und OSZE, in den vergangenen Jahren neue Aspekte in Mandate integriert.

4.2 Explizite, fokussierte Missionen: EUPM Moldau als Blaupause

Ähnlich der Situation in der Ukraine vor 2022, sieht sich der EU-Aspirant Moldau intensiven hybriden Aktivitäten Russlands ausgesetzt, die darauf abzielen, das Land politisch und ökonomisch zu destabilisieren und von einer Annäherung an die EU oder andere westliche Staaten abzuhalten.[53] Mittels einer synchronisierten Kombination von hybriden Werkzeugen, die in den vergangenen 30 Jahren in der Republik Moldau graduell positioniert wurden, versucht Russland seit spätestens 2020 massiv, eine europäische Integration des Landes zu sabotieren. Genutzt werden hierbei u. a. die Energieversorgung (Einstellung der russisch dominierten Gas- und Elektrizitätsversorgung sowie Stromnetzdestabilisierung), militärische Drohungen durch im abtrünnigen Transnistrien stationierte russische Militärkontingente, Bezahlung und Ausrüstung von Antiregierungsprotesten, Nutzung von Strukturen der organisierten Kriminalität zur illegalen prorussischen Parteiengründung und -finanzierung, Desinformationskampagnen mit *Deep Fakes* gegen proeuropäische Politiker:innen, Cyberattacken gegen Sicherheitsbehörden, *Hack-to-Leak*-Operationen oder versuchte Wahlmanipulation.

Die EU bemüht sich, ihr Engagement durch die zusätzliche Nutzung sog. *Specialized Teams* und hochspezialisierter *Visiting Experts* zu skalieren.

Nicht zuletzt auf den Lehren aus dem russischen Angriff auf die Ukraine 2022 und der im Vorfeld massiv intensivierten hybriden Aktivitäten aufbauend, hat die EU 2023 eine kleine zivile Partnerschaftsmission in Moldau initiiert, deren Fokus ausschließlich auf hybriden Bedrohungen liegt.[54] Quasi als experimentelle Speerspitze im Umgang mit hybriden Attacken, unterstützt die *EU Partnership Mission in Moldova* (EUPM Moldova) bereits im zweiten Mandat den Resilienzaufbau moldauischer Sicherheitsbehörden gegen destabilisierende hybride Aktivitäten, mit besonderem Fokus auf FIMI, Cybersicherheit und Krisenmanagement. Dabei engagiert sie sich unter anderem im Ausbau der Kapazitäten der kürzlich gegründeten Nationalen *Cyber Security*-Behörde, des Innenministeriums wie auch des Strategischen Kommunikationsteams der Regierung.[55]

Wenn auch vergleichsweise klein mit einer mandatierten Missionsgröße von maximal 49 internationalen Expert:innen, bemüht sich die EU, ihr Engagement durch die zusätzliche Nutzung temporär aus Mitgliedstaaten entsandter Expert:innen – in Form von sogenannten "*Specialized Teams*" und hochspezialisierter "*Visiting Experts*" – zu skalieren. Mit den 2024 gegründeten und Brüssel-basierten "*Hybrid Rapid Response Teams*" kann die EUPM Moldau auf weitere personelle Verstärkung zurückgreifen (siehe unten).[56]

51 S. OSCE Transnational Threats Department, Cyber/ICT Security.

52 S. OSCE Mission to Bosnia and Herzegovina, Cyber/ITC Security.

53 S. 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 S. Monika Benkler, Ringen um Stabilität: Die neue EU-Mission in der Republik Moldau, ZIF kompakt, Mai 2023.

55 S. EU Partnership Mission in the Republic of Moldova (EUPM).

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

Lessons Learned

Angesichts weiterer Destabilisierungsversuche[57] im Ostseeraum, im Kontext von Wahlen innerhalb der Europäischen Union und der geringen Anzahl der entsandten Fachexpert:innen in den Themenbereichen *Cyber Security*, Strategische Kommunikation und nationale Sicherheit sind die *lessons learned* aus der EUPM Moldau besonders hilfreich – sowohl für Friedenseinsätze als auch für zukünftige ad-hoc-Interventionen im hybriden Kontext.

Die *lessons learned* aus der EUPM Moldau sind sowohl für Friedenseinsätze als auch für zukünftige ad-hoc-Interventionen im hybriden Kontext hilfreich.

1. Das Spektrum hybrider Bedrohungen beschränkt sich nicht auf den Informations- und Cyberraum, auch wenn dieser derzeitig einen Schwerpunkt destabilisierender Operationen bildet. Sowohl in der Ukraine als auch in Moldau haben hybride Angriffsstrategien insbesondere auf systemische Schwachstellen gezielt und tun dies weiterhin: (a) in der kritischen Infrastruktur (z. B. zur Unterbrechung von Telekommunikationsnetzwerken und der Stromversorgung), (b) in der Finanzstromüberwachung (z. B. um verfassungsfeindliche Parteien zu finanzieren, Saboteure anzuwerben oder bezahlte Demonstrant:innen auszurüsten) und (c) im Bereich Rechtsstaatlichkeit (z. B. indem rechtliche Lücken gezielt ausgenutzt oder besonders unterversorgte Behördenteile zu korrumpieren versucht werden).

2. Die erfolgreiche Abwehr derartiger Aktivitäten erfordert – wie in der Ukraine gesehen und durch die EU in Moldau mittels spezialisierter Einsatzteams experimentell umgesetzt – zwei Elemente: (a) in einer aktiven Gefährdung durch hybride Aktivitäten zügig entsendbare Fachexpertise in zentralen Bereichen der nationalen Sicherheit zur Intervention, operativen Unterstützung und darauf aufbauenden Prävention weiterer Destabilisierung; (b) im Nachgang hybrider Angriffe strategische Beratungsexpertise in ebendiesen Themenfeldern, um die ausgenutzten systemischen Schwachstellen nachhaltig zu beheben (beispielhaft Ukraine nach einem Waffenstillstand/EUAM Ukraine).

Dynamische Entwicklung von Unterstützungsstrukturen und Expertiseclustern

Mit der Zunahme hybrider Konfliktaktivitäten haben internationale Organisationen – verstärkt in den vergangenen zehn Jahren – verschiedene Expertisecluster, Trainingsprogramme und Unterstützungsstrukturen im hybriden Themenkomplex etabliert. Das o. g. von EU- und NATO-Mitgliedstaaten gegründete Hybrid CoE fungiert seit 2017 als spezialisierte Forschungs-, Beratungs- und Trainingseinrichtung für Partnerländer, unterstützt GSVP-Missionen der EU und leistet weitreichende Grundlagenarbeit im Themenfeld der hybriden Bedrohungen.

Die EU hat des Weiteren auf verschiedensten Ebenen Kompetenzzentren, Forschungsstrukturen und Unterstützungsmechanismen zu hybriden Fragestellungen etabliert. Auf Kommissionsebene forschen und beraten Expert:innen am EU *Joint Research Centre* zu hybriden Bedrohungen und FIMI, während sowohl die sog. *Foreign Policy Instruments* (FPI) als auch unterschiedliche Generaldirektionen der Kommission – DG HOME (*Home Affairs*) und DG DEFIS (*Defence Industry and Space*), aber auch DG NEAR (*European Neighbourhood and Enlargement Negotiations*) und DG CONNECT (*Communications Networks, Content and Technology*) – unterschiedliche Aktivitäten und Projektfinanzierungen in den hybriden Themenfeldern FIMI, Cyber und KRITIS unterstützen. Zusätzlich wurden im EAD zentrale Strukturen in Form mehrerer *StratCom (Strategic Communication) Task Forces geschaffen*[58], um gezielt FIMI-

57 S. Council of the EU, Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners, 18 July, 2025.

58 S. EEAS Strategic Communication Task Forces.

Dynamiken zu analysieren und auch GSVP-Missionen im Bereich Desinformation zu unterstützen und zu trainieren, während die *Hybrid Fusion Cell* im EAD breitere Analysen vorbereitet und Trainings durchführt.

Auch die NATO unterstützt ihre Mitgliedstaaten und ausgewählte Partner durch Wissensaustausch, Trainings und gemeinsame Übungen im Umgang mit hybriden Bedrohungen und hat hierzu Strategien entwickelt und angepasst.[59] In den Themenfeldern Desinformation, Cyber und Energiesicherheit hat das Bündnis drei *Centres of Excellence* geschaffen, die Training und Wissensaustausch unter Allianzpartnern forcieren und ausbauen: das *Strategic Communications Centre of Excellence* in Riga/Lettland, das *Cooperative Cyber Defence Centre of Excellence* in Tallinn/Estland und das *Energy Security Centre of Excellence* in Vilnius/Litauen.

Bei der OSZE sind die Themenfelder hybride Bedrohungen und Cyber insbesondere im Sekretariat im TNDT angesiedelt, hybride Bedrohungsdynamiken werden im OSZE *Conflict Prevention Centre* (CPC) beobachtet und analysiert. Bei den UN unterstützte seit 2022 ein für zwei Jahre eingerichteter *Workstream* Friedenseinsätze unter anderem mit Training, Tools und Expertise im Bereich Misinformation, Desinformation, Malinformation und Hassrede; 2023 wurde dieser als *Information Integrity Unit* strukturell im *Department of Peace Operations* (DPO) verankert.

4.3 Multinationale *Rapid Response*-Kapazitäten

Die Fähigkeit, hybride Aktivitäten frühzeitig zu erkennen, zügig abzuwehren und gegebenenfalls entstandene Schäden rasch zu beheben, ist ein entscheidender Faktor für die nationale Sicherheit von Staaten – wie auch von Friedenseinsätzen. Die in den vergangenen Jahren von der EU entwickelten *Rapid Response Teams* können sowohl zur Unterstützung ihrer Mitgliedstaaten und Operationen im Rahmen der GSVP wie auch von Partnerländern eingesetzt werden.[60]

Aufgrund der vielfältigen Angriffsmodi hybrider Bedrohungen erscheinen schnelle und integrierte Interventionskonzepte wie das EU *Hybrid Rapid Response Team* vielversprechend und richtungsweisend.

Das 2018 im Rahmen der *Permanent Structured Cooperation* (PESCO) unter litauischer Führung etablierte EU *Cyber Rapid Response Team* (CRRT)[61] wurde mit dem Ziel geschaffen „*to respond to cyber incidents and ensure a higher level of cyber resilience*". Es kam erstmals 2022 in Moldau, 2023 im Rahmen der militärische Ausbildungsmission EUTM Mozambique (*European Union Training Mission in Mozambique*) und 2023 in einer zweiten Runde in Moldau zum Einsatz – um Schwachstellen zu bewerten und bei der Verbesserung der Cyberabwehr zu unterstützen. Ein tatsächlicher Kriseneinsatz konnte mit dem Instrument bislang nicht realisiert werden, da der EU CRRT-Prozess nicht in der Lage war „*to reach decisions and deployments in reasonable time frames*"[62].

Das 2024 als Instrument der *EU Hybrid Toolbox* etablierte EU *Hybrid Rapid Response Team* dient der Prävention und Abwehr hybrider Bedrohungen. Als eines der zentralen Ergebnisse des *Strategic Compass for Security and Defence* 2022 sollen die Teams kurzfristig maßgeschneiderte und gezielte Unterstützung für Mitgliedstaaten und Missionen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik sowie für Partnerländer bieten.[63] Vom 28. April bis 9. Mai 2025 half erstmals ein solches Team der Republik Moldau im Vorfeld der Parlamentswahlen (September 2025) in ihrem Kampf gegen externe Einmischung.[64]

59 S. FN 2.

60 Auch die NATO verfügt über Kapazitäten zur schnellen Reaktion – das NATO Cyber Rapid Reaction Team (seit 2012) und das NATO Counter Hybrid Support Team (seit 2018) –, die jedoch vorrangig für NATO-Einrichtungen und -Verbündete zur Verfügung stehen.

61 S. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT).

62 Taylor Grossman, Cyber Rapid Response Teams. Structure, Organization, and Use Cases, Center for Security Studies (CSS), ETH Zürich, November 2023, S. 33.

63 S. Rat der Europäischen Union, Hybride Bedrohungen: Rat ebnet Weg für Einsatz von Teams für die rasche Reaktion auf hybride Bedrohungen, 21.05.2024.

64 S. EEAS, Moldova: Remarks by High Representative Kaja Kallas at the joint press conference following the Association Council meeting, 04.06.2025.

Auf Grund der vielfältigen Angriffsmodi hybrider Bedrohungen, die sich nicht nur auf einzelne Sektoren wie z. B. den Cyberraum begrenzen, sondern sich umfassend entlang systemischer Schwachstellen ausrichten, erscheinen schnelle und integrierte Interventionskonzepte wie das EU *Hybrid Rapid Response Team* vielversprechend und richtungsweisend.

4.4 Kooperation mit privaten Akteuren

Für Tech-Unternehmen sind präventive und reaktive Aktivitäten im Cyber- und Informationsraum Teil ihres Business-Modells. Im Zuge des russischen Angriffskrieges auf die Ukraine setzen Akteure wie Googles *Threat Analysis Group* (TAG) und Microsofts *Threat Intelligence Center* (MSTIC) ihre technischen Fähigkeiten gezielt für die Verteidigung des überfallenen Landes ein.[65] Angesichts der Ausbreitung moderner Konflikte in den Cyberraum und der – im Vergleich zu privaten Tech-Akteuren – geringeren Fähigkeiten und Kapazitäten internationaler Organisationen, diese zu managen, plädierte der ehemalige UN-Untergeneralsekretär für Friedenseinsätze, Jean-Marie Guéhenno (et. al.), jüngst für ein neues *Multistakeholder*-Modell aus *„traditional peace enforcers (to handle the military and diplomatic tasks) and technology companies (to disrupt cyber or disinformation operations)"*.[66] Das vorgeschlagene hybride Modell, so Guéhenno, könnte die Fähigkeiten des privaten Sektors mit der Legitimität von Staaten und multilateralen Institutionen kombinieren.

Die Beteiligung von Tech-Unternehmen am internationalen Krisenmanagement bietet zweifellos Chancen, wirft jedoch gleichzeitig eine Reihe problematischer Fragen und Risiken auf.

Die Beteiligung von Tech-Unternehmen am internationalen Krisenmanagement bietet zweifellos Chancen. Gleichzeitig wirft sie jedoch eine Reihe von problematischen Fragen und Risiken auf. Dazu zählen fehlende demokratische Kontrolle und Rechenschaftspflicht, kommerzielle Interessenkonflikte und damit einhergehend Unberechenbarkeit im Engagement sowie Sicherheits- und Spionagebedenken insbesondere im Umgang mit sensiblen Daten.[67]

Abgesehen von einer institutionalisierten Kooperation mit Akteuren des Privatsektors im internationalen Krisenmanagement spielen die sich schnell entwickelnden analytischen Tools unterschiedlicher Tech-Unternehmen bereits jetzt eine zunehmende Rolle in Friedenseinsätzen und im Umgang mit hybriden Bedrohungen. Früher waren KI-unterstützte Monitoring- und Analyse-Tools teuer, kompliziert und zumeist den Geheimdiensten vorbehalten. Heute sind sie zunehmend kostengünstig und erlauben es, den Informations- und Cyberraum umfassend zu überwachen, unterschiedlichste Informationskanäle zu aggregieren und von hybriden Aktivitäten bedrohte Partner durch kosteneffiziente *„off-the-shelf"*-Lösungen schnell zu stärken.

Kooperativer Stresstest in Moldau

Im Vorfeld der Parlamentswahlen in der Republik Moldau (September 2025) fand im Juni in Chișinău eine *Digital Hybrid Threats Simulation* statt. Neben moldauischen Behörden, zivilgesellschaftlichen Organisationen, Faktenprüfern, unabhängigen Medien und internationalen Partnern nahmen Vertreter:innen von Google, Meta und TikTok freiwillig an der Simulation teil. Ziel war es, das Bewusstsein für potenzielle Desinformationskampagnen und Cyberangriffe zu schärfen, die die bevorstehenden Wahlen stören sollen, und eine effektive Reaktion aller relevanten Akteure zu ermöglichen.[68]

65 S. Shane Huntley, Fog of war: how the Ukraine conflict transformed the cyber threat landscape, Google Threat Analysis Group (TAG), February 16, 2023. Zwischen Januar 2022 und September 2023 war die Ukraine 2.776 Cyberangriffen ausgesetzt. Cyber Peace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, 2023, S. 3.

66 S. Jean-Marie Guéhenno, Olivia Grinberg, Jason Healey, A Multistakeholder Model of Cyber Peace, Lawfare, 07.02.2025.

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

68 S. 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; s. auch NIS Cooperation Group, Compendium on Election Cybersecurity and Resilience, Updated Version, 2024.

5. Zukünftige Herausforderungen an Einsätze im Kontext hybrider Bedrohungen – Empfehlungen an die deutsche Politik

Internationale Friedenseinsätze operieren vielfach in geopolitisch umkämpften Räumen und müssen sich und ihr Personal vor hybriden Aktivitäten staatlicher und nichtstaatlicher Akteure schützen. Da sie anders als Staaten keine glaubhafte Abschreckung betreiben können, müssen sie insbesondere ihre Resilienz gegen Angriffe weiter erhöhen und proaktiv hier einen Ansatz verfolgen, der sich nicht um singuläre Phänomene kümmert, sondern möglichst ganzheitlich eigene Informationsinfrastruktur abschirmt, interne Kommunikationswege und -strategien kontrolliert, den umgebenden Informationsraum überwacht und enge Kontakte zu nationalen und internationalen Sicherheitsakteuren hält. Der Personalrotation in Friedenseinsätzen – einer signifikanten Schwachstelle in der Abschirmung und Kontrolle interner Prozesse, Informationen und Strukturen – kann durch System- und Infrastrukturharmonisierung sowie verschärfte Prozesskontrolle begegnet werden.

Hybride Dynamiken erfordern eine hohe Anpassungsgeschwindigkeit von Missionsmandaten sowie technische Expertise beim Missionspersonal.

Als Akteur in der Bearbeitung hybrider Konfliktaktivitäten haben Friedenseinsätze in den vergangenen Jahren neue Ansätze umgesetzt. Diese müssen nun angesichts der verstärkten Nutzung des hybriden Instrumentenkastens seitens staatlicher und nichtstaatlicher Akteure weiterentwickelt werden. Hybride Dynamiken erfordern eine hohe Anpassungsgeschwindigkeit von Missionsmandaten sowie eine bisher nur begrenzt verfügbare technische Expertise beim Missionspersonal, von Fachexpert:innen in der strategischen Kommunikation über nachrichtendienstliche Analyse hin zu spezialisierter *Cyber Defence*. Vor diesem Hintergrund ist das Modell der experimentellen EUPM Moldau wegweisend. Sie vereint den mittelfristigen Resilienzaufbau als zentrales Handlungsfeld zur Stärkung von Staaten mit dem kurzfristigen Einsatz eines Expert:innenteams für besondere Anforderungen – ergänzt um das neue EU *Hybrid Rapid Response Team*.

Man wird bei der Sicherung des Friedens an den Fähigkeiten der großen Tech-Unternehmen künftig wohl nicht mehr vorbeikommen.

Eine Ausweitung der Mandate von UN-Friedenseinsätzen in den Cyber- und Informationsraum ist angesichts eines polarisierten Sicherheitsrats, in dem einige Mitglieder eine Konzentration von Friedenseinsätzen auf Kernaufgaben wünschen, aktuell nur schwer denkbar. Im Rahmen der UN wird daher vorerst der Resilienzaufbau in Einsatzländern im Vordergrund stehen. Dennoch kommen Vorschläge wie die Etablierung eines hybriden Modells bzw. Überlegungen zur verstärkten Zusammenarbeit mit dem privaten Tech-Sektor zum richtigen Zeitpunkt. Man wird bei der Sicherung des Friedens an den Fähigkeiten der großen Tech-Unternehmen künftig wohl nicht mehr vorbeikommen und neue Partnerschaften etablieren sowie existierende ausbauen müssen.

Empfehlungen

Angesichts der globalen Zunahme hybrider Konfliktaktivitäten wird der Bedarf an resilienzstärkenden Einsätzen und kurzfristigen Interventionen steigen. Für die deutsche Politik ergeben sich daraus Empfehlungen entlang drei zentraler Handlungsdimensionen:

→ Multilaterale Ansätze und Fähigkeiten im Bereich Hybrider Bedrohungen fördern und stärken

Angesichts multidimensionaler Herausforderungen ist eine anhaltende Einbettung des deutschen zivilen Krisenmanagements in bestehende multilaterale Bemühungen unerlässlich. Auch wenn sich die nationalen sicherheitspolitischen Prioritäten in Richtung der Landes- und Bündnisverteidigung verschieben, sollte Deutschland aufgrund der globalen Zunahme hybrider Bedrohungen, deren destabilisierende Wirkung etwa in EU-Partnerländern oder Europas Nachbarschaft auch die eigene Sicherheit beeinträchtigen kann, und nicht zuletzt aufgrund seiner personellen Expertise im hybriden Themenkomplex eine tragende, wenn nicht führende Rolle bei der weiteren Konzeptentwicklung und Umsetzung von Friedenseinsätzen und kurzfristigen Interventionen zur Abwehr hybrider Bedrohungen übernehmen.

Deutschland sollte eine tragende Rolle bei der weiteren Konzeptentwicklung und Umsetzung von Friedenseinsätzen und kurzfristigen Interventionen zur Abwehr hybrider Bedrohungen übernehmen.

Eine starke und nachhaltige Beteiligung an experimentellen, resilienzstärkenden, multilateralen Initiativen wie die EUPM Moldova oder zumindest partiell EUAM Ukraine ist gleich aus zweierlei Sicht anzuraten: Zum einen stärkt dies wichtige multilaterale Ansätze, mit neuen hybriden Herausforderungen gezielt umzugehen, gerade wenn nationale Alleingänge durch Ressourcenbegrenzung wenig zielführend wären. Zum anderen kann das gewonnene Einsatzwissen deutscher Expert:innen aus Kontexten mit aktiven hybriden Bedrohungen oder gar hybrider Kriegführung (a) unmittelbar in den weiteren deutschen Fähigkeits- und Expertiseaufbau im hybriden Themenkomplex einfließen und (b) zudem für den nationalen Kontext relevante Einsichten und Erfahrungen liefern.

Zur Abwehr akuter hybrider Aktivitäten bieten sich insbesondere schnell einsetzbare und zeitlich begrenzte Interventionen mit schlanken, aber spezialisierten Einsatzteams an. Eine anhaltend aktive, deutsche Beteiligung an der Weiterentwicklung entsprechender Instrumente wie dem *EU Hybrid Rapid Response Team* – sowohl politisch, konzeptionell als auch personell – sowie das strukturierte Vorhalten eigener deutscher Expertise ist dringend anzuraten.

→ Strukturen und Maßnahmen im Themenkomplex synergetisch gestalten und effizient bündeln

Gleichzeitig haben sich spätestens seit der Annexion der Krim 2014 multilaterale und nationale Abwehransätze im sich dynamisch entwickelnden Konfliktfeld hybrider Bedrohungen multipliziert. Ein vertieftes Bedrohungsverständnis in Deutschland und insbesondere innerhalb seiner Bündnisse und Allianzen hat über einen kurzen Zeitraum neue, themenspezifische Strukturen und Instrumente entstehen lassen, die sich zumindest partiell besser aufeinander abstimmen lassen. So haben Themen wie Desinformation eine silohafte Eigendynamik entwickelt und werden (z. B. in Moldau) von Friedenseinsätzen, bilateralen Projektfinanzierungen, internationalen Organisationen und Nichtregierungsorganisationen überlappend bedient, was teils zur Überfrachtung der nationalen Partner führt.

Deutschland sollte in diesem Zusammenhang ganzheitliche Ansätze zum hybriden Themenkomplex unterstützen, konzeptionell weitere Strukturaufwüchse beobachten und seine Ressourcen – sowohl personell als auch finanziell – redundanzminimierend fokussieren.

→ Spezialisierte Fachexpertise im ZIF-Pool effizient nutzen

Die Abwehr hybrider Bedrohungen im Kontext von Friedenseinsätzen erfordert einen breit aufgestellten, vernetzten Ansatz, nicht zuletzt da Aggressoren verdeckt und schwachstellenorientiert über unterschiedlichste Einfallstore einwirken. Deutschland verfügt im Themenkomplex hybrider Bedrohungen über umfangreiches Fachwissen in den relevanten Ressorts und hat ausgewiesene Expert:innen in verschiedenen Friedenseinsätzen und Institutionen (EU, UN, OSZE, NATO) im Einsatz. Die Sekundierung von Personal in Führungspositionen von sowohl Auswärtigem Amt/ZIF als auch Bundesministerium des Inneren (BMI) ermöglichte z. B. den zügigen und erfolgreichen Start von EUPM Moldau mit. EUPM Moldau hat im Verlauf aber auch gezeigt, dass es eine hohe Nachfrage nach schnell aktivierbaren Expert:innenprofilen im hybriden Themenfeld gibt.

Angesichts der dynamischen Fortentwicklung des hybriden Instrumentenkastens ist Agilität ein wichtiger Faktor, wenn es um die Erhöhung der deutschen Einsatzfähigkeit im zivilen Bereich geht.

Aufgrund steigenden Bedarfs an dezidierter Fachexpertise in den unterschiedlichen Themenfeldern der nationalen Sicherheit – von Analytiker:innen über *Cyber Security*-Expert:innen zu Kommunikationsspezialist:innen und Analyst:innen für Finanzströme – ist es empfehlenswert, die deutsche Einsatzfähigkeit im zivilen Bereich weiter zu erhöhen und die bereits vorhandene Expertise des ZIF *Expert* Pool gezielt zu nutzen. Damit stärkt Deutschland nicht nur die Handlungsfähigkeit gegenüber hybriden Bedrohungen auf internationaler Ebene, sondern verteidigt dadurch auch seine eigenen Werte, Interessen und seine Sicherheit.

Abkürzungsverzeichnis

CERT	Computer Emergency Response Team
CSDP	Common Security and Defence Policy
DRC	Democratic Republic of the Congo
EAD	Europäischer Auswärtiger Dienst
EEAS	European External Action Service
EU	Europäische 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
GGE	Group of Governmental Experts
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
GV	Generalversammlung
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
ICTs	Information and Communications Technologies
IT	Informationstechnologie
JNIM	Jama'a Nusrat ul-Islam wa al-Muslimin
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastruktur
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 Organization
NSA	Non-State Actor
SPM	Special Political Mission
StratCom	Strategic Communication
TNTD	Transnational Threats Department
OEWG	Open-ended Working Group

OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
POC	Protection of Civilians
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 Sudan
ZAR	Zentralafrikanische Republik

www.zif-berlin.org