STUDY | OCTOBER 2022

Protecting the truth: Peace operations and disinformation

Monika Benkler, Dr. Annika S. Hansen, Lilian Reichert

zif
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 (ad interim): Dr. Astrid Irrgang
Chairperson of the Supervisory Board: Dr. Anna Lührmann

www.zif-berlin.org

Authors: Monika Benkler, Dr. Annika S. Hansen, Lilian Reichert

The study is funded by the Federal Foreign Office.

Grafik & Layout: finedesign, Berlin

1. Introduction

Today, digital communication makes it possible to disseminate information at high speed across borders to more people than ever before, thus generating an enormous reach. This is true for crisis communication by international organisations and peace operations as well as for deliberate and targeted disinformation campaigns by internal conflict parties or external actors. The so-called weaponization of digital communications and social media poses new challenges for identifying and combating hostile influence. How disinformation can intensify conflict is apparent in a variety of countries – including South Sudan 2016, Myanmar 2017 and currently Russia's war in Ukraine (since February 2022).

Inevitably, disinformation is therefore a growing problem for peace operations as well. The recently published Strategy for the Digital Transformation of UN Peacekeeping (2021) describes hate speech, disinformation and misinformation as a threat to the safety of personnel and mandate implementation. New technologies such as artificial intelligence applications have the potential to further facilitate, accelerate and amplify the creation, spread and impact of disinformation in the future. As yet, peace operations still lack an overarching strategic approach to respond to attacks on missions and their personnel, as well as to disinformation that exacerbates conflict in the area of operation.

Disinformation is a threat to the safety of personnel and mandate implementation.

This study discusses how and to what extent peace operations are affected by digital disinformation and how international organisations (UN, EU, OSCE and NATO) as mandating bodies for peace operations have responded to limit the effect of disinformation or even prevent it. Based on this assessment of the current situation, the study identifies areas in need of action and suggests options for peace operations. These focus on four areas and include both short- and long-term measures.

Table of contents

1. Introduction . . . 3

2. Disinformation and other types of information disorder . . . 4

3. Disinformation in the context of international peace operations . . . 6
3.1 Social media in crisis and conflict . . . 6
3.2 How disinformation affects peace operations . . . 7

4. Central actors and their approaches . . . 9
4.1 Mapping actors . . . 9
4.2 States . . . 10
4.3 Big Tech and social media companies . . . 10
4.4 Civil society . . . 10
4.5 International organisations and peace operations . . . 11

5. Closing the gap: Options for peace operations . . . 15

6. Conclusion . . . 17

7. Abbreviations . . . 18

2. Disinformation and other types of information disorder

Definitions

International organisations do not share a common definition of disinformation and other phenomena that contribute to information disorder.[1] However, Wardle and Derakhshan's (2017) analysis for the Council of Europe is often cited to clarify terms. Their conceptual framework distinguishes three types of "information disorder":

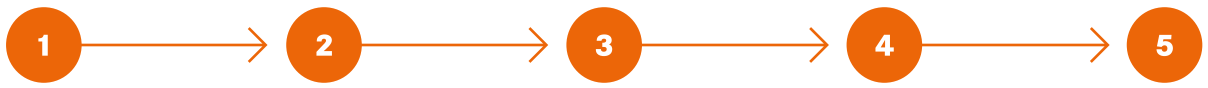
- Disinformation: Information that is false and deliberately created to harm a person, social group, organisation or country.
- Misinformation: Information that is false, but not created with the intention of causing harm.
- Malinformation: Information that is based on reality, used to inflict harm on a person, organisation or country (e. g. leaks).

Hate speech[2] is often closely linked to disinformation or amplified by it (disinformation-amplified hate speech[3]).

Actors

Disinformation is typically generated by both state and non-state actors, including individuals and groups. It is created, spread and amplified by individuals, but also artificially through campaigns that make use of technologies such as bots and recommendation algorithms.[4] There is now an industrial-scale fabrication of fake content: In 48 countries, private companies worked with political actors on disinformation campaigns in 2020. The processual development of disinformation is also described as a value chain in which actors gain influence, power, status or money through disinformation. For peace operations, it is important to understand how these incentive structures and processes are shaped in their respective conflict environments, especially who profits from the creation and dissemination of disinformation, in order to be able to counter it in a targeted manner.

Value chain in accordance with betterplace lab / Das NETTZ



Initiate
Providing the impetus or mandate for the production and dissemination of disinformation.

Produce
Creating and developing disinformation – in all conceivable forms.

Place
Publishing disinformation in a targeted manner – so as to maximise impact or create value.

Disseminate
Liking, sharing, recommending or commenting on disinformation – consciously or unconsciously, personally or automatically.

Influence
Absorbing and processing disinformation – including its influence on opinions, attitudes and behaviour.

[1] See UN General Assembly, Human Rights Council, Disinformation and freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, 13 April 2021 [Link].

[2] UN SG António Guterres defines hate speech in his first Strategy and Plan of Action on Hate Speech (2019) as: "Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is often rooted in, and generates, intolerance and hatred, and in certain contexts can be demeaning and divisive." [Link].

[3] To date, only a few empirical studies have addressed the relationship. See European Parliament, The impact of disinformation campaigns about migrants and minority groups in the EU, June 2021, p. 18 [Link].

[4] See Broadband Commission Research Report on 'Freedom of Expression and Addressing Disinformation on the Internet', September 2020, p. 19 [Link].

Scale

The global scale of disinformation has increased rapidly in recent years. While there were 70 countries in 2019, the multidisciplinary Oxford Internet Institute (OII) concludes in its latest report that 81 countries have conducted organised disinformation campaigns in 2020 - both to exercise influence on domestic politics (e. g. elections) and on geopolitics.[5] The most prolific perpetrators are Russia, Iran, Saudi Arabia, China and Venezuela, according to the Australian Strategic Policy Institute's Cyber Policy Center. This result is based on the breakdown of data sets on state-directed operations published by Twitter since 2018.[6] In addition to states, non-state actors often act as perpetrators of disinformation, especially in crisis areas such as the Western Balkans.[7]

Effects

The effects of disinformation are felt at both the individual and societal level - for instance changing beliefs, influencing voting behaviour or triggering political violence. Empirical research on how influence peddling can affect people and societies is limited and scattered, although there has been a marked increase since 2016 and as a result of the COVID-19 infodemic.[8] Research on the impact of disinformation on conflict also has clear gaps: "Across disciplines, few studies have asked direct questions on the connections between hate speech and/or information disorder and conflict."[9]

[5] The OII has been studying the manipulation of public opinion by governments and political parties via social media since 2016. Case studies also cover countries where peace operations are operating, including Bosnia and Herzegovina, Colombia, Iraq, Lebanon, Libya, Serbia, and Sudan. [Link]. For the methodological approach see Samantha Bradshaw, Hannah Bailey and Philip N. Howard, Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation. Working Paper 2021.1, Oxford, UK: Project on Computational Propaganda, p.6 [Link].

[6] See the website Understanding Global Disinformation and Information Operations launched in April 2022 [Link] and the Companion Paper [Link].

[7] See Carnegie Endowment for International Peace, Global Perspectives on Influence Operations Investigations: Shared Challenges, Unequal Resources, February 2022 [Link]; also European Parliament, Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them, February 2021 [Link].

[8] See Carnegie Endowment for International Peace, Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research, June 2021 [Link].

[9] See Sahana Udupa, Iginio Gagliardone, Alexandra Deem, Laura Csuka, Hate Speech, Information Disorder, and Conflict, Research Review, SSRC, February 2020, p.9 [Link].

3. Disinformation in the context of international peace operations

> *Like air, land and sea, the internet has become a critical domain to occupy during war.*
>
> Jared Cohen, CEO of Jigsaw[10]

3.1 Social media in crisis and conflict

The digitalisation of the public sphere has significant implications for democratic participation. Social media offer civilians new opportunities for action and influence by mobilising marginalised groups and giving them a voice. For example, the innovative mobilisation of protests during the Arab Spring in 2011 was often referred to as the "Twitter revolution". However, the early hopes that accompanied the use of social media for social mobilisation have not been fulfilled. Instead, the dark side of fast and uncontrolled communication dominates.

The information disorder described above acts as an accelerant for crises and conflicts: disinformation exploits existing divisions in societies, which harbour particularly great potential for violence in fragile, volatile contexts. For peace operations, it is therefore essential to grasp the dynamics of the information space in their areas of operation.

The spread of disinformation in conflict environments today is closely linked to the use of social media. Although the digital infrastructure and the degree of internet penetration vary greatly in different conflict areas, they are growing constantly. Sub-Saharan Africa, for example, where over 80 per cent of international peace operations are deployed, has been one of the fastest growing mobile phone regions over the past decade, with smartphone usage expanding at twice the global average growth rates.[11] Indeed, mobile and smart phones, which facilitate the creation of (dis)information content and accelerate its dissemination, are widely used in many conflict areas. Although traditional media such as radio, television or print media continue to play a role in conflict areas, social media in particular are a central source of information for large parts of the population. In African countries, including Nigeria, South Africa and Kenya, closed networks such as WhatsApp (55 %) and Telegram (18 %) together are more important for finding, sharing and discussing news than open platforms like Facebook (59 %).[12]

For peace operations, it is therefore essential to grasp the dynamics of the information space in their areas of operation.

Information has always been a valuable commodity. This is not least true in conflict zones, where competing narratives struggle to be heard and the media landscape has become a growing factor in conflict dynamics. Social networks are proving to be a particularly effective tool for manipulating emotions, reinforcing existing political and ethnic divisions, influencing elections or undermining peace processes. This includes the dissemination of extremist ideologies and narratives, which are reinforced by echo chambers[13] and dissemination networks. At worst, disinformation, misinformation and hate speech prepare the ground for physical attacks. Disinformation is particularly virulent and effective in divided and war-torn countries, where the countervailing forces that might neutralise it are weak.[14]

[10] UN News, Violence, rhetoric, hate speech, drive atrocity crimes in Ukraine and beyond, Security Council hears, 21 June 2022, [Link]. Cohen runs Jigsaw, a department of Google, which develops the technology to fight disinformation, censorship and extremism on the Internet. At a UN SC Briefing of the UN Special Adviser on the Prevention of Genocide, he described the cyber war in Ukraine as "a crystal ball of what is likely to come".

[11] See Victoria Schwanda Sosik and Rajiv Arjan, 'Harnessing the Power of Digital Mobile Maps in Africa', AfriCHI'16: Proceedings of the First African Conference on Human Computer Interaction, 2016, pp.271-275.

[12] See Reuters Institute Digital News Report 2022, June 2022 [Link].

[13] An echo chamber is the effect of confirming bias among like-minded people in social networks.

[14] See Hannah Smidt, Mitigating election violence locally: UN peacekeepers' election-education campaigns in Côte d'Ivoire, Journal of Peace Research Vol 57(1), 2020. doi:10.1177/0022343319884993.

Social media's impact on conflict[15]

- Social media are transforming how, when, and whether conflicts manifest in fragile states.
- Social media threats are not restricted to social media users.
- Ethnic and sectarian tensions appear particularly susceptible to the weaponisation of social media.
- The dangers associated with the use of social media as a weapon are particularly pronounced during 'windows of risk'.
- There are a variety of key online 'influencers' with the ability to mobilise key constituencies either to promote social cohesion or to sow division.
- COVID-19 has exacerbated inter-group and community-state conflicts that play out online.
- Top-down efforts to police online disinformation may open the door to a crackdown on speech and activism.
- Online and offline civil society actors are important to societal resilience to digital threats.

Source: Mercy Corps, Social Media and Conflict: Understandings Risks and Resilience (2021)

3.2 How disinformation affects peace operations

International and regional organisations or alliances and their peace operations not only have to deal with disinformation in their environment, they are increasingly targets of campaigns themselves. This applies equally to UN, EU, OSCE and NATO missions. According to official EU statements, all its missions were affected in 2020. The Under-Secretaries-General of Peace Operations and Operational Support, Jean-Pierre Lacroix and Atul Khare, stated in 2021: "Rumours and manipulated falsehoods directly impact the security of our police, military and civilian peacekeepers."[16] Attacks are aimed at undermining the credibility of peace operations or questioning their ability to act (strategic level), obstructing mandate implementation (operational level) or destabilising the security situation in the country of deployment.[17]

The most prominent case in the sub-Saharan context involves attacks on the UN mission MINUSCA in the Central African Republic, which led the UN Security Council in June 2020 to condemn the false accusations and reaffirm the mission's impartiality (S/2020/545). After the presidential elections in late 2020, further disinformation campaigns threatened mission personnel and spread allegations of election meddling and collusion with armed groups that questioned the legitimacy and impartiality of the mission (S/2020/994). In early 2022, MINUSCA reported a slight decrease in campaigns against it, but found that the government was not fulfilling its obligation to refrain from spreading disinformation (S/2022/491).

Case studies conducted by the NATO Strategic Communications Centre of Excellence (STRATCOM COE) found similar evidence, when examining Russian narratives in the context of five peace operations (MINUSCA, EUTM RCA, MINUSMA, EUTM Mali and Opération Barkhane) in the Central African Republic and Mali. The most widespread narrative regarding MINUSCA portrays the mission as ineffective and unable to contain the ongoing violence. The West, particularly France and the USA, is accused of actively destabilising the Central African Republic – with the aim of keeping the country weak and subservient.

[15] The described insights of aid agency Mercy Corps are based on studies in Ethiopia, Iraq, Myanmar and Nigeria. See Mercy Corps, Social Media and Conflict: Understandings Risks and Resilience. Research Summary and Policy Brief, July 2021, [Link].

[16] Jean-Pierre Lacroix and Atul Khare, Protecting the truth, a requisite to peacekeeping, 17.05.2021 [Link].

[17] vgl. Giovanni Faleg and Nad'a Kovalcikova, Rising Hybrid Threats in Africa. Challenges and implications for the EU, EUISS Brief, March 2022 [Link].

Other examples: UN peace operations affected

MONUSCO in the Democratic Republic of Congo is currently subject to anti-mission sentiment in some parts of the country and warns that fake news spread by militias on social media is difficult to distinguish from reality and will soon be virtually undetectable. (UN SC/14966)

MINUSMA has been facing an increasing amount of misinformation about its mandate and activities since the emergence of the Wagner Group in Mali. As a result, local communities are less willing to share information with the mission, which affects its ability to prevent attacks. (UN SC/14966)

UNSMIL reports hate speech against activists, particularly on social media, which has led some civil society members working on women's rights and participation to leave the country. (UN S/2022/409)

In EU terminology, disinformation as it pertains to its crisis management operations falls under the heading Foreign Information Manipulation and Interference (FIMI). The latest EEAS StratCom Activity Report (2021) warns that FIMI could jeopardise the promotion of stability and the rule of law through military and civilian CSDP missions. It points to growing interference by Russia and China, which want to expand their influence in conflict regions through information manipulation. One example is Georgia, where the EUMM Georgia observation mission is subject to an ongoing, organised disinformation and discrediting campaign by Russia.[18] EUNAVFOR MED IRINI, the EU's naval mission in the Mediterranean tasked with enforcing the UN arms embargo against Libya, regularly struggles with disinformation from Turkey. The largest OSCE mission to date – the Special Monitoring Mission in Ukraine – was also subject to campaigns aimed at undermining the mission's credibility and questioning its neutrality.

Survey among ZIF secondees on disinformation (2021)

From 12 October to 3 November 2021, ZIF conducted an online survey among its secondees on the "Use of digital technologies to combat hate speech and disinformation." The aim of the survey was to find out whether and, if so, how hate speech and disinformation manifest themselves in the mission environments and how missions respond. Of the 156 secondees contacted, 46 took part in the survey.

Almost 60% see disinformation as a significant or very significant problem in their mission area. Among other things, the respondents pointed to deliberate misinformation which targets political developments in the country of deployment, the role of international organisations, the presence of international troops or COVID-19. The perpetrators are thought to be predominantly internal actors, although external actors play a major role. The secondees identified Facebook as the dominant dissemination medium, followed by Telegram. Among traditional media, television and print are used in particular.

The majority of the missions are affected by disinformation (almost 70%), but predominantly weakly (39.13%). To a very large extent (80%), the attacks are directed at the reputation of the missions.

[18] Continuous evidence of Russia's activities is provided in the EUvsDisinfo database of the EU East StratCom Task Force: it contains over 14,101 examples of pro-Kremlin disinformation collected since the project's launch in May 2015 (as of 27 July 2022).

4. Central actors and their approaches

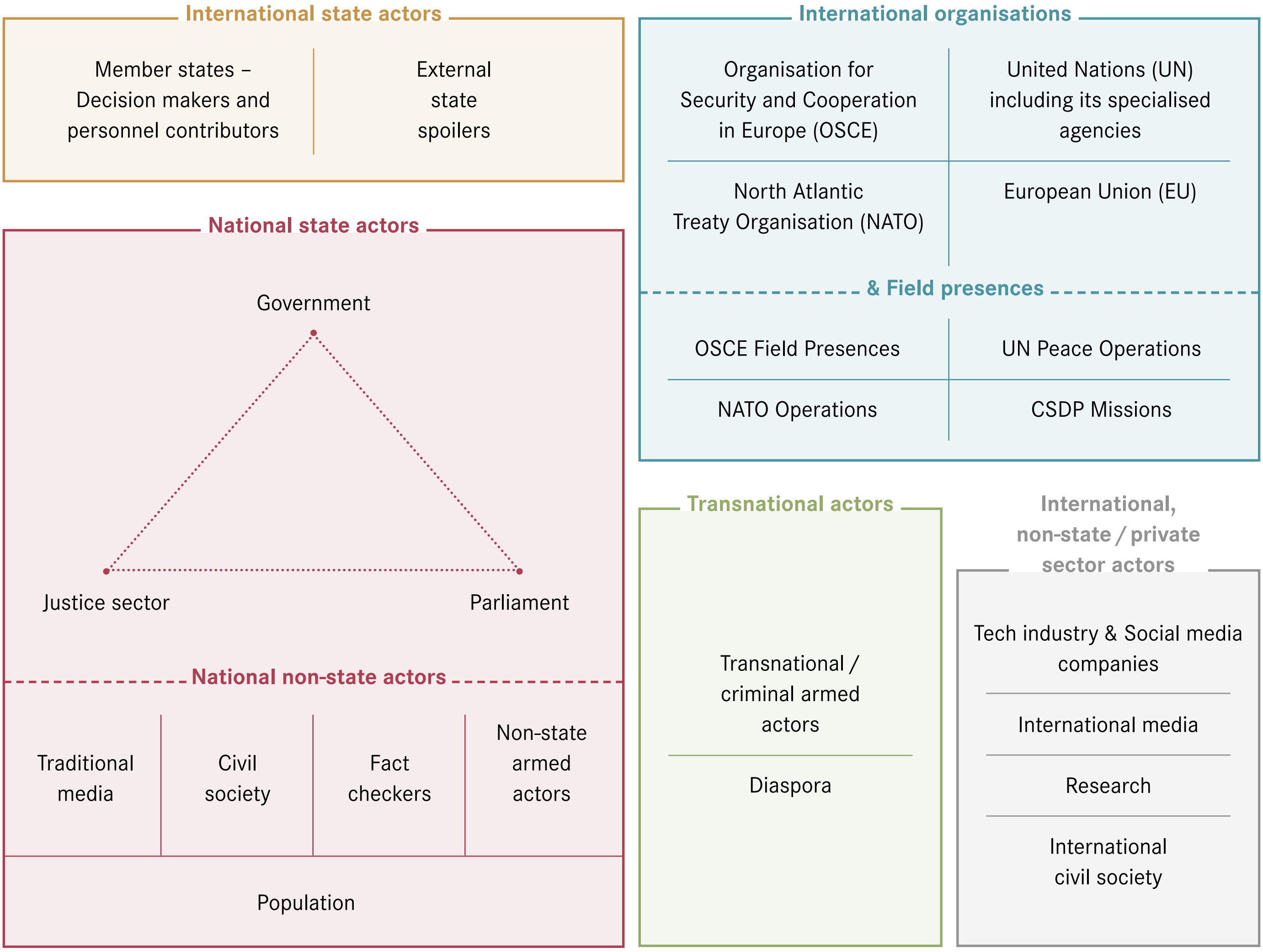
> *A surge in mis- and disinformation is also creating new and growing threats to the safety of UN personnel and the communities they serve.*
>
> Jean-Pierre Lacroix, Under-Secretary General for UN Peace Operations[19]

4.1 Mapping actors

A targeted response to disinformation requires a multi-stakeholder approach along multiple tracks. Basically, three groups of actors are involved in dealing with disinformation: legislators and regulatory institutions at state and intergovernmental level, the private sector (large information technology companies and their digital information and communication platforms) and civil society. In the complex environment of peace operations, a specific picture of actors emerges:

[19] Jean-Pierre Lacroix on the occasion of the International Day of United Nations Peacekeepers 2022, 02 June 2022 [Link].

Disinformation in the environment of peace operations: Breakdown of relevant actors


International state actors
Member states – Decision makers and personnel contributors
External state spoilers
International organisations
Organisation for Security and Cooperation in Europe (OSCE)
United Nations (UN) including its specialised agencies
North Atlantic Treaty Organisation (NATO)
European Union (EU)
& Field presences
OSCE Field Presences
UN Peace Operations
NATO Operations
CSDP Missions
National state actors
Government
Justice sector
Parliament
National non-state actors
Traditional media
Civil society
Fact checkers
Non-state armed actors
Population
Transnational actors
Transnational / criminal armed actors
Diaspora
International, non-state / private sector actors
Tech industry & Social media companies
International media
Research
International civil society

Source: ZIF

In the following, the approaches of central actors are described.

4.2 States

States can take on different roles: Organise disinformation, regulate it or be the addressee themselves. A large number of countries, including in Europe and sub-Saharan Africa, have taken regulatory measures against disinformation in the recent past. The scope of legislation ranges from media and election laws to cybersecurity and criminal laws. Some governments have enacted legal acts and codes of conduct on disinformation; others have taken steps to incorporate social media platforms into co-regulatory activities.

Fragile states where legislative processes are dysfunctional or laws are not enforced often cannot fulfil this regulatory role. In the face of fundamental social and economic challenges or a volatile security situation, dealing with disinformation is often simply not a priority. Moreover, in many conflict countries, regulations of online communication do not lead to the defence but to the restriction of the right to freedom of expression. Among others, 155 internet shutdowns were documented in 2020 in 29 countries, including Mali, Sudan, Iraq and Yemen, where peace operations are operating.

4.3 Big Tech and social media companies

Besides states, large technology companies[20] with their digital information and communication platforms are central players in dealing with disinformation. The industry has recognised the destabilising potential of social media and has taken measures to counteract the problem (e.g. by changing guidelines or supervisory mechanisms). Design decisions can also reduce the emergence of filter bubbles [21] and echo chambers by including users in more ideologically diverse online communities. Especially in contexts of fragile statehood, technology companies are encouraged to use conflict-sensitive algorithms to reduce the reach of disinformation.[22] In conflict zones, where legal and state regulation and intervention on these platforms is limited, companies are left to create their own policies. This self-regulation has not always proven effective in removing false content or preventing spoilers from spreading misleading content.

4.4 Civil society

Civil society actors are engaged in combating disinformation in different ways. Their approaches include campaigns to promote digital and media literacy with the aim of strengthening the resilience of societies. For example, civil society groups such as Africa Check or InformAction try to promote the ability of citizens to check facts and critically engage with information through projects and strategic media partnerships. Other civil society groups take a more confrontational approach to disinformation by focusing on identifying and combating hostile narratives. One example is the regional fact-checking organisation Raskrinkavanje from Bosnia and Herzegovina, which works in partnership with the European External Action Service to combat disinformation and promote media literacy.

[20] The largest IT companies in the world are called Big Tech: Google (Alphabet), Amazon, Facebook (Meta Platforms), Apple and Microsoft.

[21] The term ‘filter bubbles’ describes the space populated by like-minded people as a result of algorithms, that provide users with individualised content.

[22] To ensure conflict sensitivity, a company should: (1) understand the context in which it operates; (2) understand the interaction between its activities and the context; (3) minimise the negative effects of its operations; (4) maximise the positive effects of its operations for peace. See JustPeace Labs, Technology in Conflict: Conflict Sensitivity for the Tech Industry, 2020 [Link].

Overview: Eight types of civil society approaches to counter disinformation

1. Fact-checking
2. Identifying disinformation narratives, assets, and coordinated inauthentic behaviour
3. Advocacy towards platforms
4. Advocacy towards governments
5. Public awareness/media literacy campaigns.
6. Building trusted networks for accurate information
7. International collaboration
8. Programmatic recommendations

4.5 International organisations and peace operations

United Nations

The United Nations have recently stepped up their efforts to regulate social media. In May 2020, UN Secretary-General Guterres presented a Roadmap for Digital Cooperation based on the recommendations of the independent High-level Panel for Digital Cooperation (2019). The Roadmap defines eight areas of responsibility which include protecting human rights in the digital world and promoting digital security. To strengthen the UN as a platform for dialogue among all relevant stakeholders, the Secretary-General subsequently appointed a UN Envoy on Technology. In his report Our Common Agenda, Guterres noted in August 2021 that "governance structures at the national and global levels have not kept pace with the inherently informal and decentralised nature of the Internet, which is dominated by commercial interests" (§ 92). The proposed Global Digital Compact, "to outline shared principles for an open, free and secure digital future for all", is to be adopted in September 2023 at a multi-stakeholder digital conference.

In addition to initiatives to set standards or apply existing standards to social media, the UN has developed strategic approaches in various thematic areas to deal with disinformation. In the context of the COVID-19 pandemic, this includes the global communication initiative Verified, which was considered successful and was based on a public-private partnership between the UN, the World Health Organisation, Facebook, WhatsApp and other messenger services. The initiative shared trusted, accurate information from online (and offline) channels on health issues and sought to reduce the spread of false messages by changing media behaviour. Building on this model, the UN should continue to strengthen its key role in gathering and disseminating reliable and verified information, according to Secretary-General Guterres (Our Common Agenda, § 26).

The UN can play a key role in gathering and disseminating reliable and verified information.

Peace operations

For peace operations, there is as yet no dedicated overarching policy on how to deal with disinformation. However, there are some guiding documents: The new Strategy for the Digital Transformation of UN Peacekeeping (2021) describes hate speech, disinformation and misinformation as a threat to the safety of personnel and to mandate implementation. The strategy marks a significant step towards improving the security of mission staff and effective mandate implementation through the use of digital technologies. Also in

2019, Secretary-General Guterres had already published his first Strategy and Plan of Action on Hate Speech, which was followed by a Detailed Guidance on Implementation for United Nations Field Presences in September 2020. Some of the 13 fields of action of the strategy are also relevant for dealing with disinformation and are already being implemented in missions (e.g. observation and analysis; addressing root causes, drivers and perpetrators; use of education; cooperation with media; use of technology; development of guidelines for external communication; use of partnerships). In order to determine objective criteria for deciding whether and how to restrict freedom of expression, the UN Office of the High Commissioner for Human Rights (OHCHR) adopted the Rabat Plan of Action[23] in 2013, which is also referred to in the strategy against Hate Speech.

In July 2022, the UN Security Council addressed strategic communications in peace operations for the first time.

On 12 July 2022, the UN Security Council addressed strategic communications in peace operations for the first time. It emphasised its importance for mandate implementation and the safety of peacekeepers and civilians, and mandated Secretary-General Guterres to conduct a strategic review of StratCom in UN peace operations and headquarters by April 2023 (UN SC/14966).

Examples of mission-specific approaches:

UNMISS in South Sudan set up a WhatsApp group with 500 opinion leaders to seek and then respond to their assessment of the mission's performance and to inform the population about UNMISS tasks. Its mandate (esp. para. 7(c)(iii)) further empowers the mission to use all necessary means to monitor, investigate and report on incidents of hate speech and incitement to violence among the population. UNMISS has also trained reporters in conflict-sensitive journalism.

MINUSMA in Mali conducted training for journalists, radio reporters and bloggers on the effects of disinformation and on fact-checking.

MINUSCA in the Central African Republic distributed 50,000 solar-powered radios to communities to help them access information and combat disinformation. In addition, MINUSCA addressed disinformation directed at its staff through its own social media channels, mass text messages, press releases and radio spots.

UNSMIL in Libya, in consultation with journalists, activists and civil society actors, established a set of principles for the use of social media by a prominent group of journalists, activists and opinion leaders during the peace process in the country.

[23] See also the short explanatory video on YouTube [Link].

European Union

Disinformation has been an increasing political and security challenge for the EU since the Russian aggression in Ukraine in 2014 and has been recognised as such in numerous documents such as the Action Plan against Disinformation (2018), the European Democracy Action Plan (2020) or the Strategic Compass for Security and Defence (2022). Since March 2015, the organisation has developed a wide range of tools to counter digital disinformation from external actors. The central institution in the implementation is the European External Action Service (EEAS) with the Stratcom (SG.STRAT.2) Division.[24]

STRAT.2 is responsible, among other things, for the implementation of the Action Plan against Disinformation[25] (2018), the EU's most recent strategy document in this area. The approach is based on four pillars (analysis, coordination of measures, mobilisation of the private sector, strengthening the resilience of societies). Based on the action plan, among other things, a Rapid Alert System (RAS) was set up in 2019 to provide real-time warnings about disinformation campaigns. A STRAT.2 flagship project is also a comprehensive website EUvsDisinfo, which identifies Russian disinformation against the EU, its member states and countries in the common neighbourhood based on analysis of publicly available sources.

CSDP missions

The EU's civilian and military Common Security and Defence Policy (CSDP) operations respond to disinformation and FIMI in a mission-specific manner. The Strategic Compass for Security and Defence, which addresses the hybrid threat of foreign information manipulation and interference, in March 2022 announced various measures to better support CSDP missions. An EU Hybrid Toolbox against hybrid threats is to be developed in 2022, which will also include EU Hybrid Rapid Response Teams, as well as a toolbox against FIMI (Foreign Information Manipulation and Interference Toolbox). The goal is to equip all CSDP missions with the necessary capabilities and resources by 2024 in order to effectively use the instruments of the toolbox.[26] For civilian CSDP missions, a so-called Mini-Concept on Hybrid Threats was also developed with the aim of strengthening the resilience of missions and host-state institutions against FIMI.[27]

For civilian CSDP missions, a so-called Mini-Concept on Hybrid Threats was developed with the aim of strengthening the resilience of missions and host-state institutions.

OSCE

At the institutional level, disinformation is primarily the responsibility of the OSCE Representative on Freedom of the Media (RFoM). His/her remit includes monitoring media developments as part of an early warning function, as well as assisting participating states in meeting their commitments to freedom of expression and free media. The approaches developed address disinformation primarily as a challenge to freedom of information rather than as a destabilising aspect of inter-state relations. Since 2021, the RFoM has organised Expert Roundtables on Disinformation to address the impact of disinformation on peace and security.

Field presences

In the OSCE, measures against disinformation are embedded in the early warning system. For example, the Conflict Prevention Centre in the OSCE Secretariat co-operates with a network of Early Warning Focal Points in the OSCE field presences, who increasingly include observing the media landscape in their work. So far, there is no overarching strategy or guidelines on how to deal with disinformation, so field missions follow individual approaches.

[24] In the StratCom Division, there are, among others, the three StratCom Task Forces East (2015), Western Balkans and South (both 2017), see for the structure: [Link].

[25] A good overview of the contents can be found here: Audit preview. EU action plan against disinformation, March 2020, Table 1 [Link].

[26] See Strategic Compass for Security and Defence, p.28 [Link].

[27] See Crista Huisman, A policy response to foreign information manipulation's impact on civilian CSDP missions, 11 July 2022, ZIF TECHPOPS-Blog [Link].

However, efforts are underway to expand capacities in this field in order to sensitise staff to the (questionable) reliability of information and to strengthen knowledge in the area of social media (i.e. social media monitoring and social media literacy).[28] Some field presences such as the OSCE Mission in Skopje have set up a Social Media Monitoring Unit. All OSCE presences are asked to conduct at least an analysis of the media landscape, including radio and print media, as part of their conflict analysis. The extent to which this is done often depends on the political sensitivity of the environment and the available capacities and resources of the respective presence. The OSCE Mission to Bosnia and Herzegovina has also established a network of civil society organisations working against the spread of hate speech and publishes a monthly overview of the incidence of hate speech and countermeasures taken.

Some field presences such as the OSCE Mission in Skopje have set up a Social Media Monitoring Unit.

NATO

NATO identified hybrid threats and the misuse of digital information ecosystems as future threat scenarios as early as 2009/2010.[29] Since the Russian annexation of Crimea in 2014, the Alliance has identified a significant increase in hostile narratives, disinformation and propaganda and, following the 2018 Brussels Summit, has intensified its efforts to combat these hostile information activities. NATO is pursuing a twin-track model which, starting from an understanding of the information environment (understand), counters disinformation with various short- and long-term measures (engage). These include, in particular, (proactive) strategic communications and strengthening the resilience of societies.

To support its members, civilian Counter-Hybrid Support Teams (CHST) have been available on request since 2018; one was deployed for the first time in Montenegro in 2019[30]. In addition, the Alliance developed a Counter-Hostile Information and Disinformation Toolbox in 2021, which is currently being revised as a living document and is intended to focus more explicitly on NATO operations. The communiqué published after the 2021 Summit announced further engagement, and NATO's new Strategic Concept (2022) states that a hybrid crisis against allies could potentially trigger a collective defence obligation in accordance with Article 5.[31]

Close coordination with allies and partners is an important principle of NATO strategy. Together with the EU, it has increasingly incorporated disinformation into the broader context of its response to hybrid threats. One example of cooperation between the two organisations is the Rapid Alert System mentioned above, which strengthens each other's alert capabilities to detect enemy information activities. In addition, EU and NATO member states established the Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats) in Helsinki in 2017 to develop strategies against hacking, propaganda and disinformation campaigns.

NATO operations

The defence alliance has not yet developed a dedicated policy for dealing with disinformation in its areas of operation. The two current missions KFOR in Kosovo and the NATO Mission Iraq (NMI) react situationally to incidents, as do the NATO Battle Groups on the Alliance's eastern flank (Poland, Estonia, Latvia, Lithuania), which are strongly affected by Russian disinformation. Supported by Information Environment Assessment Reports from the headquarters, (proactive) strategic communications is the priority tool. Repeatedly disseminated narratives about NATO, its policies and operations are also intended to build resilience in the societies of deployed (and third) countries and are seen as the best line of defence.[32]

[28] For OSCE election observation missions, Guidelines for Observation of Election Campaigns on Social Networks were developed in 2021 [Link].

[29] See Karl Moritz Heil, Kollektive Strategien zur Abwehr digitaler Desinformation, Resilienz und Abschreckung bei EU und NATO, München 2021, p.85.

[30] See Lisa Sanchez, Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda, Special Report, NATO Parliamentary Assembly, October 2021, p.14f. [Link].

[31] See NATO 2022, Strategic Concept, No.27 [Link].

[32] Conversation with NATO Headquarters Strategic Communications on 06 July 2022.

5. Closing the gap: Options for peace operations

> *Peace operations are still figuring out how best to confront the scourge of misinformation, disinformation, and hate speech.*
>
> Jake Sherman[33]

Given the rapidly changing information landscape and the dynamic nature of disinformation campaigns, peace operations need to improve their existing approaches to countering disinformation and to develop new innovative tools. In doing so, missions are challenged in several ways: As **targets** of disinformation, they must protect themselves from attacks on the mission and its personnel, ward them off and repair any damage (e.g. loss of trust or legitimacy). As an actor in the country of deployment, they can be **part of the solution** by combating acute disinformation, which impairs mandate implementation and destabilises the security situation in the conflict area. Peace operations can also try to mitigate the impact of disinformation by addressing the causes of conflict.

Apart from isolated mandates to combat hate speech, peace operations to date have rarely had a dedicated remit with regard to disinformation. One possibility is to place the task within the framework of protection of civilians (POC) mandates, through which missions can intensify and structure their activities against disinformation.[34]

Action is required not just at the mission level, but also at the headquarters of international organisations.

However, action is required not just at the mission level, but also at the headquarters of international organisations, which are responsible for drafting guidance for all missions on how to deal strategically with disinformation. In particular, there are options for peace operations to take action and close gaps in the following four areas:

1. Situational Awareness

- Systematically map the media landscape and monitor social media as an integrated part of the common operating picture and analysis of conflict dynamics and actors.
- Improve the understanding of the logic/scheme of disinformation campaigns among field personnel.
- Identify vulnerabilities to disinformation in the run-up to or during sensitive events, such as elections.

2. Response

- Implement a mission-wide communication strategy closely linked to the overall policy objectives of the mission.
- Tailor a communication approach to target the groups most vulnerable to disinformation.
- Play a key role in obtaining and disseminating reliable and verified information, developing alternative narratives depending on the situation.[35]
- Monitor human rights in the digital space and report on violations; raise awareness among national human rights organisations.

[33] Jake Sherman, Strategic Communications in UN Peace Operations, IPI, August 2021, [Link].

[34] UN peace operations with a Protection of Civilians mandate are generally tasked with countering the spread of hate speech with information and strategic communications as part of their "protection through dialogue and engagement" activities, see UN POC Policy, No.53 [Link].

[35] UN SG Guterres: "The United Nations must play a more deliberate role as an information actor in conflict environments…[and] seen as a trusted source by…facilitating inclusive dialogue, demanding the removal of harmful speech, calling leaders to account, and promoting the voices of peace and unity". UN News, Reliable information 'a matter of life and death' UN chief tells Security Council, 12 July 2022 [Link].

3. Resilience

Strengthening the resilience of peace operations

- Raise awareness of the issues among mission personnel; analyse vulnerabilities; identify and review resilience factors.
- Conduct regular in-depth assessments of IT and communication systems in missions to identify and monitor vulnerabilities to disinformation.

Strengthening the resilience in the host country[36]

- Advise host governments on the development of laws regulating online platforms as well as data protection.
- Foster media pluralism and quality journalism.
- Strengthen democratic resilience in the population by providing information.
- Promote media and information literacy in society.
- Build capacity in civil society, especially among media representatives and young people by strengthening media literacy and dialogue processes.
- Support dialogue processes in order to reduce the breeding ground for disinformation in the long term.

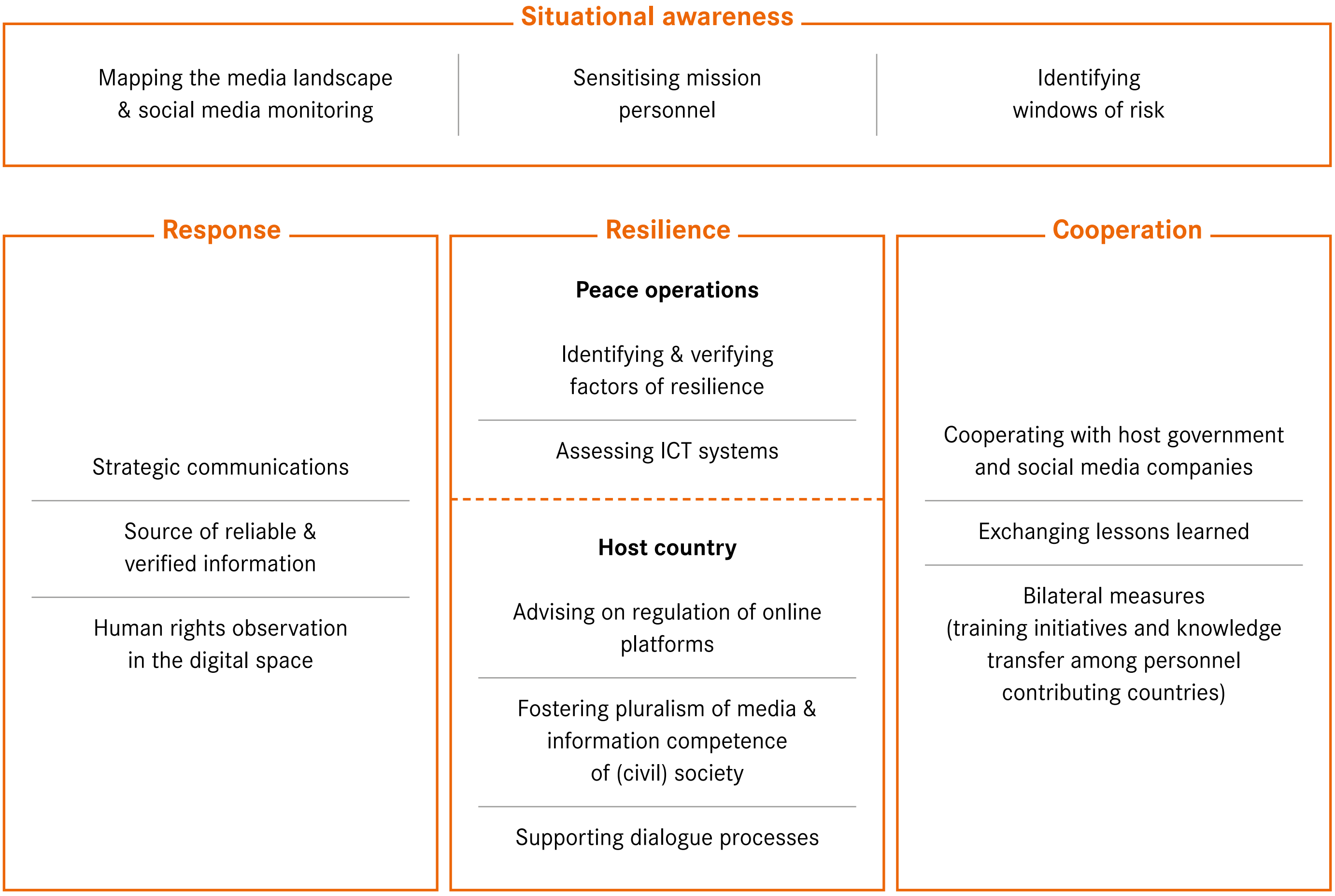
4. Cooperation

- Cooperate with host governments and social media companies to enable the regulation of content, but also to base this regulation on agreed criteria (Rabat Threshold Test) and thus prevent abuse.
- Exchange lessons learned with other international actors, especially in humanitarian operations (for instance with respect to protecting human rights in the digital space) and exchange of knowledge and experience between peace operations.
- Conduct further bilateral measures such as training initiatives and knowledge transfer among personnel-contributing countries.

In order to effectively combat disinformation, missions must also have the necessary human, financial and technological **resources**. This includes training mission personnel in social media analysis, strategic communications and data protection, as well as using open-source information and the necessary technologies and applications.

[36] See Pavel Havlíček, Andrei Yeliseyeu, Disinformation Resilience Index in Central and Eastern Europe in 2021, EAST Center, 2021 [Link].

Options for peace operations



Situational awareness

Mapping the media landscape & social media monitoring

Sensitising mission personnel

Identifying windows of risk

Response

Strategic communications

Source of reliable & verified information

Human rights observation in the digital space

Resilience

Peace operations

Identifying & verifying factors of resilience

Assessing ICT systems

Host country

Advising on regulation of online platforms

Fostering pluralism of media & information competence of (civil) society

Supporting dialogue processes

Cooperation

Cooperating with host government and social media companies

Exchanging lessons learned

Bilateral measures (training initiatives and knowledge transfer among personnel contributing countries)

Source: ZIF

6. Conclusion

Digital disinformation by state and non-state actors is a significant problem for peace operations. It undermines their credibility, challenges their ability to act, hinders mandate implementation and destabilises the security situation in areas of operation. International organisations have established various approaches to deal with this complex phenomenon and are in the process of expanding their strategies and tools. Peace operations as an actor in fragile contexts that are often particularly affected by disinformation could make greater use of various options and entry points for action. A number of approaches are visible and are evolving rapidly and dynamically, so that this study can only provide a snapshot of the current situation. What is clear, is that the increasing spread of digital disinformation, the myriad ways in which it can be used to manipulate opinion, and the expected further use of new technologies to professionalise state-led campaigns in particular, challenge international organisations and peace operations to keep pace.

The increasing spread of digital disinformation and the increasingly professional campaigns challenge peace operations to keep pace.

7. Abbreviations

CAR	Central African Republic
COVID-19	Coronavirus Disease
CSDP	Common Security and Defence Policy
DGC	UN Department of Global Communications
DPO	UN Department of Peace Operations
DPPA	UN Department of Political and Peacebuilding Affairs
DRC	Democratic Republic of the Congo
DOS	UN Department of Operational Support
EEAS	European External Action Service
EU	European Union
EUMM Georgia	EU Monitoring Mission in Georgia
EUNAVFOR Med Irini	EU Military Operation in the Mediterranean
EUTM Mali	EU Training Mission in Mali
EUTM RCA	EU Training Mission in the Central African Republic
FIMI	Foreign Information Manipulation and Interference
KFOR	Kosovo Force
MINUSCA	UN Multidimensional Integrated Stabilization Mission in the CAR (*Mission multidimensionnelle intégrée des Nations unies pour la stabilisation en Centrafrique*)
MINUSMA	UN Multidimensional Integrated Stabilization Mission in Mali (*Mission multidimensionnelle intégrée des Nations unies pour la stabilisation au Mali*)
MONUSCO	UN Organization Stabilization Mission in the DRC (*Mission de l'Organisation des Nations Unies en République Démocratique du Congo*)
NATO	North Atlantic Treaty Organisation
NMI	NATO Mission Iraq
OHCHR	UN Office of the High Commissioner for Human Rights
OSCE	Organisation for Security and Cooperation in Europe
PoC	Protection of Civilians
RFoM	Representative on Freedom of the Media
StratCom	Strategic Communications
UN	United Nations
UN GA	UN General Assembly
UN SG	UN Secretary-General
UNMISS	UN Mission in South Sudan
UN SC	UN Security Council
UNSMIL	UN Support Mission in Libya

www.zif-berlin.org