United Nations
Department of Peace Operations Ref. 2024.15
Classification: For public distribution

Policy

Information Integrity in Peacekeeping Settings

Approved by:	Jean-Pierre Lacroix, USG DPO
Effective date:	16 December 2024
Contact:	*DPO Information Integrity Unit*
Review date:	*December 2026, or as needed*

DPO POLICY ON
INFORMATION INTEGRITY IN PEACEKEEPING SETTINGS

Contents:

A. PURPOSE AND RATIONALE

1. This policy sets out the approach, principles, roles and responsibilities and processes by which United Nations peacekeeping operations and Headquarters will strengthen information integrity and address misinformation, disinformation and hate speech (MDH). While not a new imperative for peacekeeping operations, the current policy has been developed in response to the grave and growing threat to information integrity posed by harmful information in peacekeeping settings. False and/or manipulated information can weaken consent and support for peacekeeping, reduce the space for mandate implementation, threaten the safety and security of peacekeepers and fuel divisions in host countries. MDH can also hinder mandate implementation, including support to peace processes and the protection of civilians. In recognition of this challenge, through the Global Principles on Information Integrity, the Secretary-General has called on the international community to strengthen the information ecosystem – so that freedom of expression is fully enjoyed and information that is accurate, reliable, free from discrimination and hate is available to all in an open, inclusive, safe and secure information environment.[1] This policy sets out a peacekeeping response to the Secretary- General's call.

2. The policy responds to and is grounded in General Assembly and Security Council guidance. In 2022, the General Assembly requested the Secretary-General to "establish a framework to address [misinformation and disinformation]" and "to take all appropriate steps to track sources of disinformation and misinformation, to analyze trends, and to mitigate any negative impacts to the mission's mandate or personnel."[2] Further, in 2023, the General Assembly's Special Committee on Peacekeeping Operations (C34) requested that the Secretariat: "monitor and report on instances of misinformation and disinformation and to share this information with all relevant stakeholders;" "that adequate resources and expertise be provided to peacekeeping operations to identify, monitor, analyse, respond to and counter misinformation and disinformation," and that the Secretariat "work with national authorities in this regard, as appropriate."[3] For its part, the Committee on Information of the General Assembly has expressed "grave concern about

---

[1] United Nations Global Principles for Information Integrity, June 2024, https://www.un.org/en/information-integrity.
[2] A/RES/76/274, June 2022.
[3] Report of the Special Committee on Peacekeeping Operations, A/AC.121/2023/L.3.

information manipulation, including disinformation, by States, aimed at attempting to justify, provoke or encourage any threat to peace."[4]

3. The Security Council has also mandated individual peacekeeping missions to take action.[5] Resolution 2686 (2023) requested peacekeeping missions "to monitor hate speech, racism and acts of extremism that negatively affect peace and security, and to include reporting on these issues in their regular reporting to the Council."[6]

4. Under the leadership of the Secretary-General, the United Nations system has actively worked on addressing hate speech, in line with international human rights law. Key initiatives include the Rabat Plan of Action (2012) and its six-part test, which offers a framework to assess whether an instance of hate speech has reached the threshold of incitement to discrimination, hostility or violence as set out in article 20(2) of the International Covenant on Civil and Political Rights (ICCPR).[7] The United Nations Strategy and Plan of Action on Hate Speech (2019) provides strategic guidance for the United Nations system to address hate speech at the national and global levels.[8]

5. Considering the above, this policy establishes a system to monitor, analyse, respond and evaluate actions taken to address MDH and strengthen information integrity. The policy explains the principles that govern actions taken by peacekeeping operations and Headquarters.

6. This policy is aimed at peacekeeping practitioners at all levels in the field and Headquarters and is of particular relevance to components involved in the monitoring, analysis, response and evaluation cycle and crisis management functions, including but not necessarily limited to Strategic Communications, Joint Operations Centres (JOCs), Joint Mission Analysis Centres (JMACs), Political Affairs, Civil Affairs, Human Rights, Protection of Civilians, Gender, Safety and Security, Field Technology Sections (FTS), Police and Force components (notably U/S/G2, SIOC, and UNPOL intelligence and criminal analysis units), Peacekeeping-Intelligence entities and coordination structures; Information Operations; Mission Community Outreach; Military Strategic Communications.

7. This document will be reviewed every two years, with the possibility of an early review, if necessary, given the fast-paced and evolving nature of the digital information environment.

B. SCOPE AND KEY FACTORS

8. This policy applies to United Nations peacekeeping operations and DPO. It pertains to MDH in the digital and offline information environment as they affect (i) the safety and security of peacekeeping missions and (ii) mandate implementation of each peacekeeping mission. While the policy is mandatory, its provisions should be adapted to the context, size, available resources and specific mandates of each operation. The absence of language on MDH in mission-specific Security Council resolutions does not preclude missions from addressing MDH as part of their situational awareness, security risk mitigation and substantive areas of work.

---

[4] Report of the Committee on Information, 44th Session, 2022 (A/77/21).
[5] See Reference section for resolutions.
[6] SCR 2686, OP11
[7] A/HRC/22/17/Add.4; https://www.ohchr.org/en/freedom-of-expression.
[8] Since 2020, all peace operations have been tasked with monitoring, analysing and mitigating harm caused by hate speech. See United Nations Strategy and Plan of Action on Hate Speech: Detailed Guidance on Implementation for Field Missions, 2020. https://www.un.org/en/genocide-prevention/hate-speech/strategy-plan-action

9. **Situating harmful information.** (Refer to Section E for definitions) Misinformation, disinformation and hate speech are part of broader online and offline information environment. *Intent* and *veracity* are commonly understood as the defining variables of misinformation, disinformation and malinformation. (Note that malinformation is information that is based on reality, used to inflict harm on a person, social group, organisation or country. [9]) These concepts are overlapping and sometimes difficult to distinguish in practice. For example, some forms of disinformation can amount to incitement to violence, hostility and discrimination, which are the most severe forms of hate speech prohibited under international law.[10] Ascertaining the intent of the propagator of information may be challenging, while veracity in and of itself does not signify the absence of harm. Many of the concepts related to harmful information are imperfect, contingent on the broader social, political and historical context, open to interpretation and likely to evolve as new information harms and responses emerge. Nevertheless, despite their limitations, they provide parameters to understand the information environment, and to guide responses. Three significant factors should be understood:

   (i) Legal framework. The international legal framework treats hate speech and misinformation and disinformation differently. Under international human rights law (IHRL), which applies in all contexts,[11] any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence is prohibited.[12] Falsity or manipulation of information are insufficient grounds for limiting freedom of expression. Thus, misinformation and disinformation are not a valid basis to restrict expression unless it reaches the threshold outlined in Article 19(3) or Article 20 of the International Covenant on Civil and Political Rights (ICCPR). Any restrictions must adhere to the principles of legality, necessity and legitimate objectives as specified in the Covenant. Furthermore, the UN Human Rights Committee commented that defamation laws should include such defences as the defence of truth and they should not be applied with regard to those forms of expression that are not, of their nature, subject to verification. [13] Similarly, International Humanitarian Law (IHL) does not explicitly prohibit tactics such as ruses of war, propaganda, misinformation or disinformation during armed conflict.[14] Certain limitations exist, such as the prohibition of perfidy, [15] as well as the prohibition of harmful consequences on civilians from information operations, including threats of violence or attacks to spread terror among civilians, incitement to commit war crimes and orders to attack civilians.[16] Limitations on speech and expression are therefore only rarely the appropriate avenue for addressing instances of MDH.

   (ii) Target: While hate speech targets people (individuals, groups, communities) based on their identity, misinformation and disinformation can include people, and a wider range

---

[9] Cherilyn Ireton and Julie Posetti (eds.), “Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training”, https://unesdoc.unesco.org/ark:/48223/pf0000265552

[10] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Disinformation and freedom of opinion and expression during armed conflicts. August 2022. A/77/288, p.5

[11] Excepting situations in which a government has derogated from relevant ICCPR provisions.

[12] ICCPR Article 20(2).

[13] CCPR/C/GC/34, para. 47.

[14] A/77/288 and https://guide-humanitarian-law.org/content/article/3/perfidy/

[15] Perfidy constitutes acts inviting the confidence of an adversary to lead them to believe they is entitled to, or are obliged to grant, protection under the rules of international humanitarian law applicable in armed conflict, with intent to betray that confidence.

[16] Geneva Conventions of 12 August 1949, common article 3.

of targets, including States, governments, institutions and non-state actors, as well as values and concepts. Some forms of misinformation and disinformation may take the form of hate speech.

(iii) Responses: The default response in all situations should be towards the promotion of free, open and transparent exchange of information across society. The appropriate or most effective response to specific cases of MDH may vary. For example, tailored strategic communications and/or community engagement may be a viable response to misinformation about the role of a peacekeeping operation. However, those measures alone would not effectively address a disinformation campaign that may be orchestrated by local, regional or international conflict actors with a strategic intent to undermine the mission. An effective response may require additional measures such as political engagement or reporting to technology platforms on inauthentic behaviour.[17]

10. **MDH and conflict environments.** Populations in situations of armed conflict are particularly vulnerable to MDH, as rumours circulate and proliferate with ease in times of political uncertainty and change. [18] Online disinformation campaigns can contribute to social and ethnic polarization and the destruction of social ties by enabling echo chambers of like-minded groups and sabotaging horizontal connections between individuals on either side of a conflict, with impacts on different age and social groups.[19] Understanding these dynamics is a critical part of the analysis and design of effective responses in specific mission settings.

11. Disinformation is used by parties to conflict or actors outside the conflict theatre in support of strategic goals. It can be deployed to influence and shape public opinion; to sow uncertainty or confusion; or to isolate an adversary by creating new rifts or exploiting existing differences. It may be part of a multicomponent campaign composed of digital and real-world tactics aimed at shaping perceptions and worldviews. Digital tactics may include artificial intelligence-generated content, inauthentic social media accounts or news portals, astroturfing, copypasta, rapid link sharing, typosquatting, etc. Real-world actions may, for example, include forged documents, orchestrated demonstrations and the use of front organisations or agents of influence. Misinformation in the form of rumours or conspiracy theories can be leveraged as part of disinformation campaigns.

12. **MDH and Freedom of Opinion and Expression.** Article 19 of the Universal Declaration of Human Rights states:[20]

---

[17] Meta, for example, defines "inauthentic behavior" as user efforts to "misrepresent themselves, …use fake accounts, artificially boost the popularity of content or engage in behaviors designed to enable other violations under our Community Standards." Facebook Community Standards, as cited in the Report of the Secretary-General "Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms," A/77/287, 12 August 2022.

[18] Rumors enable individuals and groups to function in times of acute stress, reinforce group solidarity and provide guidance when verifiable facts are hard to come by and security-related anxiety is high. See Adam Sandor: "The power of rumour(s) in international interventions: MINUSMA's management of Mali's rumour mill", International Affairs 96: 4 (2020). 913-934; and Greenhill, Kelly M. and Ben Oppenheim. "Rumor Has It: The Adoption of Unverified Information in Conflict Zones." *International Studies Quarterly* 61, no. 3 (2017): 660–76. https://doi.org/10.1093/isq/sqx015

[19] Asmolov, Gregory: "The Disconnective Power of Disinformation Campaigns," SIPA Journal of International Affairs, 18 Sept 2018 https://kclpure.kcl.ac.uk/ws/portalfiles/portal/108892725/Asmolov_The_Disconnective_Power_of_Disinformation_Campaigns.pdf

[20] Similarly, Article 19 of the International Covenant on Civil and Political Rights (ICCPR) states, among other things, that "1. Everyone shall have the right to hold opinions without interference" and that "2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (Emphasis added.)

MDH can interfere with a person's right to seek and receive information. For example, in situations of overwhelming artificial amplification of false or misleading narratives, and/or when alternative narratives are suppressed. In this sense, information integrity is inherently linked to a functional civic and political space, in which freedom of the press, the safety and security of journalists and other media workers, and freedom of assembly and association are upheld and in which an informed public is resilient to MDH and able to participate fully and effectively in public affairs. Mislabelling or conflating criticism and negative sentiment with MDH risks undermining freedom of opinion and expression as well as civic space.[21]

13. **MDH and political freedoms**. More broadly, there is an inverse correlation between increased MDH and political freedoms and civic space. Manipulated information contributes to polarisation and eroded trust, with impacts on participation in political processes.

14. **Gendered MDH**. MDH can replicate and intensify harmful gender norms and serve to silence women and gender diverse voices. In conflict environments, women and girls are more likely to receive information by word of mouth and may be particularly vulnerable to certain types of MDH.[22] MDH may be used to reinforce prejudices, bias, structural and systemic barriers to gender equality, which can manifest as technology-facilitated gender- based violence that threatens safety of individuals and undermines the full, equal, and meaningful participation of women and girls in political processes. Women peacekeepers, including the leadership of peace operations, can also become targets of MDH campaigns.

C. POLICY

C1. Guiding Principles

15. Peacekeeping action in relation to information integrity shall be guided by the principles described in this section, all of which align with the policies on Strategic Communications in Peace Operations and Peacekeeping-Intelligence. [23] All subordinate guidance, directives, plans and operations will comply with and apply these principles.

    15.1. Multidisciplinarity. A combination of skills and expertise will be applied to understand MDH, devise and implement preventive and responsive measures, and to strengthen information integrity, within the parameters of each mission's mandate, operational context and available resources. These include expertise and skills in political and behavioural sciences; information acquisition and processing, qualitative and quantitative analysis; human rights; gender-responsive analysis; strategic communications; and planning, operational management and coordination. Moreover,

---

[21] First, falsity and manipulation are not in themselves sufficient ground to restrict freedom of expression, unless they reach the threshold established under Article 19(3) of the International Covenant on Civil and Political Rights or if they amount to incitement to violence, hostility or discrimination, which is prohibited under international law.

[22] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Gendered disinformation and its implications for the right to freedom of expression. August 2023. A/78/288.

[23] Ref. DPO 2024.04 / DPPA 2024.01; 1 June 2024; DPO 2019/08, April 2019

strengthening information integrity requires a multistakeholder approach, involving a diverse set of actors working across areas, including Member States, technology platforms, United Nations entities, civil society, the media, host communities and the research community.

15.2. Integrated effort. Effective action in the long-term benefits from an integrated, whole-of-mission and whole-of-UN approach at the country level. In integrated mission settings, relevant entities in the United Nations family should come together around jointly conceived and coordinated United Nations activities to strengthen information integrity and address MDH, with specific responses to MDH as it affects United Nations mandates. Within peacekeeping missions, various components should have the capacity to make important contributions to the monitoring, analysis and responses to MDH, including the Force, Police, Political and Civil Affairs, Human Rights, Security, Gender, Protection of Civilians, JOC, JMAC, and Strategic Communications components and advisers. More broadly, consultation, and where relevant, coordination with regional organisations that share the theatre of operations should take place.

15.3. Proactive, preventive stance. Anticipating when information integrity may be compromised and mitigating the risk and impact of MDH requires a proactive, preventive stance across the monitoring-analysis-response-evaluation cycle described in this policy. Such efforts should be grounded in human rights and ensure that efforts to address MDH do not negatively impact on human rights.

15.4. People-centred. Peacekeeping action to counter MDH and strengthen information integrity must consider the aspirations, hopes, concerns and grievances of host communities. Legitimate criticism should be recognised and peacekeeping missteps and errors acknowledged with humility. This requires a transparent, non-defensive approach, especially in regard to performance and misconduct. Freedom of opinion and expression, association and peaceful assembly should be promoted and upheld in actions taken by missions with respect to information integrity. Missions should engage with a diverse representation of people affected by MDH to deepen understanding of harms and enable agency and ownership of responses.[24] Putting people at the centre also means adopting a “do no harm” approach that is aware of potential negative second-order effects of actions against MDH and takes mitigation measures to avoid them.

15.5. Gender- and age-responsive: When analysing and responding to MDH, it is essential to identify gender- and age-specific MDH trends and impacts. The response should acknowledge the varied gender- and age-specific roles played in contributing to or being targeted by MDH. A thorough MDH response should be guided by a gender- and age-responsive conflict analysis that considers the intersectionality between these two characteristics.

15.6. Non-clandestine. Activities to monitor, analyse and respond to MDH will be undertaken in line with Security Council and General Assembly mandates, in full compliance with the United Nations Charter and consistent with the overall legal framework governing United Nations peacekeeping operations. Activities will be conducted in full respect of human rights, particularly in relation to rights to privacy, freedom of expression, and peaceful assembly and association. Consistent with the DPO Policy on Peacekeeping-Intelligence, clandestine activities, defined as the

[24] These include youth groups and women’s organizations, marginalized groups, ethnic groups, indigenous communities, traditional and faith-based leaders, refugee and IDP communities, and other stakeholders.

concealment of activities because they are illicit and/or inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations are outside the boundaries of this policy.

15.7. Respects data protection and privacy. Data gathered for monitoring and analysis of the information environment or used as part of response activities will be managed in accordance with United Nations confidentiality, classification and privacy standards and rules, and shall be gathered solely for the purposes of safety and security.

C2. Approach to strengthening information integrity and tackling MDH

16. **Understand the MDH landscape.** The first step to tackling MDH is understanding the environment in which information may cause harm. This analysis should be conducted by mission components with analytical capabilities, and part of conflict analyses that the mission may be undertaking or be contributing to (including mission concepts, concepts of operations, or Common Country Assessments – CCAs).

16.1. Historical, political and social context. Peace operations' operating contexts are typically characterised by trends of social, political and economic exclusion, inequality and polarisation, often accompanied by widespread mistrust in institutions, weak social cohesion and limited rule of law. These are fertile conditions for MDH to take root. MDH drives wedges and exploits pre-existing societal divisions, often along lines of identity and often exacerbating the targeting of minorities or other marginalized groups. To understand why certain MDH narratives may resonate requires an understanding of the historical, political, social/cultural and economic context, including gender relations, as well as familiarity with key political, security and economic actors. The geopolitical environment in which the conflict is playing out may also impact the drivers of MDH.

16.2. Online/offline dynamics. The MDH pathways between online and offline environments are non-linear and two-way. In environments with low internet penetration, individuals with access to social media may serve as important social hubs for information, spreading news in communities. Rumours or hate speech circulating offline may become viral if relayed online. In such environments, those with access to social media may belong to educated, urban elites, and thus have a disproportionate level of influence – making the online chatter as relevant as the offline environment.

16.3. Different media, different user communities. The demographics and use of media, including social media, varies from country to country and between different populations and groups (e.g. indigenous populations, migrants, diasporas, youth, etc.). Whether in designing strategic communications campaigns, or in attempting to understand the strategy behind a disinformation operation, understanding which communities tend to use what media and which digital channels is key.

16.4. Diaspora actors. How MDH spreads online is intrinsically related to the digital architecture of technology platforms. MDH can be relayed in a matter of seconds between host countries and diaspora communities abroad. Powerful influencers in diaspora dominate the online political discourse in some countries, making understanding the positions and viewpoints of individuals and communities in diaspora critical to an understanding of the MDH landscape in a peacekeeping setting.

16.5. Political economy of MDH. The production and distribution or amplification of MDH – especially disinformation and hate speech – is increasingly privatised. A

decentralised political economy has emerged in recent years across various regions, in some cases involving regional or international service providers that produce and amplify content online. Understanding the MDH marketplace in the host country – i.e., which actors may be sponsoring, producing or amplifying manipulated narratives and how they do so is important to understanding the motivations and incentives behind MDH.

16.6. Regional context. MDH narratives may relate to cross-border matters, and/or may be spread by actors attempting to drum up regional support for a particular cause. Applying a regional lens to analysis of MDH and making connections with other peace operations or United Nations entities at a regional level will help to understand the scope and extent of MDH.

17. **Map the information environment.** Any action to respond to MDH must be grounded in an understanding of how key actors and the population communicate. A baseline assessment should be conducted defining the following:
    - Television and radio coverage, including the nature of the TV or radio (international, national, community-level); ownership; the number of outlets; languages; geographical coverage
    - Internet penetration, including geographical coverage; number of hosts, etc.
    - Social media usage, including demographics; gender profile; geographical coverage.
    - Print media, including number; distribution; editorial stance; language; ownership; etc
    - Other formal or informal vectors of communication and influence, such as religious or interest-based networks and culture-specific modes of communication, and the actors that use them.

18. **Consider the harm and threat level**. MDH can be associated with six typologies of harm that can be experienced by individuals or organisations, per the list below.[25] Not all of these harms are best addressed by peacekeeping operations. The Rabat threshold test may be applied to determine whether specific speech incites discrimination, hostility or violence, which is prohibited and should thus be referred to the human rights component, where they are present. The six parameters of the Rabat threshold are: social and political context; speaker's status; intent to incite the audience against a target group; content and form of the speech; extent of its dissemination; and the likelihood and imminence of harm.[26]

    Typology of harms

    i. Physical harms: death; injury; sexual violence; starvation; displacement; identity-based violence up to and including genocide and crimes against humanity.
    ii. Economic/financial harms: loss of financial resources; loss of property; lack of access to services.
    iii. Societal/political harms: epistemic insecurity/erosion of trust in truth, evidence and evaluative standards; chilling effect on freedom of expression; spread of fear; withdrawal of consent for the mission.
    iv. Emotional/psychological harms: anxiety; powerlessness; fear of retaliation; depression; sleeplessness.

---

[25] Adapted from ICRC-Stanford Humanitarian Program study on "MDH and civilian harm", presented on 13 Nov 2023 in Geneva.

[26] The Rabat threshold test is available online in 32 languages at https://www.ohchr.org/en/freedom-of-expression. For more information on the tests against this threshold, see OHCHR, "Incitement to Hatred" https://www.ohchr.org/sites/default/files/Rabat_threshold_test.pdf

v. Social/cultural harms: reputational harm; social ostracization; stigmatisation; discrimination.
vi. Operational harms: reputational; curtailment of freedom of movement; restriction of programmatic/mandate implementation actions.

Based on the above, missions should evaluate the likelihood of the MDH threat leading to any of the above harms, and whether it is within the peacekeeping mandate to act. Within the limits of the mission's mandate, including the protection of civilians mandate, priority should be given to actions that mitigate and respond to the worst harms, starting with those that pose an imminent threat to the person. When the assessed harm falls outside the peacekeeping mandate, relevant United Nations system entities or external partners should be engaged.

19. **Ensure preparedness for prevention.** Assessing when to act, and what to act on, should be informed by the above analyses. Below are some considerations on preparedness.

19.1. Capacity and resources. Missions shall identify existing or new capacity to perform the functions for information integrity and MDH described in the Policy, particularly in Strategic Communications, JOC, JMAC, Human Rights, Political Affairs, Civil Affairs, the Office of the Chief of Staff and uniformed components. Capacities required may include human resources, technical guidance and training, specialized digital hardware and software, and special permissions or exemptions from digital resource use policies.

19.2. Internal capacity-building and resilience. Missions shall conduct induction training on information integrity and MDH, including on the specific threat profile in the mission area, and the mission's mechanism to manage threats. Technical training for personnel directly involved in monitoring, analysis and responses shall be conducted on a periodic basis. As part of the processes of analysing the information landscape, missions should assess the mission's limitations and vulnerabilities, identify resources and/or capacity needs to reach populations and/or areas and subjects on which the mission may struggle to promote timely and well-coordinated messaging.

19.3. MDH and safety and security of UN personnel. Risks of harm to United Nations personnel associated with MDH may manifest through hate speech, including incitement to violence against individual United Nations personnel; cyberbullying; threats to dox or actual doxing.[27] Instances of threats should be reported to UNDSS. MDH may also result in threats directed against specific types of personnel (e.g. international or national staff) and specific uniformed units or national contingents. The Designated Official, through the Principal Security Adviser, Chief Security Adviser or Security Adviser, must assess the risk to the safety and security of the UN personnel and take appropriate actions to manage that risk when a threat has been identified, in line with the UN Security Management System. Where threats are directed at uniformed personnel, the seniormost military or police officer is responsible to safeguard their safety and security.

19.4. Prevention. No matter what the MDH threat level may be, preparedness means taking a posture that proactively identifies and prevents negative impacts of MDH as part of strategic, operational and tactical planning processes (see separate guidelines on mitigating and anticipating MDH). Examples of prevention measures include awareness of MDH threats, proactive communications and community

[27] "Doxing" refers to situations in which personal information such as names, addresses, employment information, pictures, family members and other sensitive information are posted online.

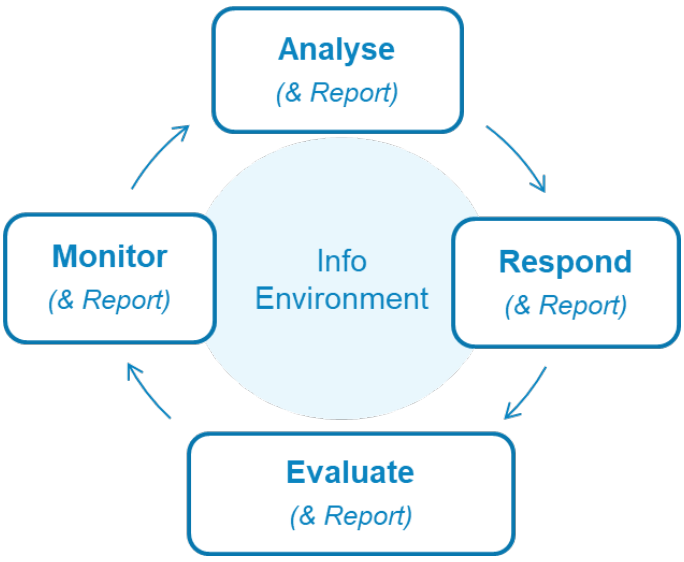
engagement. It should be noted, however, that a prevention-oriented posture must be grounded in human rights and should not support undue restrictions on speech.

19.5. Support to information integrity. A preventive approach includes measures to address the underlying structural or societal factors that allow MDH to thrive, including support to increased access to accurate and reliable information and media and digital literacy, and promotion of the civic space. This in turn requires deliberate action to plan and implement long-term programmatic activities, together with or in support of partners in civil society, state institutions, or United Nations partners.

20. **Partnerships.** MDH is made possible by a combination of technological, sociocultural, political and economic factors that are beyond the span of control of any individual peace operation, or indeed of peace and security actors. In peacekeeping settings, the focus must be on mitigating the real-world harms created by MDH on both the mission and on vulnerable groups in the host country, within the parameters of each operation's mandate, operational capacities and resources. Partnerships should be sought with key actors – other United Nations entities, technology platforms, regional organizations and Member States, among others – to address broader issues which lie beyond the mandate and capacity of peacekeeping missions. At the country level, programmatic funding and Quick Impact Project funds should be considered to build local capacity and resilience; information integrity and MDH analyses and programming should be included in CCAs and United Nations Cooperation Frameworks; and collaboration and coordination with the in- country UN Communications Group on information integrity and MDH should be established. These actions are in line with the Global Principles on Information Integrity.

C3. The monitoring, analysis, response and evaluation cycle

21. This section describes the monitoring, analysis, response and evaluation cycle. Reporting cuts across all four actions . The monitoring, analysis and reporting described applies the "ABC" Framework – focusing on Actors, Behaviour and Content related to MDH.[28]



22. The MDH monitoring, analysis, response and evaluation cycle covers the entire information environment, proactively identifying instances of MDH that may pose a threat to the mission or mandate. As described in the DPO Policy on Peacekeeping Intelligence, the peacekeeping-intelligence cycle provides for directed information gathering analysis on specific questions and using specific information gathering and analysis capacities tasked by the Mission Intelligence Coordination Mechanism (MICM). As part of the MDH cycle, the MICM may be requested to provide insight into a specific issue or phenomena, which can then feed into the MDH response planning process.

[28] Adapted from Camille François, "Actors, Behaviors, Content: A Disinformation ABC", Transatlantic Working Group on Content Moderation Online and Freedom of Expression, September 2019. Note that D – degree - and E – effect – is also examined by some.

C3.1 Monitoring

23. Monitoring of the information environment, both online and offline, must complement monitoring of the physical and human terrain. This is critical for immediate-term situational awareness and can contribute to deeper analysis into trends and dynamics in the information environment.

24. **Online monitoring** shall be conducted regularly – preferably daily - targeting the main media outlets and actors in the information ecosystem identified through the baseline mapping and based on tailored search criteria. (See para 17). Existing real-world or **offline monitoring** mechanisms in peacekeeping, used for early warning, conflict prevention and human rights/protection, shall also gather information on MDH (including community alert networks, monitoring conducted by human rights, child and women protection officers/advisors and by Community Liaison Assistants). Guidance on Force and Police components' patrolling and community-oriented policing should include information- gathering on MDH. Relevant MDH information should be reported through daily field office and line component reporting. Information on emergent or persistent narratives that involve harmful allegations targeting individuals, communities, groups, organizations or values shall be monitored. The source of the MDH narrative should be identified, where possible, and the origins and motivations behind the MDH narrative investigated.

C3.2 Analysis

25. A combination of quantitative and qualitative analytical approaches should be applied to connect online behaviour and real-world political and security dynamics, in order to inform mitigation, defensive or responsive actions. Analysis of patterns in online behaviour are important because they can reveal markers of inauthenticity, which in turn signal information manipulation and an intent to do harm. In isolation, a narrative alone may not cause significant harm, but when it is propagated and amplified using inauthentic means, the narrative may be weaponised. Through analysis, misinformation may be distinguished from disinformation.

26. Regular monitoring and data analysis can help to identify **actors** involved in the creation and dissemination of MDH content, which can be contrasted with political and security actor analyses to enrich the analytical depth garnered through online data, which may support identification of state, non-state actors at the local, national or international level that may be involved in creating, generating or sponsoring MDH. Online **behaviour** that is consistent with information manipulation tactics, techniques and procedures may be identified through data analyses.[29] The narrative **content** should also be analysed and understood to decipher the intent behind MDH. Narratives may be seeded by information manipulators to prepare the ground for real-world policy decisions, or shape operational developments. As such, it is important not only to examine the preponderant narratives, but also those that may be emergent, which may provide an early warning for a campaign to come. Lies may be blended with kernels of truth; when messaging makes use of factual reporting to promote adjustments in the narrative space, they are less likely to be dismissed out of hand.

27. In-depth MDH analysis, including network analyses, analysis of link-sharing behaviour, and consolidated online/offline actor, behaviour and content analysis shall be conducted by the appropriate entity member(s) of the Information Integrity/MDH mechanism. The Head of Mission, or the Chief of Staff on their behalf shall designate the relevant civilians

---

[29] A comprehensive and frequently updated glossary of common disinformation TTPs can be found in the DISARM Framework: https://www.disarm.foundation/framework

and/or uniformed components of the mechanism to conduct the analysis, which could include JMACs, and other peacekeeping-intelligence actors, with the support, as appropriate, of other mission entities, including strategic communications actors, and regional and/or headquarters based backstopping offices, as appropriate.

C3.3 Response

28. A range of responses should be considered and selected based on the diagnosis from the ABC analytical framework. Missions should not rely on any single response category outlined below; a combination of responses should be implemented for greater effect, within the parameters of the mission's mandate.[30]

    28.1. Strategic Communications. Effective strategic communications in line with the mission's strategy is a critical part of the prevention and response to MDH. An effective strategic communications approach to MDH should start with, and be built on, an understanding of the key MDH actors and their narratives and techniques. A proactive communications approach through multi-channel advocacy, as part of the mission's overall communications strategy, is a key measure to mitigate risks. This entails communications across a range of platforms based on audience analysis, including traditional media, in-person outreach, radio and digital media and supported by robust community engagement. Key audiences should be targeted using compelling narratives in relevant languages, voiced as possible by native speakers, with a focus on people-centered and data-driven storytelling to demonstrate tangible impact of the mission's work and value, manage expectations and build support. Proactive communications ahead of identified events, incidents or processes that may be vulnerable to MDH is an effective method of "inoculating" against harmful information, also known as "pre-bunking". Timely, accurate and impartial communications during a crisis can reduce emotional responses and engagement with MDH – these communications may aim to calm, reassure, inform or alert that more information is coming. Care should be taken to ensure that communications are on the channels used by the target audience, including social media networks where MDH may be circulating. Proxy communicators, including social media influencers, faith-based or community leaders or other informal figures of authority, may also be asked to disavow or counter MDH messages, including through "non branded messaging" as appropriate.

    28.2. Political outreach and commitments. Monitoring and analysis of MDH may suggest that key national and/or regional and international actors, state and/or non-state, may be sponsoring, actively contributing or turning a blind eye to MDH narratives. In such cases, political outreach, engagement and advocacy by mission or other UN entities with key actors to highlight the harms created and request actions to signal or to stop MDH may be warranted. Where missions may be facilitating or mediating conflict resolution processes, consideration should be given to including commitments to refrain from inflammatory messaging on social media. Similarly, ahead of and during elections, which are typically high-risk MDH periods, consideration could be given to supporting political actors in developing social media codes of conduct or declarations of commitments against information harms. The period surrounding mission mandate renewals, transition processes and reconfigurations are often used by malicious actors as key moments for the proliferation of MDH (see the 2024 DPO Guidelines Actions to Anticipate and Mitigate

[30] A full suite of response to online disinformation are captured in the DISARM Blue Framework: https://disarmframework.herokuapp.com

Mis/Disinformation and Hate Speech Risks Targeting UN Peacekeeping Operations for a detailed description of events around which risks of MDH may be highest).

28.3. Community engagement. MDH influences the beliefs and worldviews of the population; host communities are thus often the target of MDH. Community engagement serves several objectives: to strengthen trust and acceptance of the United Nations presence; to understand the fears, grievances, priorities and perceptions of peacekeeping interlocutors; to disseminate accurate, reliable and gender- and age-responsive information; early warning and management of narratives that may fuel violence against civilians; and to use credible local voices to build resilience against information harms. Engagement should be conducted by Force, Police and civilian components at the sector and mission HQ levels. Quick Impact Projects and programmatically funded initiatives can be designed to strengthen information integrity within communities, including by establishing new tools to disseminate reliable and accurate information and improve media literacy within and among communities.[31]

28.4. Protection of journalists, human rights defenders and media workers. National authorities should be supported in fulfilling their international human rights obligations on the safety of journalists and media workers (and others exercising their freedom of expression in the public interest, such as bloggers, human rights defenders, youth activists, women's rights advocates, and political activists). Missions should also provide individual protection to these actors where appropriate, in line with mandates and guidance on the protection of civilians and the promotion and protection of human rights.

28.5. Public reporting. Without a counter-narrative setting the record straight, disinformation narratives portraying falsehoods can malinger, blend into reality and become an enduring problem that influences and shapes future perceptions. It is imperative therefore to shed light on MDH, by documenting, informing of and debunking false narratives without amplifying the harms. This should be done in an ongoing manner through reporting to the Security Council, multi-channel strategic communications campaigns targeting host communities and other stakeholders, as appropriate, as well as on an ad hoc basis through the Information Integrity Unit and Strategic Communications Section of DPO. Partnerships with local or regional fact-checking organisations may also be sought.

28.6. Accountability for incitement to hostility, discrimination or violence. Where instances of MDH reach the threshold of incitement under the Rabat Plan of Action or incitement to genocide, missions should advocate for impartial, prompt and thorough investigations, and actions to bring perpetrators to justice. Where appropriate, missions should build capacity of rule of law institutions in this regard.

28.7. Reporting to technology platforms. Harmful content that violates social media and other technology platforms' "community standards" should be reported as a matter of course (see para 40 below). Suspected coordinated inauthentic behaviour identified by Mission or DPO data analyses should be reported to technology platforms for further examination and potential action.

---

[31] See various DPO guidance documents covering community engagement, including Guidelines on Engagement with Civil Society, Manual on Community-Oriented Policing; Practice Note on Community Engagement; Policy on Quick Impact Projects.

28.8. Supporting long-term societal resilience against information harms, thus mitigating their negative impact. MDH is less likely to thrive in a strong civic space in which communities and individuals feel safe in expressing their views freely, have access to a diversity of accurate and reliable sources of information and can identify manipulated or false information disseminated with an intent to do harm. Actions in support of information integrity include media capacity-building, media and data literacy for children and adults, strengthening the capacity of public institutions to promote the creation and dissemination of accurate information transparently, and encouraging a culture of truth and accountability through the empowerment of fact-checking institutions and organizations.

C3.4 Reporting

29. Daily online monitoring shall be conducted by the Strategic Communications component, in coordination with the Human Rights component, JOC, JMAC and others as appropriate. A summary of relevant MDH aspect will be submitted to the JOC for integration into regular reporting purposes. Any content that rises to the level of prohibited speech (see para 9); threatens United Nations personnel; poses a threat of violence against civilians or the protection of human rights; or impacts other mandated tasks of the mission, shall be flagged for action to Human Rights, PoC and DSS, as appropriate, and for awareness to the HoM, FC, PC, and other mission personnel as appropriate.

30. Military, Police, Political, Civil Affairs, Human Rights and other substantive components at the HQ and field office/sector levels, as relevant, shall integrate information on MDH in their reporting chain.

31. The JOC shall include consolidated on- and offline information on MDH in regular situational reports, periodic or early warning reports, ad hoc alerts and in regular situational awareness presentations to senior management, as well as in regular reporting to Headquarters.

32. Standardised and mission-specific MDH indicators will be developed by DPO, in consultation with missions, and incorporated in relevant reporting databases, particularly the Mission's Unite Aware Sage ("SAGE") incidents/events database.

33. Reporting on responses shall be integrated into periodic reporting prepared by the JOC, and separate stand-alone reporting assessing the impact of response actions may be prepared. These reports shall be shared with the relevant civilian components of the mission, notably Strategic Communications and JMAC, to be integrated into overall mission analysis. Ongoing impact assessment shall be reported through the Comprehensive Planning and Performance Assessment system (CPAS). JMAC shall include MDH reporting from civilian and uniformed components in its regular integrated analysis reports, as well as periodic specialized reporting, as appropriate.

C3.5 Evaluation

34. Impact evaluation shall be conducted in an ongoing manner to track progress and inform decisions and shall take at least two forms: 1) Tracking key performance **indicators** (KPIs) related to information integrity strategic objectives or goals. These KPIs may be included in the CPAS and should provide evidence of progress towards objectives/goals. Through CPAS, the linkage between information integrity and performance on other mandate areas, such as the protection of civilians, should also be made. 2) Tracking of operational **metrics** related to day-to-day operations, which provide insights into how campaigns and activities are performing, including in relation to other actors or narratives. "Vanity metrics," and machine-generated sentiment analysis should generally be avoided, as they can lead

to misleading or erroneous assessments. Below are examples of approaches that can be used.

- Track social media engagement. The impact of online campaigns may be evaluated by examining various variables, including: i) tracking engagement through shares, likes, views and mentions of content supported by the mission, ii) whether the content has crossed organically between platforms, iii) whether the content has been posted across identity groups (ethnic, ideological, geographical, etc.), iv) whether the content is cross-pollinating between offline and online environments, v) setting the performance of United Nations or UN-supported narratives against MDH narratives online.

- Track online engagement. These can include the social share of voice (how much people are talking about the issue), the bounce rate (percentage of people who visit one page and leave without clicking further), and search engine ranking.

- Perception surveys. Within resource limitations, Missions should commission regular independent perception surveys involving a diverse array of participants to, among other objectives, monitor the attitudes, knowledge and perceptions in the real world. Given that a significant volume of content in the online information environment is inauthentic and manipulated, sentiment online should not be understood as a reflection of organic, bona fide views.

- Proxies for consent. Disinformation targeting United Nations missions has the effect of de-legitimising and disrupting mandate delivery, with the potential to contribute towards the withdrawal of official and/or popular consent of the operation. Trends in violations of the Status of Forces Agreement (SOFA), such as restrictions on freedom of movement maybe considered proxies for consent.

C4. Managing work on information integrity and MDH

35. **Mission level.** Within each mission, an integrated Information Integrity mechanism (working group, task force or similar) shall be established to coordinate the monitoring-analysis-response-evaluation cycle. This Information Integrity mechanism shall be comprised of relevant uniformed and civilian components, including but not limited to Strategic Communications, JOC, JMAC, Mission Planning Unit, U/S/G2, Info Operations Units, Political and Civil Affairs, Gender, Human Rights, FTS, PoC, UNDSS/SIOC and the Office of the DSRSG/RC/HC. The mechanism shall be convened by the Chief of Staff of the mission or substantive sections with delegated authority.

36. The Information Integrity/MDH mechanism shall have the following core tasks: agree on preventive and responsive actions to be implemented by the mission; develop an integrated mission-wide strategy to strengthen information integrity and address MDH, which shall be consulted and coordinated with the UNCT; ensure the preparation of timely analyses and reporting; provide regular updates on the MDH landscape to senior leadership and flag issues of concern through senior management meetings; propose responses to mission leadership; and coordinate their implementation. A reduced number of staff from key components may coordinate action during rapidly evolving disinformation crises. Depending on the severity of the MDH challenge in the mission area, the integrated mechanism shall determine whether an Information Integrity Advisor/Officer position is required to achieve the core tasks of the mechanism.

37. When the Crisis Management Policy is activated and the mission is included in a Communications Group Crisis Cell convened by the Department of Global

Communications, the Information Integrity/MDH mechanism shall share information and analysis and coordinate with the Cell on the development of responses to MDH.

38. Where MDH poses risks to safety and security and/or the protection of civilians, MDH-related issues shall be included in missions' Peacekeeping-Intelligence Requirements management process by the Mission Intelligence Coordination Mechanism, thus triggering the acquisition and analysis of information related to MDH by mission peacekeeping- intelligence entities. Periodic integrated analyses of the on- and offline MDH threat landscape shall be prepared, with inputs and contributions from civilian and uniformed components.

39. Each member component shall designate a focal point and an alternate to contribute to the work of the integrated mechanism. The focal point's contributions shall be reflected in their respective workplans, and they shall be held accountable for their contributions through performance evaluations. Where the severity of the MDH challenge warrants it, Missions shall create an Information Integrity Advisor position in the Office of the Chief of Staff, Head of Mission or in an office designated by the HoM, who shall be tasked with the coordination of mission-wide work in this area.

40. **DPO Headquarters.** The Information Integrity Unit at UNHQ shall provide, in coordination with the Strategic Communications Section and other UN entities as appropriate, substantive and technical guidance and support to missions on matters related to information integrity and MDH and liaise with the Department of Global Communications and other United Nations and external counterparts on matters related to information integrity and MDH. The Unit may assist missions in conducting monitoring and analysis on a case-by-case basis and shall conduct trend analyses of MDH in peacekeeping environments. As part of regular reporting processes, missions shall share monitoring and analysis products with the Information Integrity Unit at UNHQ via code cable. The Strategic Communications Section shall continue to provide, in consultation with the Information Integrity Unit, substantive and technical guidance and support to missions on the strategic communications aspects of information integrity and responses to MDH. The Office of the Special Adviser of the Secretary General on the Prevention of Genocide shall act as focal point on hate speech provide technical assistance support to missions in developing action plans for addressing hate speech, as appropriate.

41. **Working with social media platforms.** As the policies, tools and procedures used by social media platforms to respond to MDH evolve, missions should remain familiar with the procedures for flagging content that violates community standards on each social media platform. Missions should, as needed, reach out to relevant platforms to flag content that violates community standards. Missions should maintain records of these contents and of their interactions with platforms and inform Headquarters (including SCS and the Information Integrity Unit) when content is flagged.

D. ROLES AND RESPONSIBILITIES

42. Missions have varying mandates, structures and compositions. All the roles and responsibilities described below do not necessarily exist in all missions. These responsibilities apply where the roles exist.

43. **Head of Mission.** The Head of Mission (HoM) is responsible for providing strategic direction to the Mission on all matters related to information integrity and addressing MDH in their area of responsibility. In integrated missions, the HoM is responsible for strategic

and programmatic coherence across the United Nations system's engagement on information integrity. They shall guide and create an enabling environment for timely and consistent actions across the monitoring, analysis, reporting, response and evaluation cycle, including by designating the requisite resources for this purpose. The HoM shall, where appropriate, engage in advocacy, political outreach and proactive and responsive communication initiative to address MDH. The HoM is ultimately accountable for the mission's efforts in strengthening information integrity and addressing MDH in line within this Policy. Depending on the size and capacity of the mission, the coordination of an integrated information integrity mechanism may be located in the HoM's office.

44. **Force Commander (FC).** The FC shall integrate preventive, anticipatory and responsive measures into operational plans for the military component to fulfil responsibilities to monitor and address MDH, and issue directives or other instructions specific to information integrity and MDH, as necessary, in line with this policy and the mission's plans for addressing MDH, and in coordination with civilian and police components. With support from the senior Military Public Information Officer, they will ensure coherence and coordination within the Force to enable timely analysis and responses to MDH, including between U2, Information Operations Units, Open-Source Peacekeeping-Intelligence Units, Mission Community Outreach Units, and the Sector-level, as relevant. The FC shall designate a focal point to contribute to the Information Integrity mechanism. They shall ensure that Sector, battalion, company, and unit commanders comply with orders, directives, and guidance to effectively implement this policy and ensure that all personnel under their command have a common understanding of the mission approach to information integrity and MDH, including through specific in-mission training, and that they are operationally ready, able and willing to perform their responsibilities and to identify and seek to address any gaps in capacity, training and resources.

45. **Police Commissioner (PC).** The PC shall integrate preventive, anticipatory, and responsive measures into operational plans for the police component to fulfil responsibilities to monitor and address MDH, and issue directives or other instructions specific to information integrity and MDH, as necessary, in line with this policy and the mission's plans for addressing MDH, and in coordination with civilian and military components. They shall designate a focal point to contribute to the Information Integrity mechanism. The PC will ensure that field office-based/sector and subsidiary personnel comply with orders, directives, and guidance to effectively implement this policy. They will ensure that all personnel under their command have a common understanding of the mission approach to information integrity and MDH, including through specific in-mission training, and that they are operationally ready, able and willing to perform their responsibilities and to identify and seek to address any gaps in capacity, training and resources.

46. **Chief of Staff.** Where designated by the Head of Mission, the Chief of Staff shall convene the Information Integrity/MDH mechanism (Working Group, Task Force or similar), and ensure that relevant components of the mission participate actively (see para 35 for list of relevant components). The Chief of Staff or delegated officer shall ensure that monitoring and analysis of the information environment is conducted on a regular basis and issues of concern as well as suggested actions are brought to the attention of mission leadership for decision-making purposes. The Chief of Staff shall oversee the implementation of integrated response to MDH and liaise with Mission Support as needed for timely support to information integrity-related activities.

47. **Head of Strategic Communications**. The head of Strategic Communications is responsible for developing and implementing a mission-wide communications strategy aligned with objectives in the Information Integrity strategy or action plan. They are

responsible for contributing to integrated monitoring, analysis, reporting and responses, with a particular focus on online and offline media monitoring, community outreach, communications campaigns and activities. The head of Strategic Communications shall ensure that all strategic communications personnel have a common and up-to-date understanding of the mission's strategic approach to information integrity and MDH. They shall designate a staff member and alternate to act as focal point on Information Integrity and MDH, whom shall be responsible for coordinating information integrity and MDH work within the Strategic Communications component and contribute to the work of the Information Integrity mechanism. The focal point role shall be reflected in the staff member's workplan.

48. **Information Integrity Adviser.** Where the role exists, the Information Integrity Adviser shall serve as the secretary to the Information Integrity/MDH mechanism and ensure delivery of monitoring, analysis, response and evaluation objectives. They shall serve as focal point in the mission for matters related to information integrity and MDH and shall prepare integrated mission guidance and strategies to address MDH. The Information Integrity Adviser shall be located in an office with overarching authority over mission components, such as the Office of the Chief of Staff, Head of Mission, or another location as designated by the HoM.

49. **Heads of JOC, JMAC, Political Affairs, Civil Affairs and Human Rights offices**. Where deployed, each of these office Heads shall designate a staff member and alternate to act as focal point on Information Integrity and MDH who shall be responsible for coordinating information integrity and MDH work within their component and contribute to the work of the Information Integrity mechanism. The focal point role shall be reflected in the staff member's workplan. Managers overseeing personnel involved in the monitoring and analysis of the information environment shall be responsible for monitoring and managing risks to the mental health of these personnel in so far as these may impact the health and wellbeing of these personnel as well as their analytical outputs (see the 2024 SOP on Operational Security in Monitoring and Analysis of the Digital Information Environment for further guidance on this responsibility). In addition, the following specific roles and responsibilities apply:

    49.1. Head of JOC. Designate capacity to integrate information and analysis on MDH into information management and reporting products and include these are shared with the appropriate offices in the mission and at Headquarters.

    49.2. Head of JMAC. Designate capacity to conduct in-depth analyses of the information environment, including tracking key actors, behaviors and content in coordination with the Strategic Communications section and other relevant sections, and oversee integration of these analyses with other analytical products and perspectives.

    49.3. Head of Civil Affairs. The Head of Civil Affairs shall ensure that his/her component gathers information and report on information integrity and MDH, including through the Community Liaison Assistants (CLAs) in Mission where these are deployed and operate under Civil Affairs, as part of their efforts to understand the population's perceptions of the peace process and to build trust between parties to the conflict at the local level. In line with Civil Affairs offices' roles in the development of political space, community protection and conflict resolution, they should engage with local community stakeholders in dialogue on MDH as part of efforts to deescalate

inter-group tensions, seeking to facilitate commitments from parties to not engage in the spread of MDH.[32]

49.4. Head of Political Affairs. Provide political advice and guidance on the mission-level information integrity strategy or action plan, including on outreach, engagement and messaging.

49.5. Head of Human Rights. Contribute to monitoring and analyses in the context of the information integrity mechanism. Advise on the protection of threatened journalists and media workers; act as focal point on hate speech.

49.6. Gender Adviser. Advise on gendered concerns regarding MDH and contribute to information integrity strategy or action plan.

49.7. Quick Impact Project and Programmatic Funding Managers. Ensure that projects aimed at strengthening information integrity and contributing to situational awareness are considered for QIPS and programmatic funding.

50. **Heads of Field Offices.** With delegated authority from the Head of Mission, Heads of Field Offices shall coordinate the information integrity cycle (monitoring, analysis, reporting, responses, evaluation) for their area of responsibility, including chairing field-level information integrity working groups or task forces that include all mission components.

51. **Head of Field Technology Section (FTS).** The Head of FTS is responsible for enabling relevant mission personnel to undertake monitoring and analysis of the digital information environment by furnishing technical capacities and support to colleagues as necessary. This may in some cases include specialized hardware, software and permissions.

52. **DPO Information Integrity Unit.** Part of the DPO Division of Policy, Evaluation and Training, the Unit shall lead the development of policy and guidance on addressing MDH in peacekeeping missions. It should monitor global and mission-specific trends in MDH threats and responses, and document and share good practices. It shall serve as the DPO focal point for UN-wide efforts on information integrity and to address MDH.

53. **DPO Strategic Communications Section.** The Section provides peacekeeping operations with policy and guidance on strategic communications and public information, including on strategic communications strategies and tools for addressing MDH. The Section leads Department-wide communications responses to MDH that require action outside of the mission area.

54. **DPO Office of Military Affairs (OMA) and OROLSI/Police Division (PD).** OMA and PD shall ensure that relevant guidance training, capabilities, skill profiles for uniformed personnel reflects action against MDH, and integrate information integrity and MDH considerations into planning.

E. TERMS AND DEFINITIONS

55. For the purposes of this policy, the following United Nations working definitions apply:

Misinformation: Inaccurate information that is unintentionally shared in good faith by those

[32] See DPO-DOS Civil Affairs Handbook, 2012, Chapter 10.1

unaware that they are passing on falsehoods.[33]

Disinformation: Information that is inaccurate, intended to deceive and shared in order to do serious harm.[34]

Hate speech: 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. According to this definition, hate speech can only be directed at individuals or groups of individuals. It does not include communication about States and their offices, symbols or public officials, nor about religious leaders or tenets of faith.[35]

Information integrity: Information integrity refers to an information ecosystem in which freedom of expression is fully enjoyed and information that is accurate, reliable, free from discrimination and hate is available to all in an open, inclusive, safe and security information environment. Promoting information integrity involves empowering people to exercise their right to seek, receive and impart information and ideas of all kinds and hold opinions without interference. The erosion of the integrity of information through misinformation, disinformation, or hate speech can undermine people's ability to exercise their human rights and hamper efforts to achieve peace, prosperity and a livable future.[36]

Technology-facilitated gender-based violence: A spectrum of activities and behaviors, including both online gender-based violence and gendered disinformation present in online communities.

Information environment: An environment that includes information and the individuals, organizations and systems that receive, process and share information, and the cognitive, online and physical space in which this takes place.

Inauthentic behaviour: Online activity in which a user misrepresents themselves, uses fake accounts, or engages in malicious and/or coordinated activity intended to harm others, mislead others about the origin or control of accounts and/or content, artificially enhance the exposure of accounts and/or content.

Digital and social media: Websites and other platforms such as X, Facebook, YouTube, TikTok, Instagram, Flickr, LinkedIn, Medium and others.

F. REFERENCES

Normative or Superior References

- Security Council Resolutions on United Nations Peacekeeping Missions: 2640 (2022), 2650 (2022), 2659 (2022), 2695 (2023), 2709 (2023), and 2717 (2023)

---

[33] United Nations. June 2023. Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms, p.5 https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf

[34] Report of the Secretary General. December 2021. Countering disinformation for the promotion and protection of human rights and fundamental freedoms. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/416/87/PDF/N2141687.pdf

[35] United Nations. What is Hate Speech? https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech

[36] United Nations Global Principles for Information Integrity, June 2024, https://www.un.org/en/information-integrity

- Security Council Resolution on thematic issues: tolerance and international peace and security: 2686 (2023); the protection of humanitarian personnel and UN and associated personnel and their premises and assets 2730 (2024)
- General Assembly resolution on Cross-cutting issues (A/RES/76/274)
- General Assembly reports of the Special Committee on Peacekeeping Operations (A/77/19; A/78/19) and of the Committee on Information (A/77/21)
- International Covenant on Civil and Political Rights (A/2200A (XXI))
- Secretary-General Bulletin: Observance by United Nations forces of international humanitarian law (ST/SGB/1999/13)
- Secretary-General Bulletin: Data protection and privacy policy for the Secretariat of the United Nations (ST/SGB/2024/3)

Related policies, procedures or guidelines

- DPO-DPPA-OHCHR Policy on Human Rights in United Nations Peace Operations and Political Missions, 2011.20
- DPO Policy on Peacekeeping Intelligence, 2019.08
- DGC-DPO-DPPA Policy on Strategic Communications in Peace Operations, 2024.04
- DPO Policy on Joint Mission Analysis Centres, 2020.06
- DPO Policy on Joint Operations Centres, 2020.6
- DPO Policy on Integrated Reporting from Peacekeeping Operations to UNHQ, 2019.10
- DPO Policy on Community Liaison Assistants, 2024.03
- DPO-DOS Policy on Quick Impact Projects, 2012.21
- DPO Policy on the Protection of Civilians in United Nations Peacekeeping, 2023.05
- UN System-Wide Crisis Management Policy, 2023
- Secretary-General's Bulletin on the Institutional Use of Social Media (ST/SG/2019/5)
- United Nations Strategy and Plan of Action on Hate Speech, 2019.05
- United Nations Secretariat Guidelines for the Personal Use of Social Media, 2019.02
- DPKO-DFS Guidelines Engagement with Civil Society, 2017.06
- DPO Guidelines on Open-Source Peacekeeping-Intelligence, 2022.03
- DPO-DOS Civil Affairs Handbook, 2012.02
- DPO-DFS Manual Community-Oriented Policing in United Nations Peace Operations, 2018.04
- DPO-DFS Practice Note on Community Engagement, 2018.03
- UN Global Principles on Information Integrity, 2024.06
- United Nations Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms, 2023.06

Other related references

- Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Disinformation and Freedom of Opinion and Expression during Armed Conflicts: A/77/288 (2022)
- Report of the Secretary General on Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms: A/77/287 (2022)

G. MONITORING AND COMPLIANCE

Within missions, the Head of Mission is responsible for the mission's compliance with this policy. At Headquarters, the Information Integrity Unit within the Policy and Best Practices Service (PBPS), a branch of the Division of Policy, Evaluation and Training (DPET) of DPO

will monitor compliance, in collaboration with the Strategic Communications Section of the Office for Shared Services of DPPA/DPO.

H. CONTACT

Questions or comments should be directed to the Information Integrity Unit within the Policy and Best Practices Service, a branch of the Division of Policy, Evaluation and Training (dpo-info-integrity@un.org).

APPROVAL SIGNATURE:

DATE OF APPROVAL:

12 December 2024