United Nations
Department of Peace Operations
Ref. 2022.03

Guidelines

Open-Source Peacekeeping-Intelligence (OPKI)

Approved by:	Jean-Pierre Lacroix, USG DPO
Effective date:	*1 March 2022*
Contact:	*DPO/OUSG/PICT*
Review date:	*1 March 2026, or as needed*

DPO GUIDELINES
ON OPEN-SOURCE PEACEKEEPING-INTELLIGENCE (OPKI)

Contents:

A. PURPOSE

1. The purpose of these Guidelines is both to provide a framework for and to facilitate the safe and effective acquisition of information from open-sources for peacekeeping-intelligence (hereafter "OPKI"). These Guidelines are part of the Peacekeeping-Intelligence Framework and should be read in conjunction with the DPO Policy on Peacekeeping-Intelligence[1] (hereafter "the Policy"). Neither these guidelines nor the Policy provide any type of training.

B. SCOPE

2. This guidance document shall apply to all serving members of United Nations peacekeeping operations assigned to support acquisition of information from open-sources for peacekeeping-intelligence. Compliance with these Guidelines is mandatory[2].

2.1. The Principles of Peacekeeping-Intelligence are to be strictly complied with. They are as follows:

2.2. **Under rules**: All peacekeeping-intelligence activities will be undertaken in line with the Security Council mandates of peacekeeping operations, in full compliance with the Charter of the United Nations. These activities shall be consistent with the

[1] Policy on Peacekeeping-Intelligence, DPO, 2019
[2] This guidance only applies to data, information and products gathered and managed as part of the peacekeeping-intelligence cycle. Standard information management, reporting and sharing practices that are not related to peacekeeping-intelligence will continue to be conducted in line with existing applicable guidance.

overall legal framework governing United Nations peacekeeping operations, including the basic principles of peacekeeping and all legal and human rights standards and obligations. Peacekeeping-intelligence activities must be conducted with full respect for human rights, including, in particular, the rights to privacy, freedom of expression, peaceful assembly, and association, and with particular care not to expose any sources or potential sources of information to harm.

2.3. **Non-clandestine**: **Clandestine activities, defined as the acquisition of information or intelligence conducted in such a way as to assure secrecy or concealment of the activities, because they are illicit and/or are inconsistent with the legal framework, principles, policies and mandates of United Nations peacekeeping operations, are outside the boundaries of peacekeeping-intelligence and shall not be undertaken by participating mission entities.** Regular training and education, including standardized pre-deployment training for all personnel involved in all aspects of peacekeeping-intelligence, as well as regular audits and oversight of the peacekeeping-intelligence workflow, will reinforce this principle.

2.4. **Areas of application**: The acquisition and management of information or intelligence by United Nations peacekeeping operations will be conducted to enhance situational awareness and the safety and security of UN personnel, and to inform operations and activities related to the protection of civilians tasks of the Security Council mandates.

2.5. **Respect of State sovereignty**: The sovereignty of states, including Host and neighboring States, must be respected.

2.6. **Independence**: The peacekeeping-intelligence activities of peacekeeping operations will be fully autonomous from and independent in all aspects of any national intelligence system or other operations and will maintain their exclusively international character. Missions may liaise with non-mission entities for the purposes of receiving intelligence and may share specific peacekeeping-intelligence with non-mission entities, including Host States, provided they do so under conditions and within the parameters described in this document and related guidance.

2.7. **Accountability, capability and authority**: Those who are given the authority to make decisions with regard to peacekeeping-intelligence activities must have the appropriate capabilities to execute these functions and remain accountable for the effective execution of these responsibilities within their respective chains of command to the Head of Mission and ultimately to the Secretary-General. Within the mission, the Head of Mission is accountable for the functioning of the peacekeeping-intelligence system. She/He is responsible for ensuring compliance with this Policy and associated guidance by personnel engaged with or using peacekeeping-intelligence products, through effective governance procedures, training and practices.

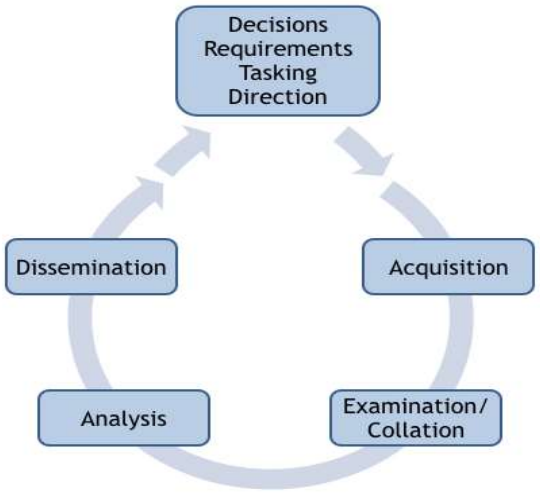
2.8. **Security and confidentiality**: Peacekeeping-intelligence shall be stored and shared in a secure manner, while ensuring access for those who require it for decision-making and operational planning. Based on an assessment of risk, missions will put in place procedural, technological and physical security tools in consultation with DPO and DOS Headquarters to ensure secure information management and communications within the peacekeeping-intelligence system.

Confidential peacekeeping-intelligence products shall be shared and disseminated on the basis of the “need to know” and “need to share” concepts, which require that peacekeeping-intelligence should be disclosed to mission personnel if and only if access to said information is required for them to carry out their official duties. It also requires a written delegation of authority from the originator of the report or staff member who originally applied the classification level. It implies that peacekeeping-intelligence is only disclosed to trusted individuals to ensure that it is not widely disseminated, in particular where disclosure is likely to result in the endangerment of the safety or security of any individual or group, violate rights or invade privacy. In doing so, missions will seek to establish and maintain a high degree of confidence among all of their interlocutors in their ability to appropriately acquire, protect and manage peacekeeping-intelligence.

C. RATIONALE

3. The Policy “sets out why and how United Nations peacekeeping operations acquire, collate, analyze, disseminate, use, protect and manage peacekeeping-intelligence in support of United Nations peacekeeping operations in the field.” The acquisition of information refers to the second step of the peacekeeping-intelligence cycle (Figure 1)

Figure 1. The Peacekeeping-Intelligence Cycle



4. The Policy defines the acquisition step as follows: **“Acquisition refers to the process of obtaining data and information to serve as the basis for analysis. Effective acquisition requires direction and planning to ensure resources are used in such a manner as to most effectively meet the Peacekeeping-Intelligence Requirements (IRs). This includes tasking assets according to IRs, ensuring data and information is reported in a timely manner, tasking assets within their capabilities, and putting in place mechanisms to ensure corroboration and/or verification of information and data as appropriate**.”

5. The Policy also states that “The parameters for the effective, responsible, and ethical acquisition of peacekeeping-intelligence shall be described in the mission’s Peacekeeping-Intelligence Support Plan. In addition to being compliant with this and other United Nations policies and guidance, the latter will describe acceptable and

unacceptable tools, techniques, and procedures of information acquisition by the mission, applicable legal obligations, and considerations that shall be undertaken when acquiring peacekeeping-intelligence, based on the assets available to the mission and in line with operational guidance that is subordinate to this Policy."

6. In UN Peacekeeping, OPKI is the Peacekeeping-Intelligence derived from the acquisition, collation, and analysis of publicly available information (PAI) in response to peacekeeping-intelligence requirements. Publicly available information, in any format, includes any freely available information or material posted on the Internet (including social media), published, broadcasted (radio and television), or provided for public consumption. It may also include information that is commercially available to the public for a fee. When paying for publicly available information, users must ensure compliance with all UN rules and regulations, PKI principles and related guidelines.

7. The acquisition of information from open sources can be generally divided into three categories, based on the direction methods used.

7.1. Undirected, **casual**: Casual, undirected acquisition refers to the gathering of information from open sources, but not in response to specific peacekeeping-intelligence requirements. Examples would include information gained from general horizon scanning, e.g. reading the newspaper or scrolling through trending tags on Twitter. This can be referred to as passive acquisition.

7.2. Directed, but **not clandestine**: This category refers to the same type of acquisition methods as 7.1. but conducted as part of the peacekeeping-intelligence cycle. In other words, information is deliberately discovered and acquired in response to information requirements developed at the Mission level and will be processed according to the peacekeeping-intelligence cycle steps. This acquisition method requires specific search methods to acquire the needed information and may include the need to pay fees for commercially available information (see paragraph 6). This category can be both passive and active acquisition.

7.3. Directed/undirected and **clandestine**: **This method of acquisition is strictly forbidden under the Peacekeeping-Intelligence Policy (see paragraph 2.3) and may bear serious consequences for the staff member (military, police and civilian) and for the United Nations as a whole. This method of acquisition is included here with the sole purpose of indicating what should not be done.** Clandestine OPKI acquisition refers to the acquisition of information in a way designed to conceal the nature of the operation. Activities are undertaken with the intent to assure secrecy and concealment, for example by presenting oneself under a false identity or not being truthful about one's employment with the United Nations in interactions on platforms such as social media, and blog posts, and through commentary to build rapport with online entities.

8. Only the directed variant (paragraph 7.2) that is conducted as part of the peacekeeping-intelligence cycle is considered OPKI. Mission entities other than the core members of the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM)[2], as described in Annex B of the 2019 Policy on Peacekeeping-Intelligence, may also utilize open sources to acquire information, but do so in an undirected, casual manner.

9. When the core entities of the MICM utilize OPKI, they must follow these guidelines.

10. Based on the above parameters the present guidelines have been developed to provide guidance to peacekeeping operations on how to perform OPKI therein.

D. Guidelines

11. General rules and characteristics

11.1. **OPKI constitutes the majority of PKI acquisition and shall be the first acquisition method to be considered for acquisition of the necessary information due to its ease of use, low risk, low costs and fast turnaround. When OPKI is deemed unsuitable or has proven unsuccessful or incomplete, other sources will be considered.** This does not discard the need for other PKI sources in any way. The most reliable PKI products are based on multisource information and OPKI needs to be validated, often by using other acquisition methods.

11.2. All OPKI operations will be carried out strictly to enhance situational awareness and the safety and security of UN personnel, and to inform operations and activities related to the protection of civilians tasks of the Security Council mandates.

11.3. All OPKI operations will be conducted in accordance with the UN Charter, basic peacekeeping principles, international human rights law, international humanitarian law, relevant decisions of the Organization's intergovernmental organs and other applicable legal frameworks.

11.4. OPKI can be used for answering many different types of information requirements within a Peacekeeping Operation (PKO). Some examples:

11.4.1. PKI personnel monitoring the current situation can use live news feeds and social media to monitor evolving crisis situations.
11.4.2. Cultural information concerning perceptions, sentiments, intentions and capabilities of local entities can inform field visits/operations.
11.4.3. Encyclopedic data supports PKI, giving the mission a critical baseline understanding of the complex operating environment.
11.4.4. OPKI can provide data to analyze how local actors are responding to mission activities in certain areas.
11.4.5. In support of Geospatial PKI, OPKI can provide access to enormous quantities of imagery, audio and video that is often geo-located.

11.5. Open-source PKI is an umbrella term for a broad array of potential sources and does not only comprise information from online sources.

11.5.1. Public speaking forums. These are events that are open to the public, where there is no expectation of privacy by either the speaker or the attendee. Examples include political rallies, religious sermons, academic debates, educational lectures, news conferences and exhibitions.

11.5.2. Public documents. These include books, newspapers, leaflets, posters, professional journals, maps, manuals, photographs and public property records. Systematic monitoring can, over time, identify useful trends.

11.5.3. Public broadcasts. These can be observed via internet, radio and television. They are a source of current information of the situation in societies. They include media broadcasts and journalistic commentary and may include propaganda and commercial advertising.

11.5.4. Internet.

11.5.4.1. **The world wide web** is only one of the many services available on the internet. It connects content with a standardized code (HTML) and is searchable using common search engines. It is however an unregulated platform, meaning anyone can upload information. Identifying the origin of a website or an article can be very difficult, but is essential in order to be able to verify the information. OPKI training can provide analysts the tools to evaluate the veracity of sources.

11.5.4.2. The **deep web** is the part of the web that is not accessible through a common search engine but is in HTML. It includes private websites that require registration and/or passwords. Examples include library, email and banking websites. UN PKOs can use the deep web when and where there is a legitimate need and legal access to the content**. Hacking websites is not allowed within the scope of OPKI**.

11.5.4.3. The **dark web** is a part of the deep web that is not accessible by a standard internet browser and is used to keep internet activity anonymous and private. Websites on the dark web end in .onion instead of the more known 'surface web' extensions like .com, .gov, and .org. Using the dark web can be dangerous for both the personnel accessing it and for the Organization, therefore:

11.5.4.3.1. **Any use of the dark web on UN-provided equipment, for the purpose of PKI, shall be authorized by UNHQ first (PICT, OICT)**.

11.5.4.3.2. UN personnel accessing the dark web on their personal equipment do it at their own risk and responsibility.

11.5.4.3.3. Any information acquired on the dark web through personal equipment shall not be used for PKI.

11.5.4.3.4. Monitoring of the dark web for any threat against the United Nations (including for the safety and security of Peacekeepers) is conducted at UNHQ and any relevant information will be communicated to the associated PKO promptly.

11.5.5. Social media is the overall term used for internet platforms where interactions of (mostly) individuals in virtual communities, such as social networking sites and other telecommunication services, take place. They upload blogs, micro-blogs, posts on social networks, on professional networks, join in video sharing (vlogs), audio sharing (podcasts), photo sharing and social bookmarking.

11.5.5.1. Social media is often used to organize demonstrations and quickly spread messages. In doing so, it can significantly influence the dynamics of a society.

11.5.5.2. In addition to individuals, social media is now widely used by political organizations, governments, commercial enterprises and interest groups.

11.5.5.3. In using information from social media it is critical to understand that social media accounts are the ultimate uncontrolled casual source. It is often unclear who exactly is behind an account (are they individuals? bots? trolls? government? Commercial party? others?) and what their goal is in publicizing certain, possibly fabricated, information. Misinformation and disinformation are widespread and sometimes difficult to identify.

11.5.6. Grey literature refers to documents that are unclassified and legally and ethically available but are not controlled by commercial publishers or subscription agencies. They can often be obtained via specialized channels. They can include blueprints, datasets, commercial imagery, working papers, technical reports, university yearbooks, dissertations, etc.

11.6. A major source for OPKI is media. Media comes in many forms, such as newspapers, news websites, television, radio and on social media platforms. It is important to take into account that many news media are involved in a commercial competition to attract audience engagement. They therefore need newsworthy coverage to attract attention and they need to be fast. This will automatically limit the detail and possibly the accuracy of the information. Many journalists are generalists that cover a wide array of topics and their reporting can therefore show limitations in the understanding of specific events and issues, including unrealistic expectations, misinterpretations and a lack of context ("jumping to conclusions"). News media, like social media, can be used to spread misinformation (false or inaccurate information). When misinformation is posted or published with an intent to deceive, this is disinformation.

11.7. Radio is often the primary source for news and information in many rural areas and much of the developing world. Radio monitoring is therefore a worthwhile part of OPKI activities.

11.8. When interacting with online entities, by posting comments or blogs or following social media accounts and sharing content, **OPKI operators are not allowed to use fake accounts and conceal their employment with the UN**. The Mission may allow the establishment and use of organizational social media accounts that reflect the job of the OPKI operator in order to protect the identity of the staff member while showing employment with the UN. This practice should be included in the Mission Peacekeeping-Intelligence Support Plan (MISP) and its use should be limited and monitored.[3]

11.9. **The use of a Virtual Private Network (VPN) on UN equipment, for the purpose of PKI, is subject to prior authorization from UNHQ (PICT, OICT)**. UN personnel using a VPN on their personal equipment do it at their own risk and responsibility, and any information acquired using a VPN through personal equipment shall not be used for PKI.

[3] OPKI operators granted the use of an organizational account should remember that everything they do online will reflect on the UN. Active engagement (like posting of comments, publication of blogs and sharing content) with an organizational account should therefore NOT be done without explicit delegated authority.

11.10. Since the method of acquiring information from public speaking forums mostly consists of direct observation (attendance), due to the overt nature the operator should take precautions. While caution should be observed, using a fabricated identity is not allowed. The safety and security of mission personnel must always be prioritized.

11.11. All OPKI operations will be conducted strictly in support of the Mission Information Acquisition Plan (MIAP) and in accordance with the Mission Peacekeeping-Intelligence Support Plan (MISP).

11.12. **OPKI operators will not engage in running sources online. This is considered online/virtual HPKI and the HPKI guidelines will apply.** Therefore, while interacting online (e.g. with social media users, journalists or other private persons), no amount of money will be paid, nor gifts offered, in remuneration for information.

11.13. Exceptions for payment are **commercially available information** (e.g. journal articles, commercial imagery, analyses, subscriptions) that will likely be considered essential in OPKI operations. A thorough analysis of required sources and information is to be made and regularly updated, and a suitable budget will need to be considered within missions to allow for these expenses.

11.14. Whenever possible, OPKI activities should be carried out by trained open-source PKI personnel, possessing skills and experience to efficiently find the required information in a timely fashion. Wherever possible, the inclusion of OPKI specialists within Mission Components' PKI entities[4] is highly encouraged.

11.15. OPKI is generally less resource-heavy than other PKI acquisition methods. The platforms and hardware are less expensive, and the operations are generally less dangerous for both the operator and the source, compared to, for example, HPKI. Information acquired through OPKI operations is not inherently less valuable than other sources of information just because it was openly available.

11.16. In line with the Policy, the Head of Mission (HoM) or a delegated authority is permitted to share PKI, including OPKI, with non-UN actors. The exchange of PKI, including OPKI, with non-UN security forces must occur in compliance with the Human Rights Due Diligence Policy on UN support to non-UN security forces (HRDDP). **Some information acquired from open sources, that has been processed through the peacekeeping-intelligence cycle, will be classified.** The safety and security of UN personnel, the Mission and the population is paramount, and these considerations must inform any decision-making regarding such sharing.

11.17. Since OPKI reports are derived from publicly available information, they may generally be shared more widely than PKI reports from other acquisition methods. If information was commercially available, distribution might be limited.[5]

---

[4] JMAC, UN Department of Safety and Security (UNDSS), Joint Operations Centre (JOC) (supporting), Force U2, Police Component Crime Intelligence Unit (CIU).

[5] Some commercially available information might be subject to copyright laws and distribution should therefore be limited.

E. Roles and responsibilities

12. Direction

12.1. The head of the Mission Component[6] must ascertain IRs, and will ensure that tasking is in line with his/her entity's capabilities and limitations.

12.2. All OPKI activities will be conducted in support of the Mission and component IAPs.

13. Acquisition/OPKI operation

13.1. All OPKI activities are planned, deliberate and determined by time, scope and available capabilities and resources.

13.2. Resources for acquisition of print publications and commercial subscriptions must be planned for and budgeted by the mission.

13.3. Before starting the acquisition, an analysis of the risk of bias, misinformation, disinformation and the likelihood of hostile entities tracking and identifying the OPKI efforts must be undertaken.

13.4. Because of the massive quantity of information from open sources that is available, OPKI efforts must be carefully planned by prioritizing and strategizing search activities and considering the available processing tools.

13.5. Regarding information acquired that warns of an imminent threat to the safety and security of UN personnel and/or civilians, please see paragraph 16.1.

13.6. Online algorithms learn from user activities. This is especially relevant for social media networks and search engines. Be aware of so called "filter bubbles" that will only show results that acknowledge your previous searches/activities.

14. Collation / Examination

14.1. Due to the large amount of data that will be acquired from OPKI, the systematic receiving, grouping, recording and filing of all acquired information is a necessity. One of the reasons to do this is to avoid circular reporting. Management of data is key.

14.2. Since in OPKI there will be a vast array of sources, it is important to consider for each piece of information the allegiance, personal agenda, objectives and interests of the author, company, website, political party, agency, etc. that published the information, in order to determine the potential for bias, misinformation, disinformation, propaganda and fake news.

14.3. A form of validation of sources is necessary. For source validation, a similar system as with HPKI can be used. In OPKI the rating will concern the author (or speaker or website of origin) and the content of the information.

[6] JMAC, UNDSS, JOC (supporting), Force, Police Component.

Table 1. Rating of source reliability

Source Reliability		
Rating	**Evaluation**	**Observations**
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
D	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
E	Cannot Be Judged	No basis exists for evaluating the reliability of the source

Table 2. Rating of information credibility

Credibility of Information		
Rating	**Evaluation**	**Observations**
1	Confirmed	Confirmed by other independent sources; logical in itself; Consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
4	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
5	Cannot Be Judged	No basis exists for evaluating the validity of the information

15. Analysis

15.1. An OPKI specialist or cell may engage in so-called single source analysis, in order to organize and structure the available information to prevent the analysts from being overloaded with too much information to process, integrate and interpret; single source OPKI must be marked as such.

16. Dissemination

16.1. Information acquired by an OPKI specialist that warns of an imminent threat to UN personnel or to civilian populations, must be immediately disseminated to its peacekeeping-intelligence component[7] via the quickest means. The PKI Component will then **immediately** alert all other Members of the MICM, including the Mission Chief of Staff.

16.2. Likewise, information acquired by an OPKI specialist that relates to suspected criminal activity, must also be disseminated to its peacekeeping-intelligence

[7] JMAC, UNDSS, JOC (supporting), U2, Police Component.

component[8] via the quickest means. The PKI Component will then alert the Mission's Police CIU.[9]

16.3. The following dissemination principles shall be adhered to:

16.3.1. **Timeliness –** Acquired information must be delivered in a timely manner so planners and decision makers can act rather than react;
16.3.2. **Relevance** – Is determined by the needs of the recipients as defined in the applicable (mission or component) IAP;
16.3.3. **Brevity** – Reports must be kept as brief as possible, but at the same time include everything that the recipient needs to know;
16.3.4. **Interpretation** – Wherever possible, all facts must be correctly evaluated, and their significance interpreted before dissemination.

16.4. An OPKI specialist or cell may choose to make their information structurally available for a wider public by means of an OPKI dashboard that integrates multiple OPKI feeds.

16.5. In dissemination of OPKI a legal basis must be considered: the majority of OPKI, especially of commercially available information, is protected by copyright laws. These laws must be taken into consideration and this type of information may only be shared to support the mission.

F. TERMS AND DEFINITIONS

17. **Component OPKI specialist** refers to a military, police or civilian staff member, with previous OPKI or Open-Source Intelligence (OSINT) training and experience, conducting OPKI activities in UN peacekeeping operations.

18. **Disinformation** is false or inaccurate information posted or published with an intent to deceive. It includes deliberately misleading or biased information, manipulated narrative or facts, and propaganda. The origin of the information can be concealed, it can be covertly spread and the intent and beneficiaries of the disinformation campaign aren't always clear. It is considered a subcategory of misinformation.

19. **Filter bubbles** are a state of intellectual or ideological isolation that may result from algorithmic filtering, which are algorithms feeding the recipient information they like or agree with, based on their past behavior and search history, potentially distorting their perception of reality because they see too much of one side, and not enough of others.

20. **Misinformation** refers to false or inaccurate information that is posted or published, regardless of whether there is an intent to deceive or mislead.

[8] JMAC, UNDSS, JOC (supporting), U2, Police Component.
[9] With current non-executive mandates, UNPOL cannot always act on the information, but can share serious crimes (as defined by local laws) with local counterparts.

21. **OPKI** is the Peacekeeping-Intelligence derived from the acquisition, collation, and analysis of publicly available information (PAI) from open sources in response to peacekeeping-intelligence requirements.

22. **OPKI operation** refers to the planning and efficient execution of an operation in a peacekeeping mission to search for, find and extract publicly available information in a safe, legal and non-clandestine manner. This includes in-person and virtual activities.

23. **VPN** refers to a Virtual Private Network. It is a service that provides a user with online privacy and anonymity. VPNs mask the internet protocol (IP) address of the device so that online actions are virtually untraceable. By connecting to a secure VPN server, the internet traffic goes through an often encrypted tunnel on the public internet.

G. REFERENCES

General Assembly and Security Council References

- Report of the Special Committee on Peacekeeping Operations, 2020 Substantive Section (A/74/19)

Normative or Superior References

- DPO Policy on Peacekeeping-Intelligence, 2019
- DPO-DOS Policy on Joint Mission Analysis Centres (JMAC), 2020

Related Guidelines

- Joint Mission Analysis Center Handbook, 2017
- Military Peacekeeping-Intelligence Handbook, 2019
- Peacekeeping-Intelligence Surveillance and Reconnaissance Staff Handbook, 2020
- Acquisition of Information from Human Sources for Peacekeeping-Intelligence, 2020

H. MONITORING AND COMPLIANCE

24. Within missions, the Head of Mission is accountable for the mission's compliance with these Guidelines and shall establish mechanisms or processes to enable the effective monitoring of compliance. All mission personnel participating in the peacekeeping-intelligence system are accountable through their chains of management/command for compliance with the Policy and these Guidelines.

I. CONTACT

25. The contact for these guidelines is the Peacekeeping-Intelligence Coordination Team (PICT) (in DPO/OUSG).

J. HISTORY

26. This is the first iteration of these Guidelines.

APPROVAL SIGNATURE:

Jean-Pierre Lacroix, Under-Secretary-General for Peace Operations

DATE OF APPROVAL:

21 February 2022

Annex A

Tips and Tools

Publicly available tools

Alexa.com (Amazon)
A tool for keyword research, website traffic statistics and finding similar sites

Datawrapper (datawrapper.de)
Create charts, maps and tables with your data

EO browser (apps.sentinel-hub.com/eo-browser)
Browse and compare full resolution satellite data from numerous satellites

Forensically Beta (29a.ch/photo-forensics/)
Digital image forensics (clone detection, meta data extraction and more)

Google Data Visualiser (datastudio.google.com)
Find, visualize and share data

Google Earth (google.com/earth/)
Browse maps and imagery, import and export GIS data, create maps

Google Trends (trends.google.com)
Explore trending topics, latest stories and insights for specific regions

In Vid (invid-project.eu)
Detect, authenticate and check the reliability and accuracy of video files

News Explorer IBM Watson (news-explorer.mybluemix.net)
Explore trending queries, trending connections and breaking news

Open Refine (openrefine.org)
Explore data sets, clean up and transform data formats, link data sets

Tin Eye (tineye.com)
Reverse image search for image identification, verification, tracking, recognition

RAWGraphs (rawgraphs.io)
Data visualization framework

TweetDeck (tweetdeck.twitter.com)
Real-time tracking and organizing of Twitter engagements

Twitter Audit (twitteraudit.com)
Authenticate Twitter accounts (fake / real)

UN subscriptions

Dataminr (dataminr.com)
AI tool for public data sets. Dataminr provides the UN with access to First Alert

Publicly available datasets

ACLED (acleddata.com)
Real-time data on locations, dates, actors, fatalities and types of events

Fragile States Index (fragilestatesindex.org)
Country dashboards, comparative analysis, trend analysis

Global Peace Index (visionofhumanity.org)
An overview of peace factors per country

Health Map (healthmap.org)
Disease outbreak and public health threat monitoring based on online informal sources

IOM (migrationdataportal.org)
Migration statistics on flows, vulnerability, policy, public opinion and more

Uppsala Conflict Data Program (ucdp.uu.se)
Data on organized violence