United Nations
Department of Peace Operations
Ref. 2025.14

Manual

Intelligence-Led Policing

Approved by:	Faisal Shahkar, Police Adviser and Director PD
Effective date:	1 September 2025
Contact:	DPO/OROLSI/PD
Review date:	1 September 2030, or as needed

DPO MANUAL ON INTELLIGENCE-LED POLICING

Contents:

ANNEXURES

A. PURPOSE AND RATIONALE

1. This Department of Peace Operations (DPO) Manual on intelligence-led policing (hereinafter referred to as "the Manual") outlines the core principles and approaches of intelligence-led policing (ILP) for United Nations police (UNPOL). Its purpose is to build the capacity of the host state and, where applicable, apply these principles mutatis mutandis while carrying out policing functions in peacekeeping missions, special political missions, or non-mission settings, as mandated by Security Council resolutions.

2. This manual is designed to ensure that intelligence-led policing practices are integrated effectively into policing strategies, thereby enhancing the capacity of UNPOL to prevent, detect, and respond to threats to peace and security. By fostering a more proactive, evidence-based approach to policing, the manual aims to guide UNPOL personnel in using crime intelligence to inform decision-making, operational planning, and the delivery of security interventions, with the overarching goal of supporting sustainable peace, security, and rule of law in post-conflict and transitional environments. A separate manual on UNPOL Crime Intelligence will address the crime peacekeeping-intelligence (CPKI) within United Nations peace operations, in depth. This manual outlines the performance in line with the strategies mentioned hereafter, with a specific focus on the implementation of intelligence-led policing strategies. Intelligence-led policing develops data and information analysis into crime intelligence processes to the point where, the collection and analysis of intelligence has

become central to contemporary policing.[1] ILP emphasizes a proactive response to crime and provides law enforcement with an evidence-based approach to decision-making. The established community policing skills[2] directly support ILP responsibilities, including problem solving, environmental scanning, effective communication with the public, fear reduction, and community mobilization to deal with problems.[3]

3. The manual is an integral part of The Strategic Guidance Framework on United Nations Police in Peacekeeping Operations and Special Political Missions, it aims to enhance the effectiveness of UN policing through more consistent, harmonised approaches to the provision of ILP management. By elaborating set of principles and concepts, the manual can also assist mission planning and operations for UNPOL operations amid an expanding portfolio of developing roles, responsibilities, and tasks besides the primary aim of capacity building and development. Strategic Guidance Framework for International Policing (SGF) emphasises the importance of intelligence-led policing and processed information on crime and criminality, to plan, prioritize and allocate resources in undertaking crime reduction strategies.[4]

B. SCOPE

4. The manual is designed to assist UNPOL components in the fulfilment of their mandated roles, primarily capacity development and support to host-state police and other law enforcement agencies in ILP, and mutatis mutandis to undertake itself the ILP strategies for efficient and effective monitoring and executive functions, whenever mandated so. The elements in this manual are designed to guide the UNPOL to advise the host state in decision making process in all aspects of policing work with the help of processed information. It will assist to undertake strategic guidance, including targeting serious crimes and/or prolific offenders, and strategic support to host-state police and other law enforcement agencies, more effectively decide on priorities, planning, allocation of resources and strategies to prevent and detect crime and maintain public safety and security. This manual shall be followed in coherence with other DPO-DOS guidance documents, published and/or under development, under the SGF.

5. The manual is applicable to all personnel of UNPOL components and provides necessary guidance to personnel in the field as well as in headquarters, to support UNPOL leadership in decision making through a consistent process of identifying and prioritizing serious crime threats against mandate implementation, protection of civilians and security and safety of UN personnel and premises. The application of this manual may be directed to complement peacekeeping-intelligence as defined in the DPO Policy on Peacekeeping-Intelligence (2019), which is intended to support a common operational picture, provide early warning of imminent threats, and identify risks and opportunities regarding the safety and security of UN and associated personnel, and the protection of civilians. ILP's scope and governance – as well as any crime intelligence-related activities - is always determined by the Mission's governing

[1] Steve Christopher, "A Practitioner's Perspective of UK Strategic Intelligence," in *Strategic Thinking in Criminal Intelligence*, ed. Jerry H. Ratcliffe (Sydney: Federation Press, 2004), 176-292.
[2] DPKO/DFS Manual on Community-Oriented Policing in United Nations Peace Operations, 2018.04.
[3] Leigh, A., Read, T., & Tilley, N. (1996). *Problem-Oriented Policing: Brit POP* (Crime Detection and Prevention Series, Paper No. 75). London: Home Office Police Policy Directorate.
[4] DPKO/DFS Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions, 2015.15.

mandates drawn solely from relevant UN Security Council resolution(s) and which are clearly stated in each Mission's Police Concept of Operations (ConOps).

C. GUIDING PRINCIPLES

C.1. Respect and protect human rights

6. All UNPOL activities related to intelligence-led policing — including crime prevention, detection and investigation, protection of persons and property, and the maintenance of public safety and law and order — shall be guided by the obligation to respect and uphold human rights, ethical norms and standards in criminal justice, as well as international human rights and humanitarian law. In all aspects of their operations, UNPOL personnel shall comply with human rights standards and shall be prepared to intervene, including the use of force where mandated, to stop on-going human rights violations and to protect civilians. There shall be a clear agreement and understanding of the responsibilities of the UNPOL and the host-State authorities and in the provision of support to host-state police and other law enforcement agencies and their operations in adherence to the United Nations Policy on Human Rights Due Diligence (HRDDP).

C.2. Gender mainstreaming

7. UNPOL components shall ensure that UN gender mainstreaming and Women, Peace & Security (WPS) mandates are followed and mainstreamed in all their crime intelligence-led policing strategies and all ILP activities conducted in support of the host-State police including the prevention, detection and investigation of crime, protection of persons and property, and the maintenance of public order and safety.[5] UNPOL officers shall use a gender analysis and incorporate gender considerations into all aspects of ILP operations such as acquisition of information, collation, analysis and dissemination of information, planning, management, budgeting, and decision making. UNPOL officers shall promote a non-discriminatory and adequate representation of qualified women in the host-state police at all levels and work actively to ensure that women in the host-State police are ensured unencumbered access to equal capacity and career development opportunities. UNPOL officers shall ensure the adequate participation of women police officers in all decision-making processes.

C.3. Partnership working

8. UNPOL shall ensure a wholesome scenario to guide the host state police crime intelligence-led operational activities under the SC mandated tasks and the stipulated legal framework of the host-state. It should augment a secure environment that promotes positive outcomes and considered beneficial to combat crime and criminal activities. It shall collaborate to enhance protection, peace building and sustainable peace keeping approach. Sustained partnership working between law enforcement agencies, government departments and public shall be emphasized to oversee criminality. Effective partnership working in ILP requires effective communication, trust, and a commitment to sharing information and resources. It also involves developing shared goals and strategies, collaborating on joint operations and investigations, and establishing strong relationships with communities to promote public safety and crime prevention. By working together law enforcers can leverage their resources, expertise, and

[5] DPO Guidelines on Gender and Peacekeeping-Intelligence, 2022.08.

experience to prevent and detect criminal activities, thereby promoting public safety and improving the quality of life for communities.

C.4. Evidence Based

9. UNPOL shall use evidence-based practices in ILP to ensure that host state police and /or UNPOL operations are effective and efficient, and that resources are targeted where they are most needed. ILP shall be based on empirical evidence and research findings rather than on intuition or guesswork.[6] The goal is to ensure that policing efforts are effective, efficient, and well-grounded in the best available means of acquiring, collation, sanitization, analysing and dissemination.

C.5. Risk management

10. ILP shall be based on an efficient and effective risk management approach, ensuring that all available resources are allocated to the operational priorities where they are most needed, as determined by an assessment of the level of risk posed by various criminal activities. It shall identify, assess, prioritize potential risks, threat to public safety, and develop strategies to mitigate the risks. In the context of ILP, risk management should involve identification of areas or individuals that are at elevated risk of criminal activity, as well as the factors that contribute to that risk. This must include crime data, conduct community surveys, and gather intelligence and information through investigations, interviews, and other best available sources.

C.6. Security and confidentiality

11. UNPOL shall ensure access control, privacy and data protection and legal compliance as per the provisions of security council mandate, host state prevalent laws and regulations. Security refers to the measures and protocols put in place to protect assets, information, and resources from threats such as unauthorized access, harm, or damage. Whereas confidentiality refers to the practice of keeping sensitive information private and ensuring that it is only accessible to those who are legally authorized to view or use it. ILP must safeguard assets, including physical property, digital information, and personnel. It should ensure risk management by identifying, assessing, and mitigating risks that could compromise security. Only legally authorized individuals should have access to sensitive information and resources. Trust building to be encouraged amongst all entities of United Nations, International organizations, and host-state that confidential information is overseen with care and respect. Confidential crime intelligence products shall be disseminated based on need to know and need to share concepts, which require that crime intelligence should be disclosed to mission personnel if and only if access to said information is required for them to perform their official duties. It implies that crime intelligence is disclosed to trusted individuals to ensure that it is not widely disseminated, where disclosure is likely to endanger the safety or security of any individual or group, violate rights or invade privacy. In doing so UNPOL will seek to establish and maintain a high degree of confidence among all their interlocutors in their ability to appropriately acquire, protect and manage crime intelligence. Security and confidentiality are interrelated and often work in tandem to ensure ethical behaviour, secure operations, and effective management in various operational assignments.

D. INTELLIGENCE-LED POLICING FOR UNPOL ROLES

[6] Ratcliffe, Jerry H. *Intelligence-Led Policing*. 2nd ed. London: Routledge, 2016.

12. The mandate of UN Security Council directs UNPOL to build and to support, or, where directed, act as a substitute or partial substitute for, host-state police to prevent and detect crime, protect life and property, and maintain public order and safety in adherence to the rule of law and international human rights law. The work of the UNPOL is undertaken within a framework which may include for example, the security sector reform, monitoring, reporting and accountability mechanisms, activities by UN agencies funds and programmes, the provision of humanitarian assistance, the protection and promotion of human rights, support to the rule of law and political peacebuilding activities, early peacebuilding for peace operations, and encompasses efforts to prevent the outbreak of or relapse into conflict. Conflict prevention involves both immediate operational activities (stabilization and physical protection) and long-term structural prevention (building of political will and national capacity) within a larger context, including reconciliation and transitional justice as critical factors for sustainable peace.[7]

13. UNPOL need to understand the issues they are dealing with, especially as applicable to the context of an international setting, the threats, risks and mitigating factors, and the positions and drivers of stakeholders to identify areas where they can be leveraged. Crime intelligence is essential for United Nations police in accurately identifying and understanding the operational context — including the nature and extent of issues, emerging trends and associated threats or risks, and relevant stakeholders. It supports strategic planning, informed decision-making, and the effective and efficient use of available resources to achieve the greatest impact and the highest likelihood of success. The manual underscores the importance of adherence to the host state's legal requirements, ensuring all activities align with national laws and legal provisions. This approach reinforces collaboration and compliance within the framework of international best practices.[8]

14. Intelligence-led Policing (ILP) and Community-Oriented Policing (COP) are the overarching approaches that guide UNPOL operational activities. While the COP strategy focuses primarily on community concerns and directly address issues of public trust in the police, it will also encourage the public to become partners in preventing and detecting crime in their communities and therefore complements ILP, which targets key peace spoilers, and prolific and/or serious offenders identified as threats through crime intelligence analysis. Intelligence-led policing has become critical to the UNPOL over the period of last decade and a half for the proper identification and understanding of the context, including the nature and extent of the issues related to crime and criminality. How they make a trend, impose threats, and create risks. It is important to identify the real stakeholders, conduct strategic planning and informed decision-making. Which should result into effective and efficient utilization of the available resources provided by the member states and host state. The benefits of intelligence-led policing should promise the greatest results and the best chances for success.

E. CONCEPTUAL FRAMEWORK OF ILP

15. As enumerated above ILP is a managerial philosophy where data analysis and crime intelligence are pivotal to an objective decision-making framework. Which leads to problem reduction and crime control. This definition of ILP requires the integration and interdependence of the following distinct concepts and practices:

[7] https://police.un.org/en/mission-of-un-police
[8] https://www.unodc.org

16. *Criminal Intelligence*: It is the processed information on criminals. It relates to the activities of criminal individuals or groups of offenders. It is the creation of an intelligence knowledge product that supports decision-making in the areas of policing and other law enforcement, crime reduction, and crime prevention. Criminal intelligence can provide decision-makers with a snapshot of criminality and criminal behaviour,[9] i.e., give information on prolific offenders and organised crime groups.

17. *Crime Analysis*: It is the processed information on crimes. Crime analysis is further defined as the "qualitative and quantitative study of crime and law enforcement information in combination with socio-demographic and spatial factors to apprehend criminals, prevent crime, reduce disorder, and evaluate organizational procedures."[10] Crime analysis includes all types of analysis performed within a police agency, except for forensic evidence (including DNA) analysis and workforce planning and other administrative analysis related to budgeting, personnel (e.g., overtime, sick and vacation leave, salary), and equipment. Therefore, crime analysis can provide understanding of crime patterns and trends, i.e., understanding the crime context of the environment in which offenders operate. Criminal Intelligence and Crime Analysis are not only separate entities, but criminal intelligence officers are typically sworn police officers assigned in dedicated units. Whereas crime analysts are frequently civilian personnel who report directly to the command staff of police agency.

18. *Crime Intelligence:* Crime Intelligence is the products of crime analysis and criminal intelligence, i.e. fusing data from crime analysis of crime patterns with that of criminal intelligence based on the criminal behavioural characteristics of individuals or groups. Crime intelligence does not only focus on certain offenders (criminal intelligence) but also on occurrence of certain categories of crime (crime analysis) and thus these two concepts "used in combination, are essential to a more complete understanding of criminality necessary to formulate effective crime reduction and prevention strategies". This integrated analysis will enable the decision makers to look at the bigger picture of criminality, which will assist them to formulate more measures to effectively address the identified issues.[11] Criminal intelligence provides information on prolific offenders and organized criminal groups, while crime analysis provides the crime context of the environment in which they offend. Both are essential to a full understanding of crime problems and recidivist criminality and are prerequisites of good decision making and effective crime reduction.

19. ILP requires institutional structures that support continuous intelligence cycles—from data collection and processing to analysis, dissemination, and decision-making. It also depends on the establishment of intelligence-led priorities, senior leadership commitment, information sharing protocols, and adherence to legal and human rights standards.

20. Ultimately, ILP empowers police leadership to make objective, evidence-based decisions. It shifts the focus of policing from reacting to individual incidents toward proactively managing threats, reducing harm, and strengthening public safety in a sustainable and accountable manner.

F. PROCEDURES

[9] Ratcliffe, J.H. (2008:87), Intelligence-Led Policing. Cullompton, UK: Willan Publishing.
[10] Boba, Rachel. 2005, 06.
[11] Ratcliffe, J.H. (2008:87), Intelligence-Led Policing. Cullompton, UK: Willan Publishing.

F.1. Crime Intelligence Process

21. The Crime Intelligence Process (CIP) consists of two distinct parts. (1) Crime and Public Safety Threat Identification and Analysis, and (2) UNPOL Crime Intelligence Cycle (CIC) as shown in figure 1 below. CIP is a term used to describe the various processes and assets used to acquire crime intelligence. It initially encompasses the crime and public safety threat identification and analysis that leads to the CIC, which includes direction/decision, information acquisition, examination/collation, analysis, and dissemination of crime intelligence products that drives the ILP (see Figure 1).

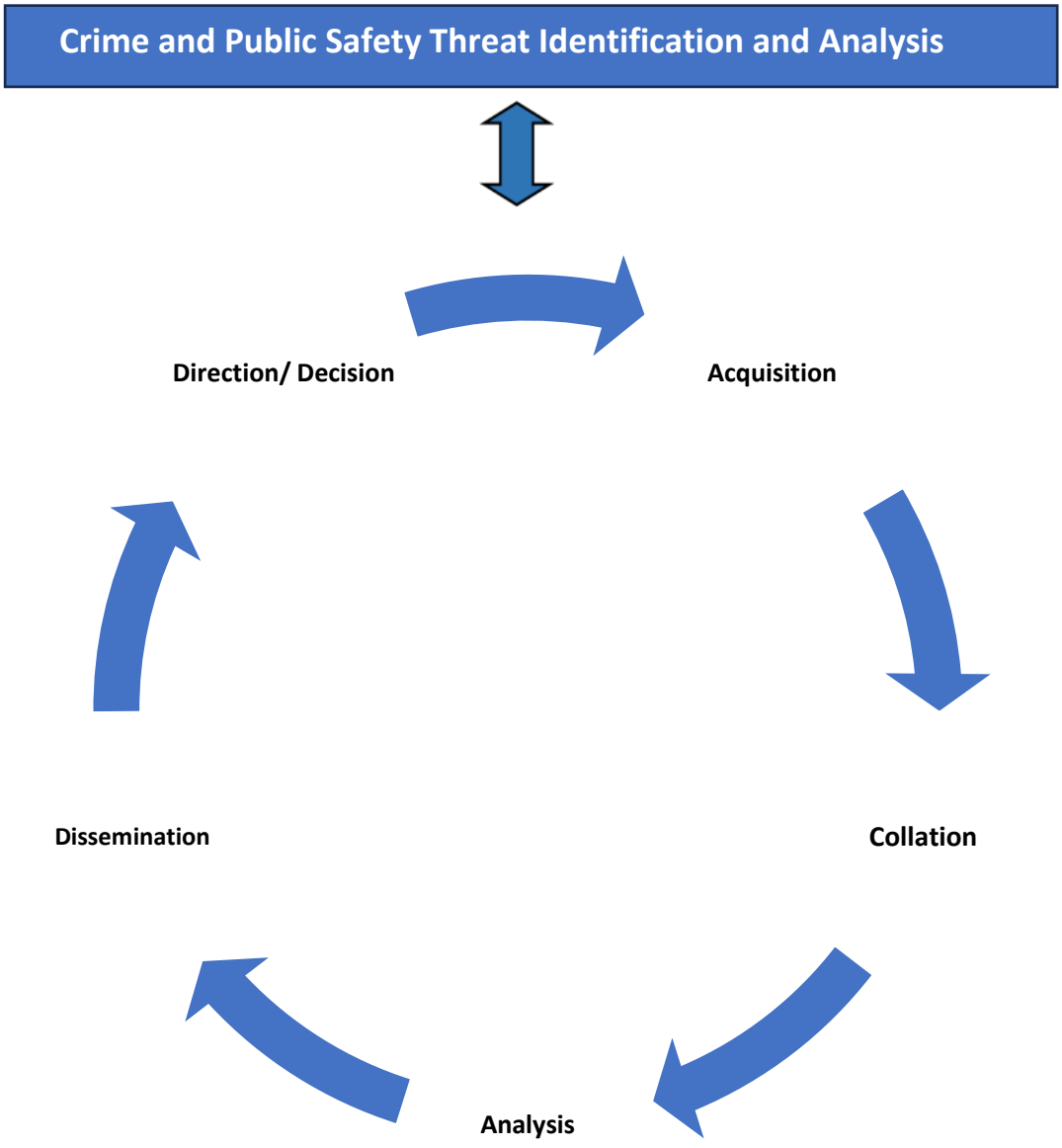

Figure 1 UNPOL Crime Intelligence Process

22. The crime intelligence cycle shown above gets a strategic guidance/direction from threat identification and analysis when a new mission is being established or a mission's mandate changes. Within an established mission, where Crime Intelligence units (CIUs) are operational, threat identification and analysis are systematically integrated across the entirety of the CIC. CIC will be explained below under section F.2. followed by detailed explanation of crime and public safety threat identification and analysis under section F.3.

F.2. UNPOL Crime Intelligence Cycle

23. The UNPOL CIC consists of following components (Figure 2).

23.1. **Direction:** Defining the focus area of the data capture.

23.2. **Acquisition:** Gathering relevant information.

23.3. **Collation:** Grading the quality of information and comparing it with other holdings and sources.

23.4. **Analysis:** Developing inferences and assumptions.

23.5. **Dissemination:** Sharing the crime intelligence product.

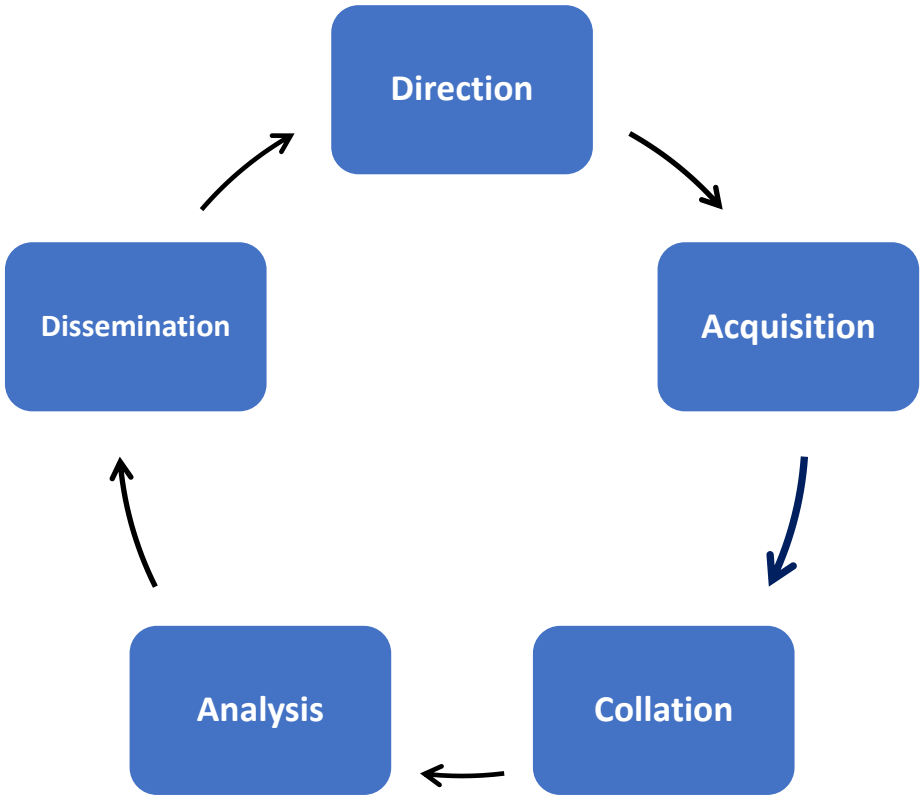

Figure 2 UNPOL Crime Intelligence Cycle

F.2.1. Direction/Decision

24. Direction for crime intelligence can be freshly initiated as per the requirements or because of completion of the crime intelligence cycle which is a well-founded decision. Any direction for crime intelligence refers to the process of identifying questions that need to be answered, specifying outstanding information in relation to those questions and seeking this information through a variety of means. Direction/decision ensures strong central control of the crime intelligence cycle, tying the crime intelligence requirements (CIRs) of the head of police component (HoPC) and the senior leadership to the crime intelligence unit/team. Crime intelligence team management mechanisms shall establish the priorities and time frames. Further decisions for crime intelligence team activities shall be carried out under the authority and accountability of HoPC or within the delegated authority.

F.2.2. Acquisition

25. The cycle of UNPOL Crime intelligence works under the direction, tasking, requirements, and decisions from HOPC as shown in figure 2. To ensure that acquired information is relevant and that data received will not become voluminous, which is a usual problem in crime intelligence production, a careful acquisition planning should be instituted in the Crime Intelligence Unit (CIU). Acquiring information in peacekeeping operations should be within the confines of the mandate and relevant policies. In this sense, acquiring information in UN policing may take in the following forms:

    25.1. Tasked Acquisition - Tasked acquisition is an activity specifically carried out based on an acquisition plan, in response to CIRs.

    25.2. Spontaneous or unsolicited receipt of information - This kind of acquisition is an unintended collection where information reaches the CIU through formal or informal UNPOL communications. These pieces of information may come from UNPOL team sites, field offices, investigation units, IPOs, FPUs, partner agencies, host-state counterparts, etc. UNPOL staff awareness is critical to ensure the flow of information from their respective fields to the CIU office.

26. *Sources of Information:* One of the sources of information could be Suspicious Activity Reports (SARs). Although SARs may come from all UNPOL officers and personnel within the jurisdictional area, the normal routine patrolling, and policing duties of IPOs and FPUs have the higher likelihood to generate SARs. The report contains suspicious person, organization, activities, etc. which deemed unusual in their respective areas of jurisdiction. Every UNPOL commanders or Chiefs of offices should ensure that SARs are submitted to the CIU once reported by their subordinates. Any information may come from the community or concerned individuals about crimes, criminals, and criminal activities. However, children must not be used as source of any information. It can also be the information provided by partner agencies and/or host-state counterparts. These pieces of information may be important to existing crime intelligence projects and shall be endorsed to the CIU in the most practical means. Open-source intelligence is amongst the sources of information used for crime intelligence gathering.[12] One very notable subset of open-source information is so called grey literature.[13] It can consist of research, technical, economic reports, white papers, conference

[12] DPO Guidelines on Open-Source Peacekeeping-Intelligence (OPKI), 2022.03.
[13] https://vocabularies.unesco.org

documentation, dissertations, thesis, discussion papers, subject-related newsletters, etc. One of the main difficulties in working with this type of source is appraisal, as information available in the public domain can frequently be biased, inaccurate or sensationalized. Restricted or closed source is a type of source information which has limited access and availability to the public. Closed source information is often found in the form of structured databases. In the context of crime intelligence analysis, these databases will largely include data available with host-State crime record bureaux, personal data acquired as part of ongoing targeting operations, or broader criminal records, vehicle registration data, weapons licensing, etc.

F.2.3. Collation

27. During the collation stage of the crime intelligence cycle, the acquired material is transformed from its assembled format into meaningful information. It is crucial for the acquisition and assembly stages to be conducted thoroughly to ensure the accuracy and objectivity of the information. Through summary, assessment, and interpretation, the raw data is enriched and transformed into valuable insights. The comprehensive view of the information obtained during the collation stage provides an overview of the situation at hand. The validity of an inference is directly linked to the quality of the data behind the inference. Thus, data evaluation is a crucial step in the crime intelligence cycle. It should occur at the same time or right after data is gathered to ensure it is assessed in the context in which it was collected. This helps prevent errors that arise when information is not accurately presented within its local setting. Evaluation requires a separate assessment of the reliability of the source (the provider of the information) and validity and accuracy of the information. Once information has been acquired it must be evaluated, a stage that must not be overlooked or ignored. A full and proper evaluation requires the assessment of the reliability of the source and the validity of information. *It is important that information should be cross-checked and rigorously evaluated based on the inputs from more than one source, if possible.* Three fundamental principles shall be applied to collation:

    27.1. It must not be influenced by personal feelings but be based on professional judgement.

    27.2. Evaluation of the source must be made separately to the information.

    27.3. It must be carried out as close to the source as possible.

28. Collation is principally an orderly organization and arrangement of acquired information, and the placement of data in a system that will facilitate easy and fast retrieval and analysis.[14] Arranging the information into categories like criminal groups, criminal networks (e.g., regional/country-specific human trafficking, money laundering via betting shops, etc.), modus operandi and geographical operational locations is more advisable since it can be retrieved faster and can be manipulated across categories. Collation can be more efficient using information technology. However, post-conflict areas may lack equipment and technology thus old-fashioned systems can be practical and easy implementable in this situation.

29. *Sanitization:* Sanitization is part of the collation process but distinctly important in information and intelligence sifting. Reports should be sanitised for onward transmissions by removing material which explicitly or implicitly identifies a source or UN methodology. The text (as opposed to the source reference) should give no indication of the nature of the source,

[14] Schneider, S.R., “The Criminal Intelligence Function: Toward a Comprehensive and Normative Model” n.d.

whether human or technical or the proximity of the source to the information. In the context of crime Intelligence, sanitization refers to the process of removing sensitive or confidential information from crime intelligence products, such as reports, briefings, and assessments, before they are disseminated or shared with external partners. The purpose of sanitization is to protect the sources, methods, and capabilities of the crime intelligence community, as well as the privacy and rights of individuals who are not associated with criminal activities. It also helps to avoid compromising ongoing investigations or operations, as well as national security interests. The sanitization process may involve redacting or removing specific information, such as names, locations, dates, and other identifying details, which could reveal the identity of sources, or the methods used to collect the information. The process may also involve removing information that is not relevant or necessary for the intended audience or purpose of the crime intelligence product.[15]

30. Sanitization is a key component of the crime intelligence production process, and it is often subject to strict regulations, policies, and guidelines to ensure consistency, accuracy, and accountability. The process requires careful consideration of legal, ethical, and operational implications, as well as the balancing of competing interests and priorities. Following evaluation, it is advisable to continue with a system of sanitization. This is intended to protect the source or origin of the information from being detectable from the context or wording of the report. It also seeks to protect the circumstances or method by which the information was obtained.

F.2.4. Analysis

31. Analysis is a vital step in the crime intelligence cycle, aimed at understanding, predicting, and preventing criminal activities. It involves systematically applying analytical methods to evaluate and interpret acquired and collated data, with the goal of providing actionable insights. These insights will help law enforcement agencies in decision-making, resource allocation, and strategic planning at tactical, operational, and strategic levels. Below are the key elements and types of crime intelligence analysis:

31.1. *Data Integration and Validation*

- Analysts should compile, integrate, and validate data from multiple sources, assessing its quality, reliability, and relevance. This process ensures that the analysis is based on accurate and comprehensive information, forming the foundation for identifying connections between criminal activities, individuals, and groups.

31.2. *Pattern, Trend, and Predictive Analysis*

- Pattern and Trend Recognition: By analyzing large data sets, analysts must identify patterns, trends, and recurring behaviors in criminal activities, such as crime hotspots, preferred methods, and shifts in criminal behavior over time.

- Predictive Analysis: Advanced statistical models and machine learning techniques should be used to forecast future criminal activities, enabling law enforcement to proactively allocate resources and implement preventive strategies.

31.3. *Network and Link Analysis*

[15] Ratcliffe, Jerry H. *Intelligence-Led Policing*. Cullompton, UK: Willan Publishing, 2008. 2008.

- This method focuses on uncovering relationships between individuals, groups, and criminal activities. Using tools like link analysis, analysts can identify the structure, hierarchy, and operational dynamics of criminal networks, which is critical for dismantling organized crime groups.

31.4. *Geospatial and Temporal Analysis*

- Geospatial Analysis: Geographic Information Systems (GIS) should be utilized to map crime data and identify spatial patterns, such as high-risk areas or routes frequently used for criminal activities.

- Temporal Analysis: Analysts examine the timing and frequency of crimes to understand patterns over days, weeks, or seasons, aiding in resource allocation and preventive measures.

31.5. *Threat and Risk Assessment*

- This involves evaluating potential threats, vulnerabilities, and risks to communities or regions. Threat assessments help law enforcement prioritize interventions, mitigate risks, and enhance public safety through targeted action plans.

31.6. *Tactical and Strategic Analysis*

- Tactical Analysis: Focuses on supporting immediate, case-specific investigations by providing actionable insights, such as suspect profiles or links to ongoing crimes.

- Strategic Analysis: Examines long-term trends and broader issues to guide high-level planning, resource distribution, and policy decisions.

31.7. *Collaboration and Operational Support*

- Crime intelligence analysis is most effective when analysts collaborate closely with investigators, field officers, and other stakeholders. This ensures real-time information sharing and enhances the operational response to criminal activities.

31.8. *Ethical and Legal Considerations*

- Crime intelligence analysis must operate within ethical and legal boundaries, respecting privacy rights, avoiding discriminatory practices, and maintaining transparency and accountability. This is essential to uphold public trust and adhere to international standards, particularly in UNPOL operations.

32. Advances in technology, such as machine learning, predictive analytics, and data visualization, have significantly enhanced crime intelligence analysis capabilities. These tools enable analysts to process vast amounts of data quickly and make informed decisions. However, ethical considerations must remain a priority to balance technological advantages with the protection of civil liberties and data privacy as per the legal provisions of the host state laws.

F.2.5. Dissemination

33. Dissemination refers to the process of sharing and distributing relevant analysed intelligence information to appropriate stakeholder within the UNPOL mission or outside (in case of non-mission settings). The dissemination stage in ILP is crucial for effective collaboration, informed decision-making, and the operationalization of intelligence to prevent and investigate criminal activities. Following components shall be involved in the dissemination of information in ILP:

    33.1. Intelligence products: Intelligence analysts create intelligence products that distil the analysed information into format suitable for dissemination. These products will include strategic assessments, tactical reports, briefings, alerts, and bulletins depending upon the intended audience and purpose.

    33.2. Targeted dissemination: Intelligence will be disseminated selectively to relevant stakeholders based on their need-to-know and operational responsibilities. This can include law enforcement agencies, investigators, frontline officers, policymakers, and other authorized recipients who can benefit from the intelligence for their operational or strategic purposes.

    33.3. Timeliness: Dissemination will occur in a timely manner to ensure that stakeholders have the most up-to-date information. Rapid dissemination can support proactive interventions, investigations, or preventive measures.

    33.4. Secure Communication: Due to the sensitive nature of crime intelligence information, secure communication channels and protocols should be employed to protect the confidentiality, integrity, and availability of the disseminated intelligence. This may involve the use of encrypted systems, secure databases, or controlled access to information.

    33.5. Collaboration: Dissemination promotes collaboration among different agencies and units within the law enforcement community. By sharing intelligence, agencies can benefit from a collective understanding of threats, criminal networks, or emerging patterns, leading to more effective and coordinated responses.

    33.6. Feedback Loop: Dissemination is not a one-way process. Feedback mechanisms should be established to gather insights, observations, or additional information from the recipients of the disseminated intelligence. This feedback helps refine the analysis and dissemination process, enhancing the overall intelligence cycle.

34. The dissemination of analysed information under this manual shall ensure that relevant stakeholders are informed, empowered, and equipped to make informed decisions and take appropriate actions to address crime and security challenges. It should facilitate the utilization of intelligence as a valuable resource for crime prevention, investigations, resource allocation, and strategic planning within the law enforcement community.[16]

35. There are several concepts to be understood when recording, analysing, and disseminating crime intelligence. The table elaborated in at Annex-A is the UNPOL 5x5x5 crime Intelligence system which is used in evaluating and classifying received information and/or crime intelligence, and in determining its further dissemination.

[16] DPO Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities, 2022.05.

36. The well evaluated and sanitized information shall be processed in this stage to initially see either it is to be disseminated or not, and if appropriate for dissemination, to whom? Handling codes are designed to assist the CIU in the risk assessment decision of these tasks. The codes provide clarity over the purpose for communicating the piece of crime intelligence to others. By recording this on the UNPOL crime intelligence system of 5x5x5 (Annex-A), it clearly outlines the conditions which should be met when disseminating that specific piece of crime intelligence to other parties (detailed description will be covered in forth coming DPO manual on UNPOL Crime Intelligence 2025).

37. Once crime intelligence is integrated into an assessment tool, and it is graded as 'Restricted,' then the whole document would have this protective marking. Similarly, if any item were graded with a handling code of "Confidential," then the entire product would bear the same restriction. The cycle as shown in figure 2 started with the threat identification and analysis in the premise that the whole cycle is an off shoot of a new mandate or new mission. In some cases where mission is already advancing and a Crime Intelligence Unit (CIU) is already functioning, threat identification and analysis phase will in addition be integrated throughout the CIC. At a strategic level, it can also be external to the CIC where CIU is not already functioning. This process in part is the core element of ILP.

F.3. Crime and Public Safety Threat Identification and Analysis

38. UNPOL usually operates in post-conflict or pre-emptive environments, either in capacity building role and/or monitoring/executive role. Therefore, it is a practical necessity to simplify the processes in identifying, analysing, and prioritizing threats in the mission area or area of jurisdiction. This process starts with scanning of operational environment in the area which may include identifying and examining factors such as demographic characteristics (age, population size, racial and ethnic composition of population, etc.), over-all crime rate, general objectives, and strategies, and economic, and physical conditions. It is the creation of a crime intelligence knowledge product that supports decision-making in the areas of law enforcement, crime reduction, and crime prevention.[17] Processed information on criminals is used to answer the questions:

    38.1. Who poses the threat? (This response identifies and describes people in movements or ideologies who commit crimes that pose threats to safety and security of both the community as well as UN components).

    38.2. Who is doing what with whom? (This includes the identities, descriptions, and characteristics of conspirators or people who support criminals/criminal enterprises) and

    38.3. How does the criminal enterprise operate? The methodical breaking down of crime information into its component parts; the examination of each crime data to find interrelationships; and application of reasoning to determine the meaning of the information on crimes.

[17] DPO Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities, 2022.05.

39. Crime Analysis (CA) is the processed information on crimes.[18] Crime analysis includes all types of analysis performed within a police agency, except for evidence analysis and some administrative analysis related to budgeting, personnel (e.g., overtime, sick and vacation leave, salary), and equipment. Crime Intelligence is the combined product of crime analysis and criminal intelligence,[19] i.e., fusing data from crime analysis of crime patterns with that of criminal intelligence based on the criminal behavioural characteristics of individuals or groups. The focus of crime intelligence does not only focus on certain offenders (criminal intelligence) but also on occurrence of certain categories of crime (crime analysis) and thus these two concepts "used in combination, are essential to a more complete understanding of criminality necessary to formulate effective crime reduction and prevention strategies". This integrated analysis will enable the decision makers to look at the bigger picture of criminality, which will assist them to formulate more measures to effectively address identified issues and understanding the crime context of the environment offenders operate.[20]

40. On one hand, criminal intelligence can provide decision makers with a snapshot of criminal activities and criminal behaviour, i.e., give information on prolific offenders and organized crime groups, and on the other, crime analysis can provide understanding of crime patterns and trends, i.e., understanding the crime context of the environment offenders operate. In relation to this cycle, the UNPOL crime intelligence-led policing approach addresses functions of criminal threat identification and risk analysis, crime prioritization leading decision-making, resource allocation and the direction, planning and commissioning of crime intelligence products and operational activities.

41. As shown in figure 1 above there are several steps to be followed to achieve well informed operational directives through ILP. This process, which involves management tools and frameworks, will help the HOPCs and/or host-State counterparts in determining the focus of policing or law enforcement activities in their respective areas. Utilizing informed decision in policing direction increased the possibility of achieving higher efficiency and effectiveness rate in addressing policing and other law enforcement issues and concerns in mission areas. Preferably, this process will be initiated prior to any movement of police units in a policing or other law enforcement operation. However, due to the cyclical nature of crime intelligence works, this process should be revisited also after police action have been carried out. Figure 3 below explains the relationship of the UNPOL Crime Intelligence Cycle leading to Directions that initiate/feed into operational planning that constitute actions/ response by the UNPOL.

[18] International Association of Crime Analysts (IACA) definition.

[19] Ratcliffe, Jerry H. *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*. Washington, DC: Police Foundation, 2007.

[20] The result highlighted the integrated analysis model. For more information read "Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Managers" (Ratcliffe:2007).

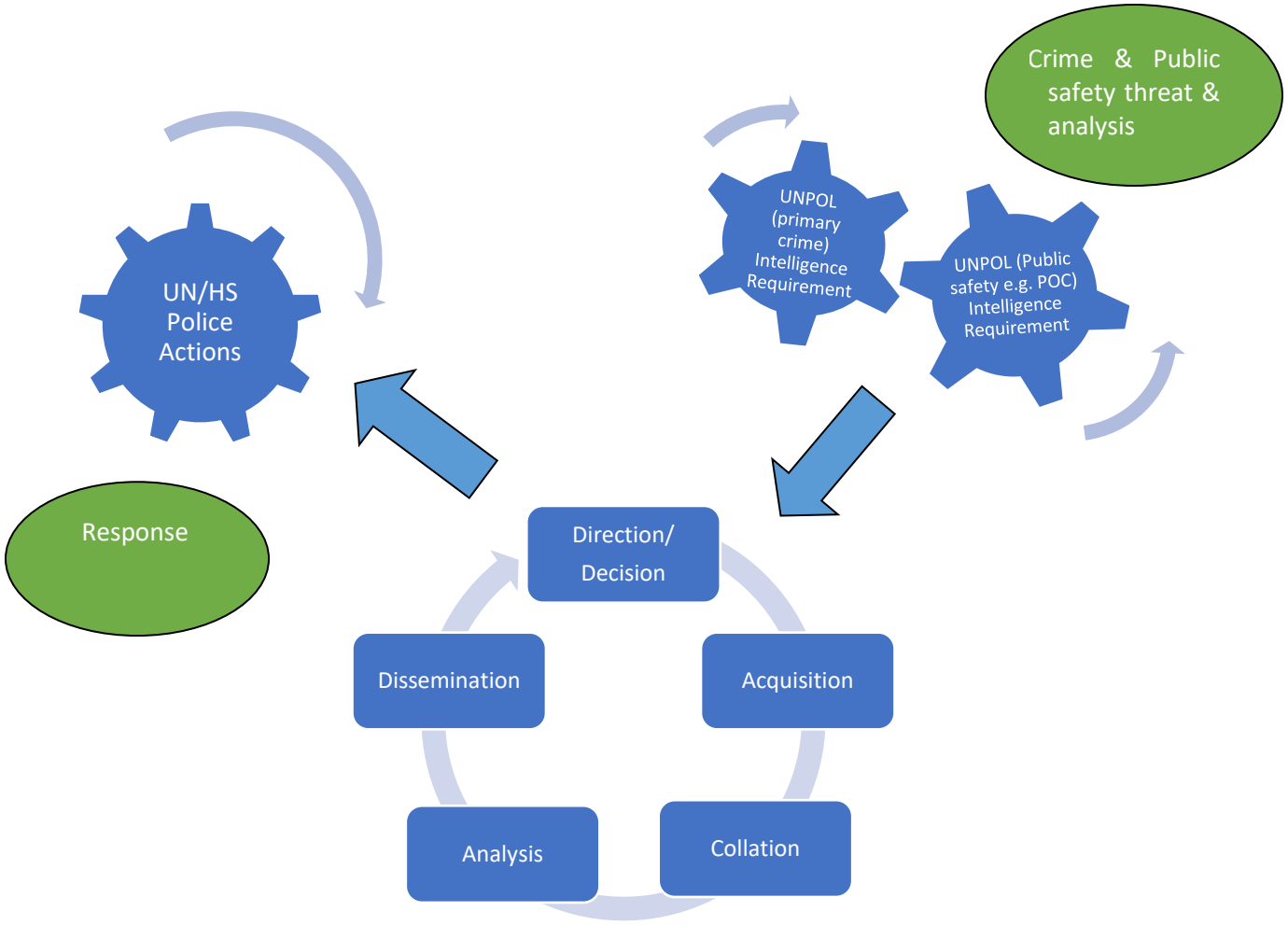

Figure 3

F.3.1. Safety risk identification and assessment:

42. The crime and public safety risk identification must be completed to get simplified information for police planning processes which aim to enhance the efficient utilization of resources in the mission or the jurisdictional area. Most of the time, UNPOL works in places where there has been an armed conflict, where technology as well as skills may not have advanced. These steps will help all those who make choices maintain their objective and make better decisions based on facts. These tasks should ideally be done by a team of senior officers and/or managers who work in strategic offices like HOPC, D/HOPC, Chief of Operations, Regional heads of UNPOL, or the host state head of police department etc. Any instructions or decisions that come out of this process will be added to the UNPOL Component's Annual Workplan, Operational Plan (OPLAN), or Operational order, as applicable. Officials with this strategic-level job will be the core group that makes plans and strategies for the crime intelligence-led police planning process in the UNPOL component. This process has following three main parts.

    a. Identifying and analysing/assessing threats,

b. Setting priorities.
c. Making decisions.

These three parts will be used to figure out the needs (crime and other public safety needs) for the main output, which is planning and direction. **Figure 4** below shows the flow of steps from threat identification and assessment to planning and finding a forward direction.

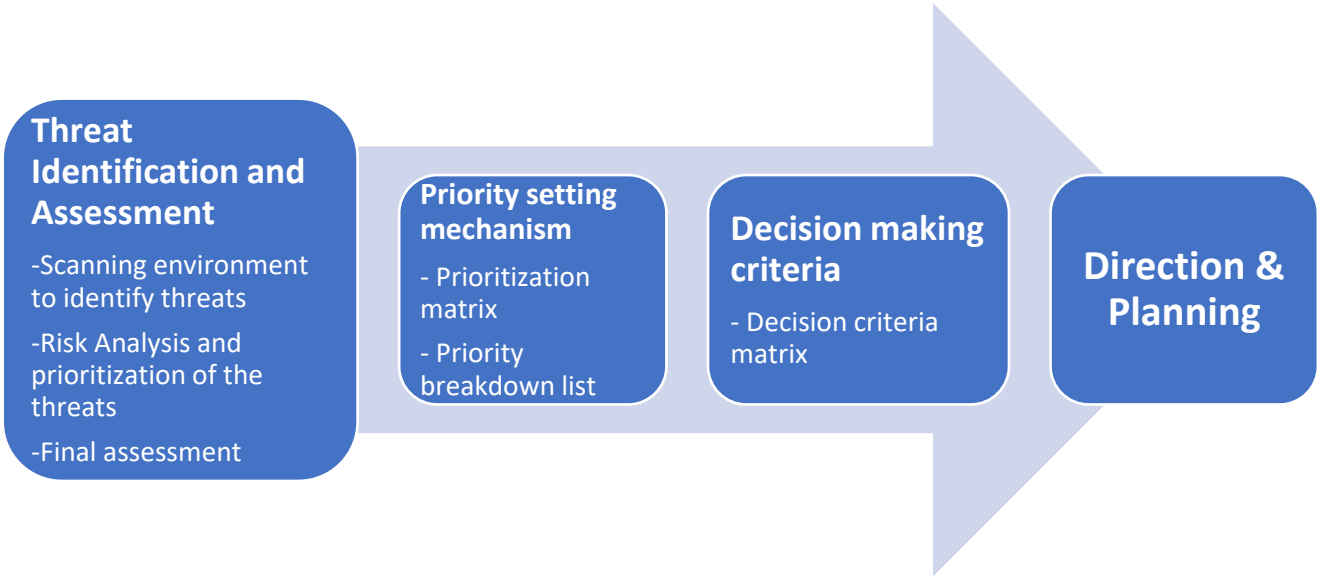

Figure 4

F.3.2. Threat Identification:

43. For all the practical purposes ILP processes in identifying, analysing, and prioritizing threats shall be simplified, keeping in mind the post conflict usual role of UNPOL where advance-level training and /or high technical equipment in crime intelligence may not be readily available. The most important is that the processes in identifying, analysing, and prioritizing threats will enable the decision makers to focus objectively in achieving informed decisions and that biases are minimized. These processes can be carried out at the mission level where the head of mission and other senior mission leadership (*see also Task and Co-ordination Group in the manual*) are involved. Further, it can be carried out as well at the CIU level (*see also Operational Review in UNPOL Crime Intelligence Manual 2025*) where any outputs of the process in identifying, analysing, and prioritizing threats can be presented before the HoPC for their decision.

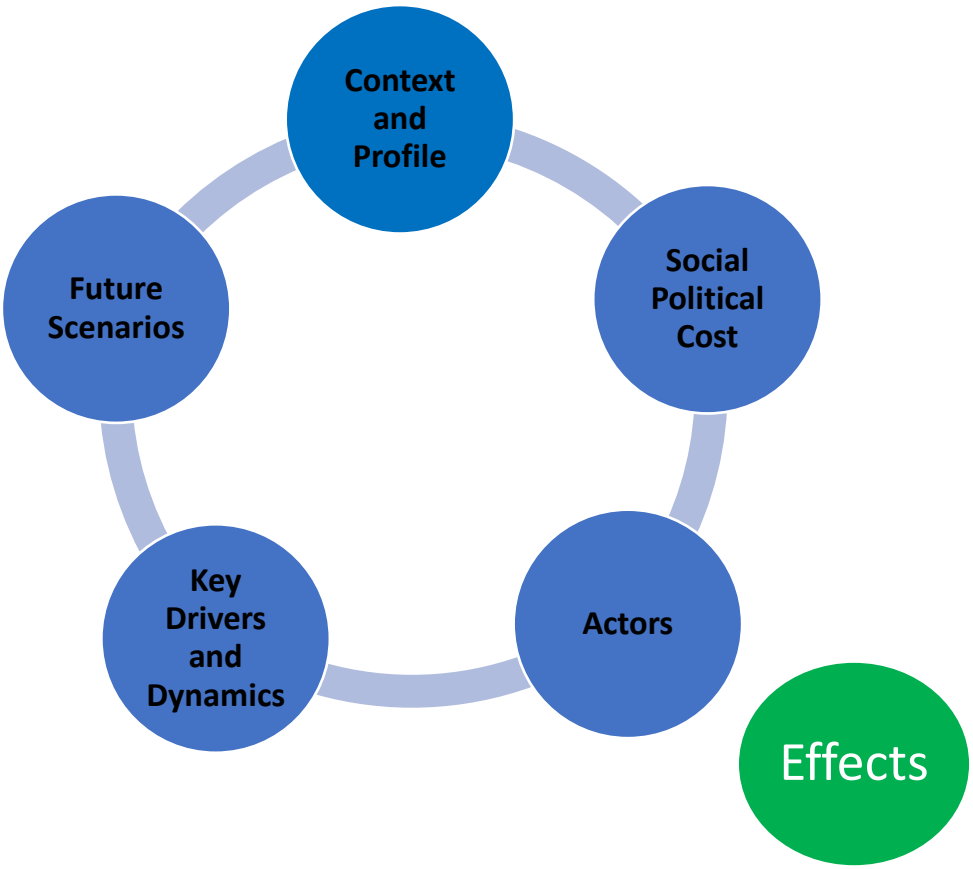

Figure 5

44. The process of threat identification as shown in figure 5, starts by scanning of operational environment on the ground which may include context, social/political causes, responsible/ identifiable actors, identifying and examining factors, key drivers & dynamics such as demographic characteristics (age, population size, racial and ethnic composition of population, etc.), over-all crime rate, general objectives and strategies, future scenarios, and economic, and physical conditions.[21] PESTEL models[22] in environmental scanning can also be effectively applied in the context of ILP to facilitate a comprehensive analysis of external factors. These environmental scanning models, if utilized in this process, shall be used more particular within the scope of policing. This shall be limited to areas in policing, other law enforcement, crime prevention, and the maintenance of peace and order.

45. The UN categories of crimes[23] can be used in cross matching the crimes and the PESTEL factors. The identified categories of crimes in the mission area will be used as the backbone of analysis to ensure detailed and focused analysis of policing and other law enforcement issues. With this approach, the analysis will link the strategic environment and the operationally categorized crimes. This process is an analysis that will determine the issues

[21] Schneider, S.R., "The Criminal Intelligence Function: Toward a Comprehensive and Normative Model."
[22] UNICEF Toolkit for SWOT and PESTEL, understanding external and internal context for better planning and decision making.
[23] International Classification of Crime for Statistical purposes (ICCS). It was adopted at the 24th session of the Commission on Crime Prevention and Criminal Justice in May 2015.

and concerns within the operational environment and how it may affect the organization, which in our case is the peacekeeping/special political operations and/or the host-State police organization. This analysis will focus on cross matching the PESTEL factors with that of policing and other law enforcement issues and concerns in each mission area to come up with the overall law enforcement and policing picture that may spell out its threat to the peace operations.

46. The policing and other law enforcement issues and concerns of UN mission/host State under review shall be put in the context and terms used in the UN categories of crimes, which is part of the 2030 Sustainable Development Goals. The identified categories of crimes will be used as a simplified example of analysing topmost threats in mission areas utilizing PESTEL[24] and labelling it according to its impact with the PESTEL factors is shown below in Table 1. Impacts can be based on the number of occurrences of crimes in mission areas. It should be noted that other types or tools in analysing threats can be utilized as well in this process.

47. The backbone of analysis to ensure detailed and focused analysis to policing and other law enforcement matters. With this approach, the analysis will now link the strategic environment and the operationally categorized crimes.

Table 1: Simplified example of analysing topmost threats in mission areas utilizing PESTEL

Prevalent policing and other law enforcement issues and concerns of UN Mission in Country X (Category of crime)	Impact to						
	Political Stability	National Economy	Socio-cultural	Technology	Environment preservation	International laws/Host state laws	Total value
Violence against person – with death or attempt	No	Yes	Yes	No	No	No	2
Violence against person and property crime	No	Yes	Yes	No	Yes	No	3
Threat against person and property crime	No	Yes	Yes	Yes	No	No	3
Drug offense	No	Yes	Yes	No	No	Yes	3
Financial crimes	Yes	Yes	Yes	Yes	No	No	4
Public violence	Yes	Yes	Yes	No	No	Yes	4
Acts against state security	Yes	Yes	Yes	No	No	Yes	4
Terrorism	Yes	Yes	Yes	Yes	No	Yes	5
Serious and organized crime (SOC)	Yes	Yes	Yes	Yes	No	Yes	5
Cross-border crimes	Yes	Yes	Yes	Yes	Yes	Yes	6
Environmental crime	No	Yes	Yes	No	Yes	Yes	4
Acts under universal jurisdiction	Yes	Yes	Yes	No	No	Yes	4

Note: Yes = 1; No = 0

[24] PESTEL is used in this analysis to give emphasis also to the Environmental factors in the analysis.

F.3.3. Threat Assessment:

48. Following are the guide questions in filling the matrix:

    48.1. What are the crimes or policing, and other law enforcement issues and concerns prevalent in the mission area that are included in the list of the UN categorized crimes?

    48.2. Do the level of crimes or policing and other law enforcement issues and concerns (e.g., violence against person involving death or attempt) strategically negatively impacted the country's political stability national economy, socio-cultural norms, technology, environment preservation and legal implementation negatively?

    48.3. Are there any crimes or policing and other law enforcement issues and concerns prevalent in the mission area not listed in the UN categorized crimes list? How do they impact the mission area and/or country?

49. The categories of crimes mentioned in the matrix (Table.1) and their impact on the enumerated factors in the columns are shown here as a model example. *HoPC/Chief CIU may issue mission specific SOPs to fill in the table, as per their mandated priorities and collective wisdom. This also implies to the later matrices of risk and harm analysis.*

The UN defines Early Warning as: "The provision of timely and effective information, through identifying institutions, that allow individuals exposed to a hazard to take action to avoid or reduce their risk and prepare for effective response" (ISDR, 2003).

F.3.4. Early Warning and Indicators:

50. Threat identification/assessment and early warning systems are closely interconnected, with threat assessment serving as one of the foundations upon which early warning and indicators are built. Early warning systems are intended to empower decision makers of police components in peacekeeping operations against risks towards host populations they are serving and to act in a timely way, proportionately to reduce the likelihood of personal injury, loss of life and damage to property and the environment.

51. Early warning systems need to have a strong focus on the people exposed to risk, and with a systems approach that incorporates all relevant factors in that risk, whether arising from armed conflicts or social vulnerabilities.

52. An effective early warning system comprises four inter-related elements: (1) risk knowledge, (2) monitoring and warning service, (3) dissemination and communication and (4) response capability.

    52.1. Risk Knowledge: Risks arise from the combination of threats and vulnerabilities at a specific location. Assessments of risk require systematic acquisition and analysis of data. Risk assessments and maps help to prioritise early warning system and guide preparations for prevention, intervention, and mitigation.

52.2. Monitoring and Warning Service: There must be a sound scientific basis for predicting and forecasting threats. Continuous monitoring of threats indicators is essential to generate accurate warnings in a timely manner. Likely questions to be considered during this phase would be: (1) What patterns of activity do we normally associate with the activity we are monitoring? (2) What events normally take place before this activity? (3) What would you expect to see happening? And (4) In what order do these activities normally take place?

52.3. Dissemination and Communication: Warnings must reach those at risk in a timely manner. Clear messages containing simple, useful information are critical to enable proper responses that will help safeguard lives and livelihoods. The use of pre-set communication channels is necessary to ensure that the right officials in a position to consider and act upon the warnings are informed.

52.4. Response Capability: It is essential that threat management plans are in place, well-practiced and tested. The community should be well informed on options for safe behaviour, available escape routes, and how best to avoid damage and loss to property.

F.3.5. Risk Analysis

53. Risk analysis in the context of Intelligence-Led Policing (ILP) is the systematic process of identifying, evaluating, and prioritizing potential threats and vulnerabilities to inform strategic and tactical decision-making within law enforcement agencies. It involves the analysis of intelligence data to predict and mitigate potential criminal activities, allocate resources efficiently, and enhance public safety. Risk analysis or risk assessment is crucial because it shifts the focus of policing from reactive, incident-driven responses to proactive, intelligence-driven strategies. Here is how it fits into the broader ILP framework:

53.1. **Strategic Decision-Making**: Risk assessments inform strategic planning by identifying long-term trends and potential threats. This helps law enforcement agencies develop comprehensive plans to prevent crime and ensure public safety.

53.2. **Operational Efficiency:** By assessing risks, agencies can allocate resources more effectively, ensuring that limited personnel and funding are directed toward areas where they will have the most significant impact.

53.3. **Targeted Interventions**: Instead of using a blanket approach to crime prevention, risk assessments enable law enforcement to focus on specific individuals, groups, or locations that present the highest risk.

53.4. **Enhancing Community Trust:** By proactively addressing risks and vulnerabilities, law enforcement can build stronger relationships with the community, reducing crime rates and increasing public trust.

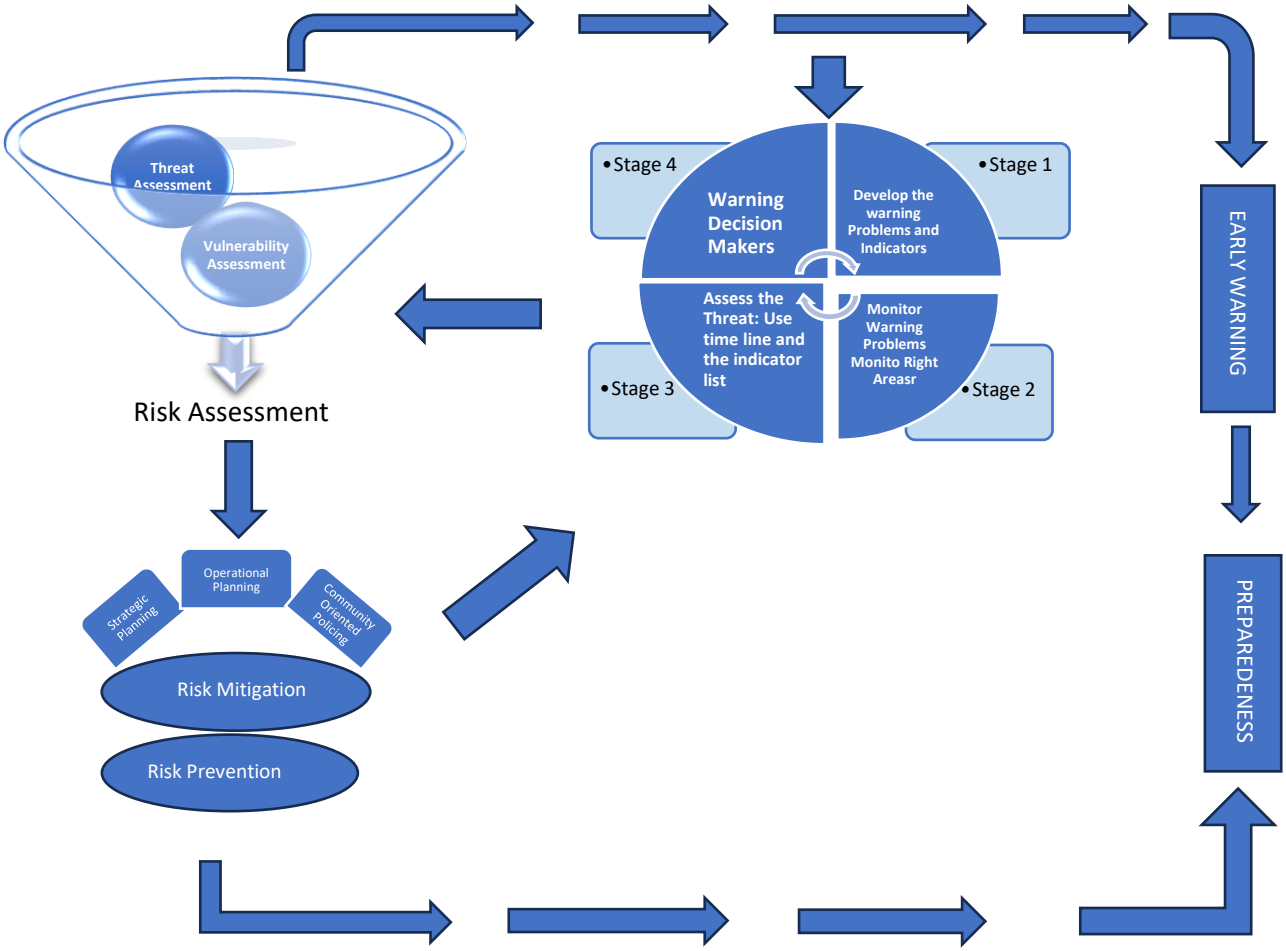

Figure 6 Risk Analysis

54. Risk assessment is an integral part of Intelligence-Led Policing, providing law enforcement agencies with the necessary insights to proactively address threats and improve the effectiveness of their operations. By focusing on data-driven analysis, it ensures that police resources are used efficiently to protect communities and prevent crime before it happens. The eight highest valued crime issues and concerns (highlighted in Table 1) as identified will be put into the Risk Analysis Matrix (Figure 6) accordingly.

F.3.6. Harm Analysis:

55. Harm analysis matrix (figure 7) is a tool that will help UNPOL strategize which category of crime has higher implication to the overall policing operation with due respect to some factors associated with maintaining the stability of the country and/or mission. In this example as shown in figure 7, the criteria being used in assessing the harm in peacekeeping operation are the level of violence and monetary value of losses vis-à-vis actual occurrences and affectation of the crime according to its category. Harm analysis matrix is divided into four boxes:

55.1. Box Number 1 - lists of crimes or law enforcement concerns with high level of violence and low value of losses (economic). This falls between Box 4 (highest)[25] and Box 2 (lowest).

55.2. Box Number 2 - lists of crimes and law enforcement concerns with lowest posed risk, i.e., low violence and low economic loss.

55.3. Box Number 3 - lists of crimes or law enforcement concerns with low level of violence and high value of losses (economic). This falls between Box 4 (highest) and Box 2 (lowest).

55.4. Box Number 4 - lists of crimes or policing and other law enforcement concerns with highest posed harm, i.e., high violence and high value of losses (economic).

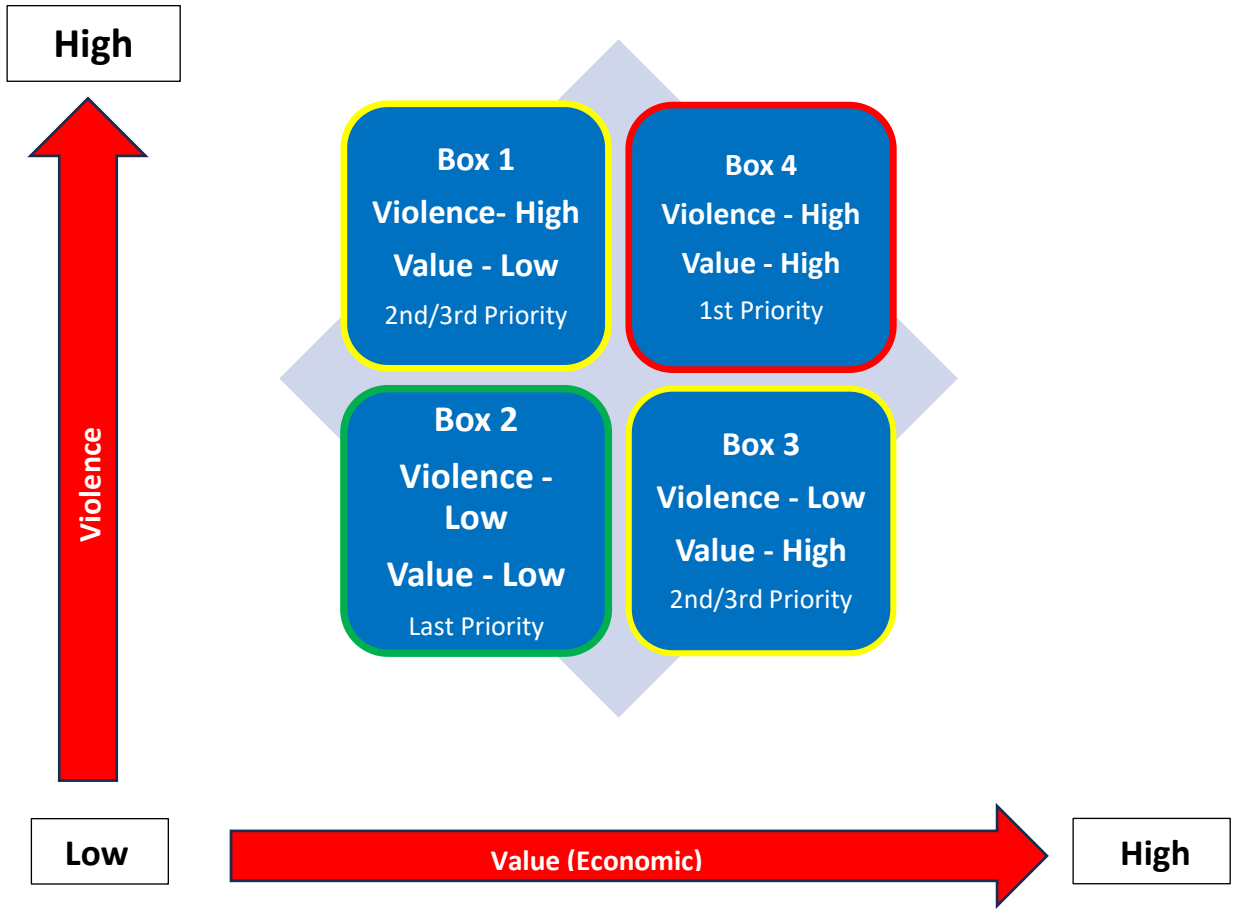

Figure 7 Harm analysis matrix

56. **Figure 8** below is an example of Harm Analysis Matrix with "filled-in" categories of crimes respective to harm priority. It should be noted in this example that all eight categories of crimes

[25] NOTE: It will be decided by the Team, which of the Boxes between 1 and 3 has the higher harm over another, according to ground situation.

(*based on the data from table 1 above*) were given equal status i.e., no weights or values, once subjected into the Harm Analysis Matrix. Again, the "filling-up" of these boxes are based on the crimes or categories of crimes' posed future risks, actual occurrences (historical data) and affectation with respect to the criteria used.

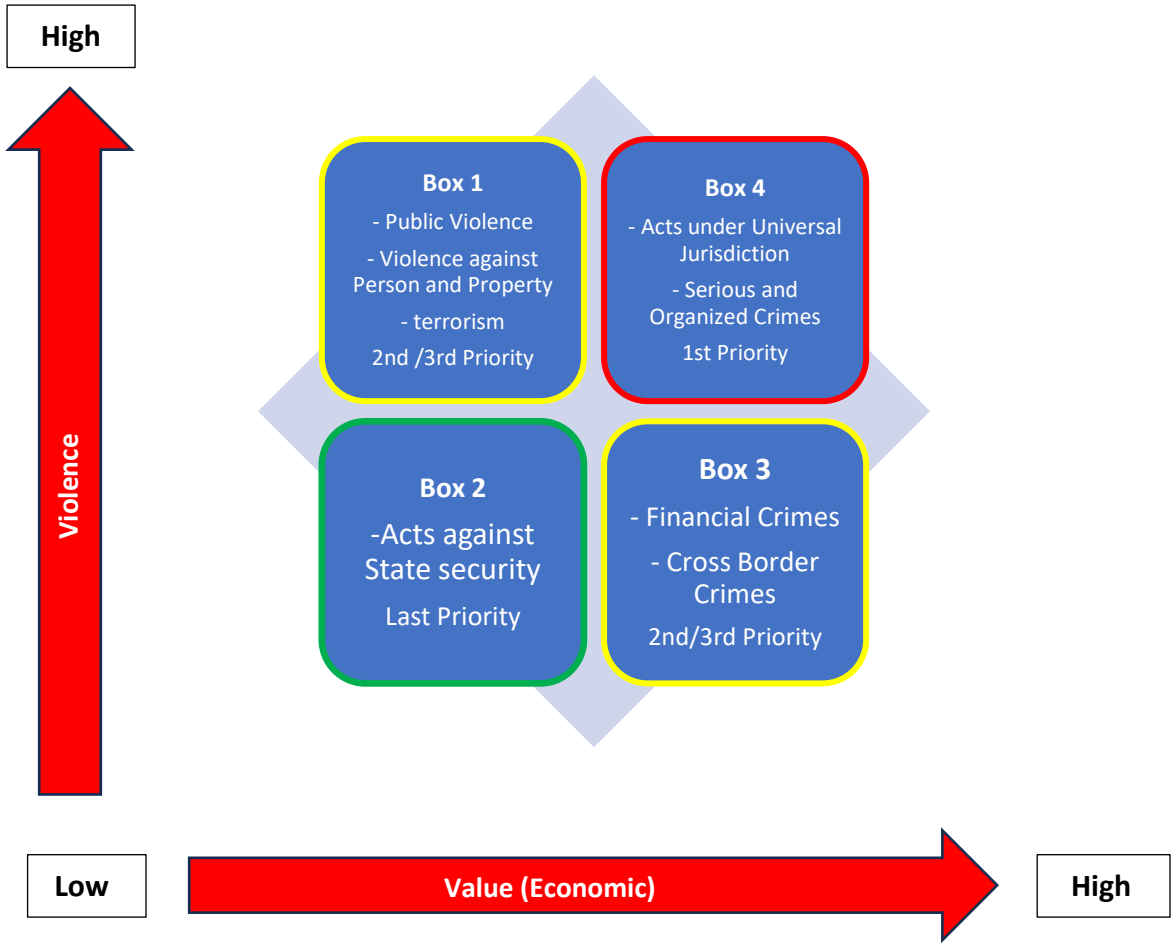

Figure 8 Categories of crimes respective to harm priority matrix

F.3.7. Prioritization of Threats:

57. In continuation of the above example (see figure 8), all categories of crimes listed in the boxes are broken down into hierarchical order based on the priority of boxes with the assumption that it was decided by the Team that Box 3 will be the 2nd priority and Box 1 will be the 3rd priority. Thus:

- Box 4 – highest priority
- Box 3 – second highest priority
- Box 1 – third priority
- Box 2 – last priority

**Note*: Categories of crime respective to harm priority is illustrated as an example which can be altered as per the recommendation of the Chief CIU in consultation with HoPC.

58. The priority list below in **table 2** is based upon the above-described *Harm Prioritization Matrix*

Table 2: Sample Prioritization matrix *(based on Figure 8 data*)

	Country X Categories of Crimes Priority List	*Based on priority box number*
1	Serious Organized Crimes	4
2	Acts under Universal Jurisdiction	4
3	Financial Crimes	3
4	Cross Border Crimes	3
5	Terrorism	1
6	Public Violence	1
7	Violence against person and property	1
8	Acts against state security	2

59. The priority list shall be trimmed down for simplicity and ease from excessive and/or irrelevant analysis. It is preferred to use *only two of the four boxes* to avoid complex analysis. In this example, the first (Box 4) and second priority (Box 3) categories of crimes are being used for decision making (see Table 2). In this case, the team only lifted the top four crimes in the priority list. These crimes or policing and other law enforcement issues and concerns will now be cross matched with criteria/factors[26] that the team had decided to use in processing their decision.

F.3.8. Decision Making:

60. Prioritization in terms of decision-making is deciding the sequence of priority in which the crimes will be dealt with first. Other tools (e.g. Pareto Analysis[27], Grid analysis, Decision trees, etc.) can be utilized as well to arrive at the needed decision. It is important to note that decision making can be achieved as well by using very sophisticated tools and models as applied in practices[28]. However, in a typical post-conflict environment where UN Peacekeeping mission operates, the luxury of utilizing these tools and concept may not be practicable.

61. Table 3 below is an example of a simplified decision-making tool that can be applied in mission areas. It illustrates how the list (derived from the table 2 above) is subjected into a decision criteria matrix in relation to the operating environment of the mission area. A “remarks” column has been added to put relevant qualitative information that can be useful in reaching the final decision. In the example, values (1 for Yes and zero for No) are also assigned to the relevant responses regarding crimes in the operational environment of a mission area. The more these values accumulate, the higher the probability that the crime or category of crime becomes the highest priority, taking into consideration specific factors and associated information.

[26] Criteria are subject to the domestic operating environment. This shall be decided by the Team on what will be the criteria. The criteria can be the result of SWOT Analysis, Force field Analysis, Stakeholder Analysis etc.

[27] Vilfredo Pareto 1896 book, "Cours d'économie politique."

[28] Turpin, S.M., Decision-making: Theory and practice, 2004.

Table 3: *Decision Criteria Matrix vis-à-vis operating environment (derived from table 2)*

Country X Categories of Crimes Priority List	*Politically Feasible*	*Organizational Capability to Required Resources*	*Capacity of domestic experts to process/investigate*	*Actions may take beyond territorial sovereignty*	*Total*	*Remarks*
1) Serious Organized Crimes	No	Yes	Yes	Yes	3	*Confirmed involvement of some rebel group in organized crimes that are signatories to the peace process*
2) Acts under Universal Jurisdiction	Yes	Yes	Yes	No	3	
3) Financial Crimes	Yes	Yes	No	No	2	
4) Cross Border Crimes	Yes	Yes	Yes	Yes	3	*Some crimes perpetrated within boundaries*

62. For the purposes of this exercise, it is assumed that the team reached the conclusion that the highest priority category of crime (Serious and Organized Crime), as displayed in the table 3 above be endorsed to appropriate entity[29] due to the political implication it may have upon the existing peace accord. As a result, the Priority No. 2 (Acts under Universal Jurisdiction) will now become the most prioritized category of crime since it reflects the highest cumulative value. It will be followed by cross-border crimes and financial crimes in the list of priority.

63. Now that the team has identified crimes or law enforcement issues that needs to be addressed first, i.e., topmost priority, the process of boiling down these categories of crimes to specific actionable decision for direction shall begin, resulting into breaking down the categories of crime according to the affiliation and/or crime personalities. Before going to the next process, it is at this stage that the team will determine if there are evidence-based pieces of information available from the ground that will identify any criminal groups, affiliations and individuals that are perpetrating these crimes including other information relevant to their overall criminal activities. If evidence-based information is not available (therefore presence of intelligence gap) then the focus should be on gathering more information in this gap before proceeding to the next process. If, during the process, the Team receives information that priority subject may have implication upon the peace process (if it is existent in the country or mission area) then the team should refocus its directive to the second-most priority.

64. In the case that information on the identity and activities of criminal groups is available, the analytical process will continue (see succeeding paragraph) on itemizing all information to

[29] The HoPC may also endorse the findings to his/her or first reporting officer or immediate supervisor.

achieve a more detailed list that can be used for direction. To continue with our example above, the team will list or populate the Decision Matrix (see Table 5) with all the identified groups or individuals that are reportedly known to be involved in the most prioritized crime or category of crimes, i.e., acts under universal jurisdiction, which the team had identified throughout the process.

65. The Team should also where possible elaborate the specific crimes committed by these groups or individuals and further rank them according to the harm they have done as reflected in their respective criminal history and their capacity in recent months. Harm committed by a criminal or criminal group shall be based on the harm classification[30] as defined below:

Table 4: Type of Harm, its definition, and examples

Harm Type	Harm Definition	Examples
Social	Negative physical, psychological, or emotional consequences cannot be readily expressed in cash terms	Homicide, rape, injury, intimidation, and assaults
Economic	Negative effects on an individual, community, business, institution, government, or country; can be readily expressed in cash terms.	Theft, loss of business because of counterfeiting. Complicity of associated business, unfair competition
Political	Negative effects on the political stability of a community, institution, region, or country	Corruption, loss of confidence in government, or diminished vie of effectiveness of law enforcement or government
Cultural	Negative effects on cultural heritage, social norms, cultural and social values.	Destroying places of worship, historical sites, imposing unacceptable practices for day-to-day life in a society.
Indirect	Secondary adverse consequence of criminal activity	Environmental damage from clandestine drug laboratory or marijuana grows operation waste

66. Table 5 below is an example on how the criminal group/individual are ranked according to the harm they caused and their level of operability/activities in the last 6 months, i.e., most harmful group will be ranked 1 and so on, and the most active group will be ranked 1 and so on. The group/individual with *lowest cumulative total* will be the *first or topmost priority.*

[30] Based on the definition of "Harm" by the London Metropolitan Police Service in UK as mentioned in Criminal Intelligence Service Canada: Integrated Threat Assessment Methodology (2007).

Table 5: Decision Matrix vis-à-vis specific criminal group/individual (as subsequent exploration from table 3)

Category of Crime	Criminal Group/	Specific Type of Criminal Activity/ies committed	Harm done[31]					Most Active in last 6 months	Cumulative rank
			Social	Economic	Political	Cultural	Indirect		
Acts under Universal Jurisdiction	A	Torture, recruitment and use of children, property (village burning) intentionally directing attacks against civilian population	1	2	4	1	1	4	13
	B	Recruitment and use of children, taking of hostages, extensive destruction of (private and public places)	2	4	1	4	4	2	17
	C	Piracy, attacks against personnel involved in a humanitarian assistance or peacekeeping mission, recruitment, and use of children	3	1	2	1	2	1	10
	D	Torture, attacks against personnel involved in a humanitarian assistance or peacekeeping mission	4	3	3	3	3	3	19

67. The result of table 5 above shows that criminal perpetrator/s C (groups/individual) has the least cumulative total of all according to the harm they done and their level of operations in the last 6 months. This Decision Matrix result can be used as:

    67.1. Main subject of the UNPOL/Crime Intelligence Requirement

    67.2. Basis for the UNPOL leadership in deciding where to focus the resources on its policing operations and gathering sufficient pieces of evidence that could lead to the arrest and neutralization of the prioritized group leaders and members.

    67.3. Basis for directing new policing strategies in the mission policing operations (e.g., patrolling, community policing).

F.3.9. Direction and Planning

[31] Based on the definition of "Harm" by the London Metropolitan Police Service in UK as mentioned in Criminal Intelligence Service Canada: Integrated Threat Assessment Methodology (2007).

68. In terms of crime intelligence related to UNPOL's mandate implementation, a clear direction is needed from UNPOL managers, usually the Tasking and Coordination Group, following threat identification and analysis. Direction outlines the UNPOL Senior leadership requirements and provides a clear focus for the operational/ tactical level UNPOL officers involved in the acquisition of crime intelligence within the peacekeeping context.

69. Direction and planning include the processes of elaboration of Crime Intelligence Requirements (CIR), providing instructions/ requests to subordinate units and maintaining and oversight of the Crime Intelligence assets. Direction and planning are applicable at both the strategic as well as operational/ tactical levels and requires consistent overview to refine the acquisition strategy. Direction can be the initiating stage of the Crime Intelligence Cycle or operational planning and response to public security threats. Effective direction ensures that the crime intelligence effort is appropriately prioritised and aligned to organisational mandates, strategies, and objectives (See Figure 9).

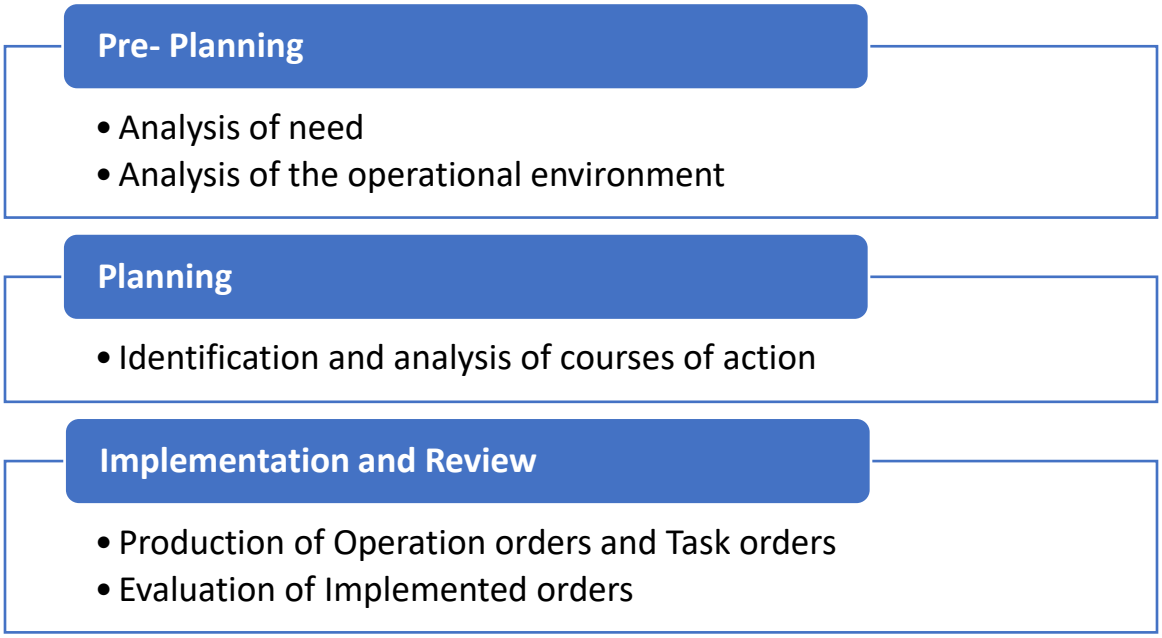

Figure 9 Direction and Planning

F.4. Tasking and Coordination

70. Tasking and coordination are undertaken at two levels – Strategic and tactical. UNPOL managers make decisions at strategic and operational/tactical levels. These decisions are operationalised through tasking and coordination. To enable UNPOL managers to prioritise the deployment of resources, decisions should be based on a thorough understanding of the situation and the associated problems. While strategic tasking and coordination, associated with crime Intelligence-led policing, is part of police governance and planning, operational/ tactical tasking on the other hand is about police operational response, including agreeing on tactical/ operational options and aligning resources to priorities.

71. In a peace mission scenario, the Mission Tasking and Co-ordination Group (TCG) is ideally composed of senior mission leadership (e.g. SRSG, deputy SRSG) and other strategically positioned managers or commanders (e.g. UNDSS chief, HoMC, HoPC) including the Chiefs of CIU, JOC and JMAC as members. Whereas special political missions and non-mission settings will have a TCG composition in line with their strategic, tactical, and operational leadership. TCG shall hold quarterly meetings purposely for operational and strategic assessment and decision making. INTERPOL's representatives or liaisons, when available, may be invited as advisors or contributors to TCG meetings. Their insights into international crime trends and access to real-time global crime data can inform strategic assessments and aid in prioritizing transnational crime threats.

72. TCG's primary role is to consider identified threats in the mission/jurisdictional area and to collectively agree which of the threats shall be prioritized to be addressed. These priorities are part of the Control Strategy which is produced from a strategic assessment. Further, TCG also sanctions recommendations e.g., Peacekeeping-Intelligence Requirements (IRs), Crime intelligence Requirements (CIRs), to the Mission Peacekeeping-Intelligence Coordination Mechanism (MICM), which is responsible for overseeing the development of and validating the Mission Peacekeeping-Intelligence Acquisition Plan (MIAP).

73. MICM structure is composed of the participating mission entities responsible for the acquisition, collation, analysis, and dissemination of information with the role of meeting the objectives of peacekeeping-intelligence activities in the mission, i.e., the JMAC, Military and Police Components, and UNDSS. The JOC should also be a permanent member of the structure in its function as the mission information manager and thus facilitator of the peacekeeping-intelligence cycle. Other mission entities such as Legal Office of the mission, Political Affairs Division, Civil Affairs Division, Human Rights Component, etc may be invited to participate on a permanent or ad hoc basis in the MICM.[32] Some Missions may wish to consider including INTERPOL into the MICM, as their information-sharing framework can strengthen the acquisition and analysis of transnational crime data. INTERPOL's tools, such as I-24/7, and its Notices system, can be leveraged to ensure seamless information flow between international and mission-specific entities, enhancing the peacekeeping-intelligence cycle.

F.5. Control Strategy:

74. Control strategy forms the outline for strategic policing and other law enforcement (if applicable) priorities as the result of threat and other strategic-level assessments (e.g., criminal threat assessment), risk analysis and prioritisation process within the ILP-process. It is implemented by the UNPOL component mission-wide for six months and will be reviewed and amended, if necessary, by the TCG after this period. This strategy sets out and communicates the operational priorities for the UNPOL and sets the long-term priorities for crime prevention, crime intelligence and capacity-building and development. It may also include reassurance opportunities and provides senior leaders with a framework to enable them to implement decisions on prioritizing the allocation of resources. The control strategy is located at the strategic levels of the UNPOL workplan and will not necessarily capture every issue. The content of the control strategy must be set at the Strategic Tasking and Coordination Group (TCG) and should be determined by a prioritization process – including on the allocation of resources. Each priority has an owner who is responsible for its delivery plan, and the priority should be communicated to appropriate staff and partners. The role of

[32] DPO Policy on Peacekeeping-Intelligence 2019.08, pg. 10.

the CIU is to ensure the delivery of the crime intelligence functions within the control strategy. The crime intelligence priorities stipulated in the control strategy are the basis of the IR and/or CIR, which directs the information acquisition activities relevant to the policing and other law enforcement issues that are described in the control strategy.

F.6. Strategic Risk Assessment Review (STRAR):

75. There shall be a STRAR Team, which is normally composed of UNPOL senior management[33] with CIU Chief and Chief of UNPOL Investigation Unit (position is subject to mission mandate), as members. The frequency of these meeting is monthly (operational matters) and quarterly (strategic matters).

76. STRAR team shall monitoring and review the existing crime intelligence projects and progress of the tasks detailed to Police Component by the TCG (Monthly). Progress of existing crime intelligence projects and policing activities in response to previously identified criminal threats will be discussed during CTR meetings. Issues and problems as recognized during the implementation of these project/ activities should be discussed as well to determine alternative solutions. Additionally, all directives and tasks specified by the TCG to the police component shall be reviewed in detail to determine its accomplishment vis-à-vis goals and time frame given.

77. STRAR team shall sanction new projects/measures to address new criminal threats (Quarterly). The process starts with identified emerging new criminal threats by the CIU which should be presented during the meeting. The discussion may include validation from other UNPOL sources. If the likelihood of threat is high and intervention is deemed necessary, the UNPOL management will issue directives to address the threat. These directives may include the following:

    77.1. Crime Threat Assessment Report to the mission leadership.

    77.2. Crime intelligence Requirement/s for CIU on emerging crime threats not included in the control strategy.

    77.3. Directives for administrative and logistical support.

    77.4. Guidelines for new policing activities or tasks.

78. STRAR team shall do closure and evaluation of crime intelligence projects/activities (Quarterly). Part of objectives of Quarterly Criminal Threat Review is to determine if the goals of existing crime intelligence projects/activities have been achieved already and thus requires eventual closure. For each crime intelligence project an evaluation shall be carried out to know if the objectives of the project have been achieved. This also includes re-examining the mechanisms, processes and tools utilized in the production of crime intelligence to achieve its objectives. The review and evaluation shall be designed in a way that it will capture the good practices employed in the crime intelligence production/project including determining the lessons learned from it that can be replicated in future undertakings.

[33] The membership shall be identified by the Head of the Police Component to ensure responsiveness to mission UNPOL structure. However, Chiefs of CIU, Chief of Gender Unit and Investigation Unit are required members. Women representation should be ensured by HoPC in his/her membership selection.

F.7. Crime Type mapping (profiling):

79. Crime Type Mapping (CTM) is a process/tool that will help visualize crime type, crime patterns and crime occurrences in mission areas. It evolved throughout the years from using simple pins and markings to complex computer-based programs that can be filtered whatever an analyst or user wanted to determine. Crime mapping may not be feasible in mission areas due to its disadvantageous operational situation (e.g. Physical infrastructure, technology, limited/no access to crime data) not to mention the limited capacity of UNPOL in crime mapping generation and analysis. However, it will significantly enhance crime intelligence analysis processes if implemented in the mission area. Therefore, it is highly encouraged that the Chief, CIU will facilitate training and equipage of Crime Mapping Technology via Unite Aware SAGE i.e., Geographical Information System, into the main CIU analytical processes.

80. The least that can be done in the absence of modern technology on crime mapping is to create basic physical maps with pins and colours that describe current crime types, crime patterns, crime occurrences and hot spots within the mission geographical boundaries. It is best that the crime type map will also feature information on sociological, demographic, geographic, environmental, and economic factors[34] vis-à-vis crimes committed and crime occurrences.

81. Manual crime pin mapping has disadvantages. The most obvious is that it is difficult to keep updated since it can only display limited amount of information, and it will become more complex and unreadable once old pins are not taken off once updated. Thus, it is practicable to remove the crime pins or hot spot pins in updating the map. But this will likely lead to another problem of comparing the developments of crime map between time periods i.e., previous months versus present month.[35] This can be addressed by taking photographs of every updated map and store it accordingly. Additionally, a computer map using open sources (e.g., google map) can be used as well but it is less effective than manual pin mapping.[36]

F.8. Criminal Group Mapping (CGM):

82. CGM shall focus on the modus operandi, organization spans, criminal behavioural patterns, crimes committed, span of operations, criminal network associations, harm done, and economic losses caused of organized criminal groups.[37] It can be spread out in a map as well to know the criminal group/s areas of operations and their possible linkages with other groups (although this can be done also in association matrix). However, this map shall be exclusive from crime type map because the manual combination of CTM and CGM can cause difficulty in analysis due to complexity.

83. CGM offers strong representation of the crime intelligence gathered on criminal groups through collaboration from other UN personnel and external partners. It may also provide preventive measures for crimes that the criminal group/s committed. CGM may also

[34] Michael, "Crime Analysis: The History and Development of a Discipline" (2013). Honors Senior Theses/Projects. Paper 77.
[35] Boba, Rachel, “Introductory Guide to Crime Analysis and Mapping", 2001.
[36] Ibid
[37] Ibid

elaborate the most prolific criminal group/s where UNPOL leadership may take cognizance in planning resource allocation.

84. In line with the quarterly STRAR all CGM's must be reviewed to establish if they still pose the same threat as previously assessed.

F.9. DATA STORAGE, SECURITY, AND HANDLING

85. To ensure data management, security and handling on crime intelligence products and relevant documents in mission areas, following should be adopted:

85.1. Data should be stored and shared in a secure manner, ensuring proper access for those who require it for decision-making and operational planning.

85.2. Policy of clear desk should be adopted.

85.3. UNPOL 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 crime intelligence system.

85.4. Confidential crime intelligence products shall be shared and disseminated based on 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.

85.5. While disseminating it shall be mandatory that a written delegation of authority from the originator or staff member who originally applied the classification level is acquired. It implies that peacekeeping-intelligence is only disclosed to trusted individuals to ensure that it is not widely disseminated, where disclosure is likely to endanger the safety or security of any individual or group, violate rights or invade privacy.

85.6. The human rights due diligence policy (HRDDP) is applicable when UNPOL shares information or intelligence with non-UN security forces, including civilian authorities directly responsible for such forces. Prior to sharing of information with non-UN security forces, UNPOL in collaboration with the human rights component (or OHCHR presence, as relevant) must conduct a human rights risk assessment and adopt adequate mitigation measures.[38]

G. ROLES AND RESPONSIBILITIES

86. The main tasking Authority (TA) for crime intelligence unit is the senior police leadership (HoPC and D/HoPC) and other strategically positioned managers or commanders (e.g., UNPOL Chief of Operations, Chief of Capacity-Building and Development, Chief of CIU, and as needed UNPOL Sector Commander/s, including the Chiefs of JOC and JMAC as members). The Chief of crime intelligence unit is best positioned to understand the

[38] DPO Policy on Peacekeeping-Intelligence 2019.08, pg12.

capabilities of its assets and, as such, to generate and deconflict crime intelligence requirements.

87. This TA (e.g., TCG in peacekeeping missions) shall hold periodic meetings purposely for tactical/operational assessment and decision making.

88. The TA primary role is to consider identified crime threats in the mission area and to decide collectively which of the criminal threats/elements shall be prioritized to be addressed.

89. Further, the TA also makes policy and resource decisions based on analytical reports and recommendations – especially hypothesis and inferences - from the CIU. In addition, the TA also issues instructions on what crime intelligence is required and where the focus of proactive policing activities will be based on assessments and evaluations undertaken following a CIR process.

90. The TA functions can also be cascaded from requirements identified by the Mission Peacekeeping-Intelligence Coordination Mechanism [39] whose functions and roles are defined in the DPO Policy on Peacekeeping-Intelligence. In SPMs and in non-mission settings the similar coordination mechanism will assume these functions accordingly.

91. The management of crime intelligence is arguably the most important part of the CIU. If the reporting, sanitization, and dissemination of the crime intelligence is not managed correctly, then it cannot be used optimally. And in some instances, it can be counterproductive.

92. The management of crime intelligence is generally carried out by the Chief/Deputy-Chief CIU who will manage the flow and quality of crime intelligence in and out of the unit. An alternative officer shall also be designated from within the CIU to act as a substitute when exceptional circumstances arise. All information, crime intelligence and work requests shall pass through the desk including the release of crime intelligence as requested.

H. TERMS AND DEFINITIONS

Advising: A process of working together with the host-State police organization to find solutions to its problems and to improve its performance.

Analysis: The methodical breaking down of information into its component parts and the examination of each to find interrelationships.

Assessment: Process of evaluating strategic, operational, and tactical impacts of a crime group or a criminal activity on a jurisdiction, now or in the future. Threat assessments, vulnerability assessments, or risk assessments are some examples.

Capacity: Aptitudes, resources, relationships and facilitating conditions necessary to act effectively to achieve some intended purpose.

[39] DPO Policy on Peacekeeping-Intelligence 2019.08, MICM details of functions and membership.

Capacity-building: Efforts to strengthen the aptitudes, resources, relationships and facilitating conditions necessary to act effectively to achieve an intended purpose. Capacity-building targets individuals, institutions, and their enabling environment.

Collation: —The process whereby information is grouped and recorded in a manner that allows it to be readily accessible and traceable when required, and which allows easy comparison, evaluation, assessment, and retrieval whenever required.

Acquisition: The systematic process of gathering or obtaining relevant information and data from all available sources, which can then be analysed to generate actionable intelligence.

Acquisition plan: A plan that directs the acquisition of data on a particular topic with a specific objective, a list of potential sources of that data, and an estimated time frame.

Data: Factual elements or discrete pieces of information in their most atomized form, regardless of file format or structure.

Data Evaluation: An assessment/review of the reliability and credibility of the information, including its source and accuracy of the raw data or information.

Dissemination: The process of delivering or sharing actionable crime intelligence with the appropriate individuals, units, or agencies to support decision-making and operational activities under certain protocols.

Dissemination Plan: A plan that shows how a crime intelligence product is to be disseminated, at what security level, and to whom.

Estimate: A numeric forecast of activity based on facts but not able to be verified or known.

Forecast: A look at what has happened or what may happen, based on what is known and verifiable, suspected and not verifiable, and unknown. Likelihoods or probabilities of future activity are usually included, with suggested steps to protect against criminal activity.

Information: Any knowledge that can be communicated or any documentary material, regardless of its physical form or characteristics that is not processed.

Criminal Intelligence: The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in

nature. Intelligence is information that has been analysed to determine its meaning and relevance.

Organized Criminal Group: A structured group of three or more persons, existing for a period and acting in concert with the aim of committing one or more serious crimes or offences as defined in the United Nations Convention against Transnational Organized Crime, to obtain, directly or indirectly, a financial or other material benefit. (UNODC SOCTA Handbook). Although this is a definition used by UNODC, it is acknowledged that modern crime threats are evolving (i.e., Cyber enabled crime) so a broader consideration is necessary when applying this definition.

Open-Source Information: Information that is publicly available. One very notable subset of open source is the so called "grey literature." It can consist of research, technical reports, "white papers" conference documentation, dissertations and theses, discussion papers, subject related newsletters etc.

Peacekeeping-Intelligence: The purpose of peacekeeping-intelligence in UN peacekeeping operations is to enable missions to take decisions on appropriate actions to enhance situational awareness and the safety and security of UN personnel, and inform activities and operations related to the protection of civilians.[40]

Peacekeeping operation: UN mission led by the Department of Peace Operations.

PESTEL analysis: PESTEL is a strategic framework used for analysing the external macro-environmental factors that affect the implementation, planning, and success of ILP. The acronym stands for *Political, Economic, Social, Technological, Environmental, and Legal* factors. It helps in understanding how these external forces influence opportunities, risks, and decision-making.

I. **Political**: Refers to government policies, political stability, penal laws, trade regulations, labor laws, and international relations.
   - Example: Changes in criminal law affecting right to speak freely or right to protest peacefully.

II. **Economic**: Encompasses economic trends such as poverty, unemployment, and economic development, which often correlate with crime rates.
   - Example: High unemployment in a region might lead to an increase in property crimes or organized criminal activities, shaping ILP focus areas.

III. **Social**: Involves cultural norms, societal values, population demographics, and attitudes toward law enforcement.

[40] DPO Policy on Peacekeeping-Intelligence 2019.08. para 5.

- Example: Understanding societal trust in police or cultural attitudes toward crime is essential for effective intelligence gathering and community cooperation.

IV. **Technological**: Examines the role of technological advancements in crime prevention, intelligence gathering, and policing operations.

- Example: The availability of surveillance tools, forensic technologies, and data analytics systems can significantly enhance the effectiveness of ILP.

V. **Environmental**: Focuses on ecological issues, natural disasters, and environmental crimes (e.g., illegal mining, deforestation).

- Example: In a peacekeeping mission, environmental factors might include monitoring crimes related to resource exploitation or responding to disaster-related criminal activities.

VI. **Legal**: Analyzes laws, regulations, and the legal frameworks governing law enforcement, international cooperation, and data sharing.

- Example: Adherence to international legal standards and host nation laws is critical for ILP operations, particularly in managing cross-border crimes and extraditions.

Evaluation: A review of the operation of the crime intelligence process and the value of the output to the consumer.

Source Reliability: A scale (A to E) that reflects the reliability of information sources; It ranges from factual source to unknown reliability.

Strategic intelligence: Intelligence that is required for the formulation of strategy, policy and plans and operations at national levels.

Tactical Intelligence: Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer's safety.

Threat Assessment: A report that looks at a criminal group or criminal activity and assesses the threat that activity, actor, or group poses to a jurisdiction, either at present or in the future, and recommends ways to lessen the threat.

United Nations Police (UNPOL): Includes both Headquarters staff in the United Nations Police Division (inclusive of the Standing Police Capacity) and mission staff in UNPOL components.

UNPOL component: United Nations police organized within a peace operation.

I. REFERENCES

Normative or superior references

A. Security Council Resolutions: on policing 2185 (2014) and 2382 (2017); and on women, peace and security: 1325 (2000), 1820 (2008), 1888 (2009), 1889 (2009), 1960 (2010), 2106 (2013), 2122 (2013), 2242 (2015), 2467 (2019) and 2538(2020).
B. Report of the Secretary-General on United Nations police, A/66/615, 15 December 2011.
C. Report of the Secretary-General on United Nations policing, S/2016/952, 10 November 2016.
D. Report of the Secretary-General on United Nations policing, S/2018/1183, 31 December 2018.
E. DPO Policy on Peacekeeping-Intelligence (2019.08).
F. DPKO/DFS Policy on United Nations Police in Peacekeeping Operations and Special Political Missions (2014.01).
G. DPKO/DFS Guidelines on Police Capacity-Building and Development (2015.08).
H. DPKO/DFS Guidelines on Police Command in United Nations Peacekeeping Operations and Special Political Missions (2015.14).
I. DPKO/DFS Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions (2015.15).

Related procedures and guidelines

J. DPKO/DFS Guidelines for Integrating Gender Perspectives into the Work of United Nations Police in Peacekeeping missions (2008.30).
K. DPKO/DFS Policy on Civil Affairs (2008.09).
L. DPKO/DFS Manual on Civil Affairs Handbook (2012.02).
M. UNODC Criminal Intelligence Manual for Frontline Law Enforcement (2010).
N. UNODC Criminal Intelligence Manual for Managers (2011).
O. UNODC Police Information and Intelligence Systems (2006).
P. DPO Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities (2022.05).
Q. DPO Guidelines on Open-Source Peacekeeping-Intelligence (OPKI) (2022.03).
R. DPO Guidelines on Gender and Peacekeeping-Intelligence (2022.08).
S. DPO Guidelines on Acquisition of Information from Human Sources for Peacekeeping-Intelligence (HPKI) (2020.05).
T. OHCHR/DPKO/DPA/DFS Policy on Human Rights in United Nations Peace Operations and Political Missions (2011.20).
U. United Nations Human Rights Due Diligence Policy on United Nations Support to Non-United Nations Security Forces – HRDDP (S/2013/110).
V. DPKO/DFS Manual on Police Monitoring, Mentoring and Advising in Peace Operations (2017.14).
W. DPKO-DFS Manual on Mission-based Police Planning in Peace Operations (2017.13).
X. DPO Military Peacekeeping-Intelligence Handbook, 2nd Edition (2025.10).
Y. DPO-DOS Manual on Donor Coordination and Fund Management in Peace Operations (2019.06).

J. MONITORING AND COMPLIANCE

93. In field missions, this manual will serve the Head of Police Component and other managers, specifically the heads and staff of units responsible for Crime Intelligence. At Headquarters, the Police Adviser to the Department of Peace Operations and Director of the Police Division shall monitor compliance with this document.

K. CONTACT

94. The Chief of the Strategic Policy and Development Section, Police Division, Office of Rule of Law and Security Institutions, Department of Peace Operations.

L. HISTORY

95. This is a new manual on Intelligence-led Policing. It shall be reviewed not later than 2030, or as needed.

APPROVAL SIGNATURE:  Faisal Shahkar

DATE OF APPROVAL: 15/08/2025

Annex- A

UNPOL Crime Intelligence 5 x 5 x 5 System

	A	B	C	D	E
Source	Always Reliable Source	Information from the source is mostly reliable	Information from the source is sometimes reliable	Information from the source is unreliable	Source not yet judged or proved

	1	2	3	4	5
Information	Accurate and known to be true	Information known personally from the source but not the officer passing it, logical and agrees with other information on the subject	Information not known personally to the source but corroborated by other information on record	Suspected to be false	Information cannot be judged

	1	2	3	4	5
Dissemination To be completed by the CIU Staff prior to entry into the crime intelligence system. To be reviewed by Chief CIU before dissemination.	Default: Permits dissemination within the UN Mission	Permits Dissemination to UN agencies Funds and programmes	Permits dissemination to Host-State Police	Permits dissemination within UNPOL only: specify reasons and internal recipient(s) Review period must be set	Permits dissemination to international partners (AU, EU, NTERPOL, NATO, etc.) but receiving entity to observe conditions as specified

Source matrix (A-E): There is a need to evaluate both the SOURCE and the CONTENT "separately "of each piece of information. The source will be evaluated using the A-E grading system:

A. *(Always Reliable)* 100%. There is no doubt of the authenticity, trustworthiness, and competence of the source. Examples might include technical deployments and information known directly to police and other law enforcement officers including the host-State police and other law enforcement agencies. Informants (if applicable) give information for a reason, and they will rarely if ever be graded an 'A.'

B. *(Mostly Reliable)* Sources where information in the past has, usually, proved to be reliable. Examples might include contacts and informants (if applicable) whose information has proven correct most times. This includes databases of host state police and other law enforcement agencies, court records, bank statements, etc.

C. *(Sometimes Reliable)* Sources where information in the past was not true or was not accurate. The source has provided information that has been correct on some occasions but more often the information has been incorrect. In these circumstances the information provided by the source should not be acted upon without checking the accuracy of the information from an independent source.

D. *(Unreliable)* Examples might include individuals, who have routinely proven unreliable in the past, or there is some doubt about the authenticity, trustworthiness, or competency;

for example, the information is known second, or third hand and an audit trail may be needed to ensure the long-term reliability of a source.

E. *(Untested Source)* This does not necessarily mean that the information is unreliable but should nonetheless be treated with caution. Corroboration should be sought. An example of this is a first-time source or a member of the public on the street.

Information matrix (1-5): The value of information must not be influenced by personal feelings but be based on professional judgment. Its value must not be exaggerated to ensure action is taken. Officers recording intelligence on reports are personally responsible for ensuring the accuracy and proper evaluation of the material based upon their knowledge of the circumstances prevailing at the time.

1. *Accurate and known to be 100% true*. Examples might include the product of technical deployment or events witnessed by UNPOL officers including host-State police or other law enforcement officers. However, exceptional care should be taken in assuming that everything heard using technical equipment is a '1'. Whilst it will be an accurate record of what the officer heard, the information itself may still not be accurate, for example the source may be repeating hearsay or may be lying.

2. *Information known personally from the source but not the officer passing it, logical and agrees with other information on the subject.* The information is known personally to the source but is not known personally to the reporting officer. Example, something an informant has seen that is then related to the reporting officer.

3. *Information not known personally to the source but corroborated by other information on record.* The information is not known personally to the source but is corroborated NOW by information already recorded. e.g., something overheard by an informant/source, which has been reported independently by another source. It must be recorded in the system now – not something that can go and be corroborated later.

4. *Information cannot be judged.* The information is not known personally to the source, and it cannot be corroborated in any way. The value of the information cannot be judged at this time.

5. *Suspected to be false or malicious.* Action should be taken with extreme care and corroboration by a more reliable source. Collating this type of information may prove useful in evidencing why an informant should be treated as 'dangerous. Whilst it may be desirable to record such intelligence into an intelligence system, it must be correctly and clearly graded and assessed for the potential risks arising from its inclusion. *It is important to use common sense and critical thinking during the information evaluation thus information highly unlikely to be true or those which are opposing fundamental laws of the universe should not be recorded."*

Example: An incident of an adult male spray-painting hates slogans against a particular community captured on CCTV will be ordinarily classified as **A.1.**

Dissemination matrix (1-5): To be completed at time of entry into the crime intelligence system and reviewed on dissemination.

1. *Dissemination may be permitted to non-prosecuting organizations operating in the mission area* (permission from HoPC/CIU Chief before dissemination is required) For example- UN Security

2*. Dissemination may be permitted to non-UNPOL and other law enforcement and prosecuting entities (*permission from HoPC/CIU Chief before dissemination is required) For example – Host state law enforcement agencies, Interpol, etc.

3. *Disseminate only to units/offices within the UN mission*. Under this Code, for example, a report written by an UNAMID police officer will be only disseminated within UNAMID. All recipients within UNAMID must be specified.

4. *Dissemination may be permitted to UNPOL* (permission from HoPC/Chief-CIU before dissemination is required) This handling code covers dissemination within the UNPOL. Specific handling conditions should be attached along with the identity of recipients.

5. *No Further dissemination refer to the originator.* This handling code is primarily for disseminating crime intelligence to individual people or units.