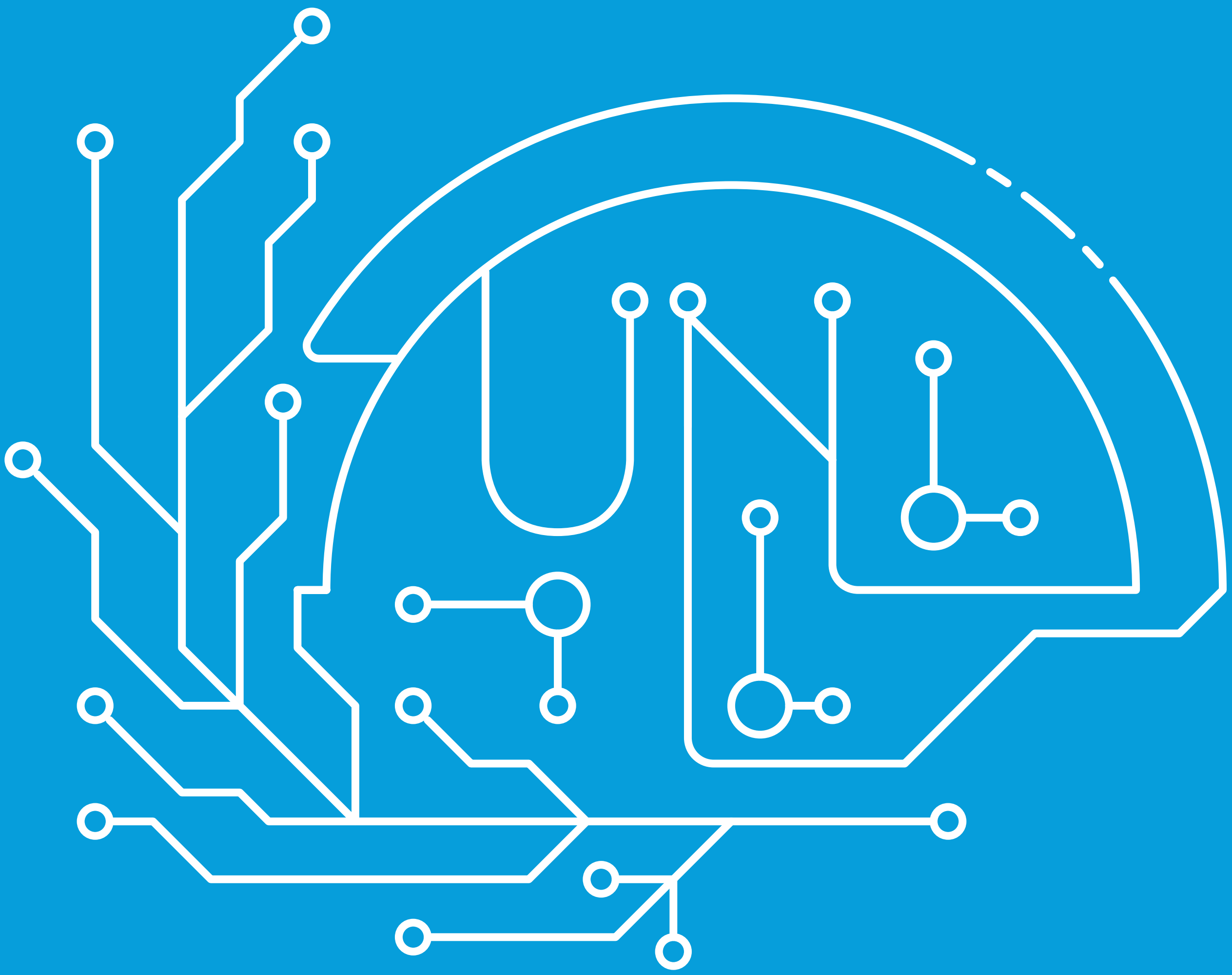
United Nations
Peacekeeping
un.org/peacekeeping

# Strategy for the Digital Transformation of UN Peacekeeping



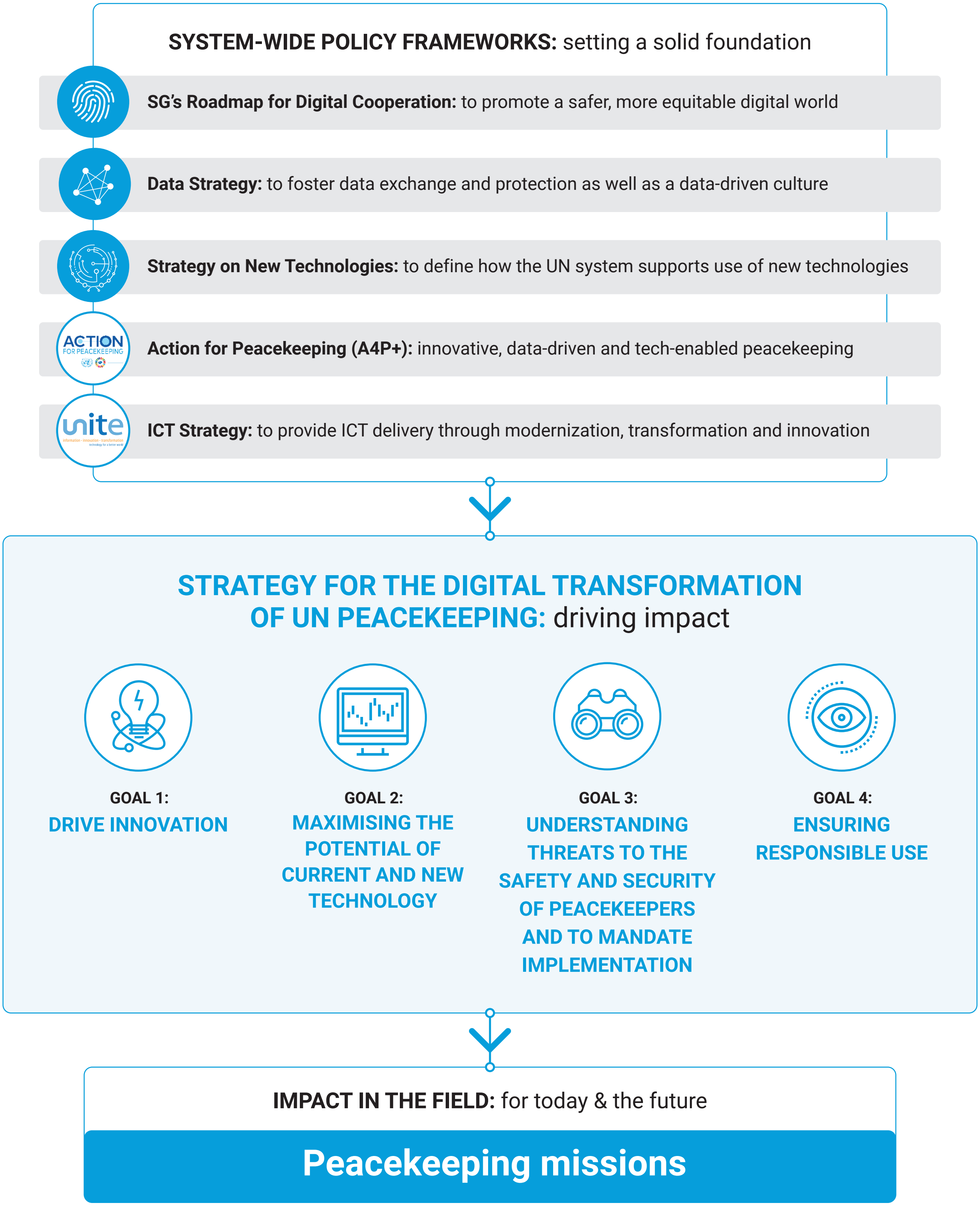
17-09-2021

Department of Peace Operations (DPO)
Department of Operational Support (DOS)
Department of Management Strategy, Policy And Compliance (DMSPC)
United Nations
New York, September 2021

**Visit peacekeeping.un.org
for downloads and more information**

# Table of contents

FIGURE 1. SITUATING THE STRATEGY IN THE BROADER POLICY AGENDA



**SYSTEM-WIDE POLICY FRAMEWORKS:** setting a solid foundation

**SG's Roadmap for Digital Cooperation:** to promote a safer, more equitable digital world

**Data Strategy:** to foster data exchange and protection as well as a data-driven culture

**Strategy on New Technologies:** to define how the UN system supports use of new technologies

**Action for Peacekeeping (A4P+):** innovative, data-driven and tech-enabled peacekeeping

**ICT Strategy:** to provide ICT delivery through modernization, transformation and innovation

**STRATEGY FOR THE DIGITAL TRANSFORMATION OF UN PEACEKEEPING:** driving impact

GOAL 1:
**DRIVE INNOVATION**

GOAL 2:
**MAXIMISING THE POTENTIAL OF CURRENT AND NEW TECHNOLOGY**

GOAL 3:
**UNDERSTANDING THREATS TO THE SAFETY AND SECURITY OF PEACEKEEPERS AND TO MANDATE IMPLEMENTATION**

GOAL 4:
**ENSURING RESPONSIBLE USE**

**IMPACT IN THE FIELD:** for today & the future

**Peacekeeping missions**

# Foreword

**The UN Secretary-General is leading a digital revolution throughout the UN system. In his 2018 Strategy on New Technologies, he calls on “UN leadership to encourage initiatives at all levels and with all staff designed to deepen our understanding of new technologies and their impact on individual and entity wide mandates, [and] how these technologies can be used to support mandate delivery.”**

With this **Strategy for the Digital Transformation of UN Peacekeeping,** the Departments of Peace Operations, of Operational Support and of Management, Strategy, Policy and Compliance – have jointly heeded the Secretary-General’s call.

Moreover, the key enablers identified in the Secretary-General’s Data Strategy – “Empowered people and culture, cross-cutting data governance and strategy support, sustained partnerships, and user-focused technology” – are centre pieces of this strategy for peacekeeping and our focus on digital transformation fits squarely with the Secretary-General’s own vision for his next five years in office. Digital transformation also cuts across all the areas of Action for Peacekeeping and will be a central vector in the next phase of implementation through A4P+.

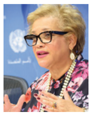
This strategy represents an essential step towards enhancing the safety and security of peacekeepers and enabling more effective mandate implementation through the use of digital technologies. Ultimately, it aims to deliver timely, responsibly-managed, integrated analysis for decision-making; to empower technology-aware, data literate and innovation-minded staff; to effectively monitor evolving, technology-related threats and opportunities; and provide access to the tools, processes, knowhow, resources and support to innovate and respond to these threats and opportunities in a timely manner. Recognising its part in a broader system-wide transformation process, the strategy seeks to leverage existing initiatives and structures, to establish and expand synergies, and strengthen coherence, while ensuring that our field missions are at the heart of the move towards agile, data-driven and technology-enabled peacekeeping.

We are committed to the digital transformation of UN peacekeeping and to the full and joint implementation of this strategy.

Jean-Pierre Lacroix

**Jean-Pierre Lacroix**
Under-Secretary-General
Department of Peace
Operations

Catherine Pollard



**Catherine Pollard**
Under-Secretary-General
Department of
Management, Strategy,
Policy and Compliance

Atul Khare

**Atul Khare**
Under-Secretary-General
Department of
Operational Support

# Executive summary

**The framework of the Secretary-General's strategies on new technologies and on data sets the stage for UN peacekeeping to forge its own path toward harnessing the potential of digital technologies and better deliver on its mandates.**

The Action for Peacekeeping "Plus" (A4P+) priorities of 2021, as well as Security Council and the General Assembly's Special Committee on Peacekeeping Operations (C34) acknowledged the need to better integrate the use of new technologies for the purposes of increasing safety and security, improving situational awareness, enhancing field support and facilitating substantive mandate implementation. This led the Departments of Peace Operations (DPO), Operational Support (DOS) and Management, Strategy, Policy and Compliance (DMSPC) to jointly initiate the development of this strategy with four key goals in support of UN peacekeeping and for action by the Secretariat and external partners over the next three years.

The strategy recognises its part within the **system-wide digital transformation,** seeks to capitalise on ongoing initiatives, especially the SG's Data Strategy, and to align with established systems in peacekeeping to avoid duplication, ensure coherence and promote the efficient and responsible use of resources. Still, peacekeeping, with over 90,000 peacekeepers across 12 operations and almost half of the annualised Information and Communications Technology (ICT) budget, brings with it specific challenges and opportunities.

The strategy views digital transformation as a change process that is driven and enabled by digital technologies, but involves a significant measure of cultural change, and conceives of **digital technologies as an enabler** that allows UN peacekeeping to achieve an analysis-driven, forward-looking understanding of the conflict environment, strengthen the safety and security of its personnel, and shape agile and responsive mandate implementation. The digital transformation of peacekeeping is to be guided by **twelve principles** to ensure that the use of technology is accessible, protects data and privacy, is demand-driven, does no harm, is gender-sensitive, human-centred, inclusive and transparent, multidisciplinary, fosters partnerships, engenders realistic expectations, and is sustainable and scalable.

The strategy's goals were developed through extensive consultations across the organisation, complemented by a survey, research papers, roundtables and other input from external sources, and draws on valuable insights from UN system and other partners, including Agencies, Funds and Programmes, Member States, international organisations, researchers and civil society peacebuilders. Its **target audience** consists of Mission and Headquarters staff, Member States, and UN system and external partners.

A thorough understanding of **how conflicts are being shaped by technology** is essential to recognise the risks and opportunities and to pinpoint entry points for the use of digital technologies. The purposes for which technologies are used by actors in the conflict environment range from disinformation, misinformation and incitement to violence through hate speech, to surveillance, control and intelligence gathering, to dialogue platforms, mobilisation, outreach and recruitment into armed groups, and to cyberattacks and other types of attacks. The large amounts of data captured places tremendous power in the hands of those holding and analysing data and risks "collective data harms," i.e. the misuse and abuse of population data, including breaches of confidentiality, behavioural surveillance, information disorder, information infrastructure sabotage or disruption. It raises **key ethical questions** around data ownership, sovereignty and consent, social justice and potential social harm, as well as biases in algorithms for processing and analysing data, and underscores the importance of choosing a do-no-harm approach. For peacekeeping, understanding an ever more fragmented, expanding and constantly shifting conflict landscape requires a mission to continuously digest, structure, re-structure and analyse large amounts of information, and to respond in a timely manner. Peacekeeping mandates, and responsibilities to protect personnel, make the use of digital technologies a necessity in today's world. At the same time, peacekeeping must think carefully about which data can and should be collected to minimise vulnerability and potential harm, and aim to detect any cyberattacks and resulting compromised data in near real-time.

The strategy focuses on **four goals that are central to the transformation of peacekeeping missions and critical to their effectiveness** and/or that address **long-standing challenges** which might have relatively simple technical solutions. These goals require the resources, commitment and support of UN leadership, both in the field and at headquarters, as well as partnerships across UN offices and with external partners, whether Member States, the technology sector, or civil society.

**Goal 1** aims to **drive innovation** for effective mandate implementation and safety and security. Actions include a liaison function that connects users and developers to collaboratively match mandate implementation challenges with technology solutions, bridge gaps between HQ and the field

A 34-year-old peacekeeper from India that works at the Movement Control wing of UNMISS, responsible for monitoring the smooth conduct of the mission's air operations from Juba. Photo by Gregorio Cunha (February 26, 2021) and foster cultural change; an innovation and digital transformation space at Headquarters that allows leadership to elevate, propagate and promote innovation in support of mandate implementation and safety and security; a foresight analysis capacity to monitor, analyse and advise on emerging technology issues as they affect peace operations; and the mobilization of adequate funds/resources in order to encourage innovation and facilitate use of fast-tracked funding and procurement mechanisms when appropriate.

**Goal 2** seeks to **maximise the potential of current and new technology** in order to empower missions and augment their capacity to carry out their mandates more efficiently and effectively. Actions include training and capacity building to enable a level playing field and develop a peacekeeping workforce equipped with the requisite digital skills, know-how and tools to be able to carry out their work effectively and technological solutions to consolidate ICT/data systems, promote mobile, low bandwidth and offline applications, introduce advanced analytics tools, deploy additional technology for protection or provide service to remote sites and mobile deployments.

**Goal 3** strives to **understand threats** against civilians, peacekeepers, political processes or missions in a timely and integrated manner, identify opportunities to promote mandate implementation and build awareness and support. Actions include a comprehensive, timely and accurate picture of the situation for better informed planning and decision-making; an integrated approach to mis/disinformation and hate speech; and measures to reduce the likelihood and impact of cyberattacks, as well as other attacks enabled by digital technologies, including through remote activated IEDs and uncrewed aerial vehicles.

**Goal 4** looks to **ensure responsible use** by developing clear principles for the ethical use of digital technology, especially data, guidelines for how these should be applied and regular reviews as well as a complaints mechanism, in line with UN system standards and in collaboration with other efforts in this area.

The digital transformation of UN peacekeeping in missions and at Headquarters requires dedicated attention and resources, broad consultation and coordination, and oversight. The strategy proposes a tentative governance structure that engages leadership in supporting a culture of innovation and transformation, eliminating barriers and seeking accountability; that calls for active involvement of multidisciplinary partners; and that includes a dedicated capacity for co-creation between technology users and developers/managers to flourish.

To meet the challenge at Headquarters, the creation of an **Innovation and Digital Transformation Team** is proposed. This multidisciplinary centre of gravity for innovation and digital transformation could promote a culture of innovation, draw together expertise from across the Secretariat and oversee implementation of the strategy. The proposed team would provide advisory support to individual missions on the design and configuration of capacity for technology innovation, as well as supporting specific initiatives in missions. The configuration of resources and organisational set-ups to enable innovation in missions would be driven by mission-specific considerations and the needs of each conflict environment.

# A Strategy for the Digital Transformation of UN Peacekeeping

## Background

### WHY A STRATEGY FOR THE DIGITAL TRANSFORMATION OF UN PEACEKEEPING?

**With digital technologies taking on a prominent and ever-more complex role in 21st century conflicts, the framework of the Secretary-General's strategies on new technologies and on data set the stage for UN peacekeeping to forge its own path toward harnessing the potential of digital technologies and better deliver on its mandates, now and for the future.**

In his Roadmap for Digital Cooperation, the Secretary-General specifically recognises that "digital technologies can support United Nations peacekeeping efforts globally, including by ensuring the safety and security of peacekeepers." The vision for deeper internal capacities and exposure to new technologies is consistent with the Action for Peacekeeping (A4P) initiative; the A4P "Plus" (A4P+) priorities of 2021 emphasise the need for innovative, data-driven, and technology-enabled peacekeeping.

The Security Council and the General Assembly's Special Committee on Peacekeeping Operations (C34) have acknowledged the efforts to better integrate the use of new technologies for the purposes of increasing safety and security, improving situational awareness, enhancing field support and facilitating substantive mandate implementation. They have encouraged the use of field-focused, reliable, cost-effective technologies that are driven by practical needs of end-users on the ground.[1]

While leveraging the opportunities that digital technologies offer to strengthen the effectiveness of peacekeeping, this strategy highlights that with greater use of digital technologies come greater vulnerabilities, and hence a strong focus is on building safeguards and protections to ensure the responsible use of digital technology.

In recognition of the above, the Departments of Peace Operations (DPO), Operational Support (DOS) and Management, Strategy, Policy and Compliance (DMSPC) initiated the development of this strategy. It proposes goals in support of UN peacekeeping, to be taken forward by the Secretariat and external partners, for action over the next three years.

[1] See Security Council resolution 2518 (2020), para 13, and the Report of the Special Committee on Peacekeeping Operations, (A/75/19), para 160.

## HOW DOES THE STRATEGY RELATE TO OTHER TECHNOLOGY-RELATED INITIATIVES?

The strategy recognises its part within the broader digital transformation that is taking place throughout the UN system. This necessitates harmonisation and integration with wider efforts that affect peacekeeping missions, not least the possible development of a new ICT strategy. Indeed, the initiatives spurred by this strategy may provide value beyond peacekeeping.

The strategy seeks to capitalise on ongoing UN-system-wide initiatives,[2] especially the SG's Data Strategy workstreams fostering data exchange and data protection, as well as cultural change in the organisation and workforce planning, while recognising the particular needs of peacekeeping operations. The implementation of the strategy's goals looks to align with already established systems in peacekeeping to avoid duplication, ensure coherence and promote the efficient and responsible use of resources.

That said, it must also be recognised that peacekeeping, with its over 90,000 peacekeepers across 12 operations, is a massive enterprise with a complex digital ecosystem that brings with it specific challenges and opportunities stemming from missions' operating environments, size, high turnover, and diverse composition. With almost half of the annualised ICT budget relating to peacekeeping missions, the imperative for services to align with needs is strong.[3]

[2] See Annex I.

[3] 44.89 per cent in 2018/19. Source: fourth progress report of the Secretary-General on the status of implementation of the ICT strategy for the United Nations (A/73/384).

Peacekeepers of the Rwandan Battle Group in MINUSCA preparing to launch an observation drone to spot the positions of armed groups. Photo by Leonel Grothe (January 15, 2021)

## DIGITAL TRANSFORMATION IN THE CONTEXT OF THIS STRATEGY

The strategy views digital transformation as a change process that is driven and enabled by digital technologies, but involves a significant measure of cultural change. It understands digital technologies to be electronic tools, systems, devices and resources that generate, capture, store or process data. In line with the four areas identified by the USGs, the strategy has focused on digital transformation that directly enhances safety and security, empowers and enriches mandate implementation, helps to uncover threats and opportunities in the conflict environment, and the training and capacity-building required to enable these efforts. Even though it is critical to the success of peacekeeping, how digital technologies are used and can be further promoted in the area of mission support falls outside of the scope of this strategy.

## A VISION FOR PEACEKEEPING IN YEARS TO COME

This strategy conceives of digital technologies as an enabler, to be managed responsibly, for more effective and impactful operations. A robust foundation in digital technologies allows UN peacekeeping to achieve an analysis-driven, forward-looking understanding of the conflict environment, which can strengthen the safety and security of its personnel, while shaping agile and responsive mandate implementation.

This strategy sets a path to achieve this vision. It aspires peacekeeping to:

- Have timely, responsibly-managed information that enables integrated analysis for decision-making;
- Have a body of staff that is technology-aware and data literate, has an ‘innovation mindset’, and that actively applies digital technologies for safety and security and mandate implementation;
- Be alert and continually scan the horizon to monitor the evolving, technology-related threats and opportunities; and
- Have access to the tools, processes, knowhow, resources and support to innovate and respond to threats and opportunities in a timely manner.

## HOW THE STRATEGY WAS DEVELOPED

The recommended goals and actions were developed on the basis of extensive consultations across disciplines within the organisation, complemented by input from external sources. The methodology included over 100 consultations, a baseline survey and four focus groups, four commissioned research papers, and four roundtable discussions.[4] In addition, the content of the draft strategy was subject to a reference and validation process through meetings of an interdepartmental working group[5] and an external Red Team, which reviewed the relevance, feasibility and sustainability of proposed recommendations. UN system and other partners, ranging from Agencies, Funds and Programmes to Member States, international organisations, to researchers and civil society peacebuilders, contributed valuable insights from their own digital transformation journeys and use of digital tools, identifying common challenges and sharing good practice all of which have informed the goals and actions laid out in this strategy.

[4] See Annex II.

[5] For composition, see Annex III.

## WHO THE STRATEGY IS FOR

The strategy has multiple target audiences, including:

- **Mission and Headquarters staff working in and/or supporting peacekeeping operations.** The strategy should provide tangible support when introducing, expanding and managing the use of digital technologies and identify gaps where guidance and clear direction may be required, with a particular focus on the role of senior leadership in the stewardship of transformation.

- **Member States,** including troop and police contributors, as well as Member States contributing equipment, training and capacity-building support. The strategy recognises Member States as an integral actor in safety and security and mandate implementation and seeks Member State engagement and support for equal opportunities when it comes to access and use of technology as well as their responsible application.

- **UN system and external partners** in international organisations, research communities and civil society. Peacekeeping's path towards digital transformation will be strengthened by learning from others; the strategy will cultivate opportunities for practical and multidisciplinary collaboration.

## RISKS AND OPPORTUNITIES FOR UN PEACEKEEPING IN AN EVOLVING TECHNOLOGY LANDSCAPE

A thorough understanding of the context, including mission-specific environments and how conflicts are being shaped by technology, is essential to pinpoint entry points for the use of digital technologies in peacekeeping and for engaging with conflict parties, communities and other stakeholders. It is crucial to recognise the risks and opportunities inherent to this dynamic context.

A key feature in the recent evolution of digital technologies has been their convergence, particularly a convergence of artificial intelligence (AI) and dual-use technologies. These technologies are designed and developed for beneficial uses, but can be weaponised or used with other malicious intent. The purposes for which technologies are used range from disinformation, misinformation and incitement to violence through hate speech, to surveillance, control and intelligence gathering, to dialogue platforms, mobilisation, outreach and recruitment into armed groups, and to cyberattacks.

Social media, mobile phones and internet platforms are increasingly used for communication that connect people for the purposes of dialogue, consultation and community just as well as for sowing distrust, recruitment and incitement to violence, and various forms of crime. With the support of AI, popular consultations can generate content and consensus among thousands of participants. At the same time, digital technologies can also be used to heighten political influence and suppress individual freedoms. Election cycles are particularly precarious times where social media is increasingly used for campaigning and mobilising voters, and the spread of disinformation is expected to increase. "Deep fakes", easily produced using tools available on the internet, are already difficult to distinguish from reality and will soon be virtually undetectable.

New technologies are central to intelligence, surveillance and reconnaissance (ISR). Armed groups are able to produce their own, untraceable long-range unarmed aerial and marine systems, both for surveillance and attack, dramatically increasing their areas of operation and raising questions over the hitherto "asymmetric" nature of civil wars. While both mobile phones and UAVs have been used in positive ways to capture evidence and bear **witness** to atrocities, they can also be used for surveillance as the first step towards **suppression and control.**

The large amounts of data captured places tremendous power in the hands of those holding and analysing data and is accompanied by a **high risk of "collective data harms,"** i.e. the misuse and abuse of population data, including breaches of confidentiality, behavioural surveillance, information disorder, information infrastructure sabotage or disruption. It raises **key ethical questions** around data ownership, sovereignty and consent, social justice and potential social harm, as well as gender, race or other biases in algorithms for processing and analysing data, and underscores the importance of choosing a do-no-harm approach.

Mobile phones – as triggers for Improvised Explosive Devices (IEDs) – and UAVs can be used for **physical attacks** on civilian populations and peacekeepers. Even though they have not been used against peacekeeping missions, Unmanned Combat Aerial Vehicles (UCAVs) now feature heavily in some conflict areas and might also be used for attacks on UN staff and facilities. **Cyberattacks** for financial gain, destruction or disruption of infrastructure, theft or manipulation of information are clearly on the rise and have begun to target peacekeeping. Growing links between systems, dual-use technologies and critical infrastructure increase the vulnerability manifold and ramifications can range from breaches of privacy, destruction or alteration of data to disabling utilities, disrupting communications, manipulating the population and inciting physical violence. Where governance of the digital space is weak, there is a danger of inadvertently offering an attractive home for attackers. Sophisticated technology is no longer the prerogative of state actors as the cost of computing power decreases and more non-state actors turn to cyberspace, representing a growing challenge to peacekeeping missions.

For peacekeeping, understanding an ever more fragmented, expanding and constantly shifting conflict landscape becomes increasingly challenging. Shifts are complex – actors with multiple identities and affiliations, an intricate web of motivations, needs and ambitions – and fast-moving, requiring a mission to continuously digest, structure, re-structure and analyse large amounts of information, and to respond in a timely manner. This suggests that peacekeeping missions need to employ different skill sets and capacities such as advanced situational awareness and analytics, constantly review security measures, work towards nimbler administrative processes, including decision making, budgeting, procurement and staffing, and consider how to better leverage partnerships and maximise strategic communications efforts including outreach to local communities. They also underscore the need for ethical risk assessments, clear guidance and safeguards.

Peacekeeping mandates, and responsibilities to protect the safety and security of personnel, make use of digital technologies a necessity in today's world. An awareness of the ethical implications is a fundamental precondition for its digital transformation. Peacekeeping must think carefully about which data can and should be collected to minimise vulnerability and potential harm, and aim to detect any cyberattacks and resulting compromised data in near real-time.

Ultimately, these developments may give rise to the introduction of a cyber capacity and resilience in peacekeeping missions to ensure safety and security. The need to monitor potential escalations or growing cyber abuse is already an increasingly pressing challenge in many areas of operation that requires a strategic and comprehensive response.

# Principles guiding the Strategy for the Digital Transformation of UN Peacekeeping

**Accessibility.** In accordance with the UN Disability Inclusion Strategy, and relevant bulletins and conventions, the introduction, design and operation of digital information and communication technologies ensure that persons with disabilities have access, on an equal basis with others.

**Data protection and privacy.** Data gathered is managed in accordance with UN confidentiality, classification and privacy standards and rules; and used solely for mandate implementation.

**Demand-driven.** Technology employed by peacekeeping missions is driven by their needs for solutions, not by supply, and based on consultations with peacekeeping missions throughout development and implementation.

**Do-no-harm.** Digital technologies in peacekeeping place the best interests and needs of people first, as subjects and users of new technologies.

**Gender-sensitive.** The design and use of technology factor in gender considerations, including differences in access, literacy and bias.

**Human-centred.** Technology used in peacekeeping is simple, intuitive, and enable accessibility to all relevant peacekeepers.

**Human rights compliant.** Technology use is consistent with the legal framework governing UN peacekeeping operations, in particular with full respect for human rights standards and obligations.

**Inclusion and transparency.** The adoption of advanced technology by peacekeeping operations is in support of mission mandates and used in an inclusive and transparent manner.

**Multidisciplinarity.** Technology builds upon strength in diversity and incorporates different skills, experience and perspectives.

**Partnerships.** Peacekeeping seeks to engage and work closely with diverse partners as part of a multistakeholder approach, including Member States, in particular T/PCCs, other international organisations, the technology sector, research institutes, and civil society organisations, to increase and share collective knowledge and overcome challenges.

**Realistic expectations.** Technology is an enabler, but will not resolve or compensate for fundamental operational or strategic challenges.

**Sustainability and scalability.** Technology used is interoperable with other systems in use, build on what has already been achieved and learned, be sustainable over time, with training, hand-over, maintenance and continuity measures in place, and flexible enough to be easily adapted and deployed to multiple missions to achieve greater returns on the investment.

# Setting up peacekeeping for the future: challenges and goals

**The strategy outlines four goals, which will promote the digital transformation of UN peacekeeping. Each goal is supported by a diagnosis of challenges that derives from the extensive consultations and background research conducted as part of the strategy development process.**

Many actions were proposed during consultations, some of which represented continuations or extensions of ongoing initiatives. The strategy's goals and actions reflect two types of objectives:

- those that are **central to the transformation of peacekeeping missions and critical to their effectiveness.** If left unaddressed, these present a risk, whether political, ethical, reputational, or performance-related, and are likely to require the mobilisation of additional resources and capacities; and
- those that are **long-standing challenges** that nevertheless might be addressed through relatively simple technical solutions.

These four goals can only be realised with resources, commitment and the support of UN leadership, both in the field and at headquarters, as well as partnerships across UN offices and with external partners, whether Member States, the technology sector, or civil society.

## GOAL 1: DRIVE INNOVATION

*Position peacekeeping to* ***continue to evolve and capitalise on technological innovation*** *for effective mandate implementation and safety and security.*

### 1.1 LIAISON FUNCTION FOR TECHNOLOGY AND INNOVATION

**KEY RECOMMENDED ACTION:**
Establishment of capacity or mechanism in the field to promote co-creation between Field Technology Services (FTS) and substantive components in missions and foster innovative technological solutions that are easy-to-use and fit-for-purpose, as well as compliant with ICT policies and standards and within the delegation of authority framework. This capacity would be complementary to and supported by a HQ-based Innovation and Digital Transformation Team (see below). The liaison function would have as a primary goal the ongoing matching of mandate implementation challenges with technology solutions, using a collaborative, human-centred design approach and bridging any gaps between Headquarters and the field, as well as foster the required cultural change. With existing capacities and set-ups varying across missions, mission-specific approaches to realising this function should be developed. For instance, where FTS components have innovation capacity, they could convene regular ideation or brainstorming meetings with substantive components, or FTS innovation

capacity could be embedded in a substantive pillar of the mission. Where business analytics components exist, these sections could potentially be the centre of gravity and run a mission-wide task force or alliance of technology champions, or similar.

***Rationale:*** Some of the impediments to making better use of existing technologies pertain to how/which digital technologies are developed or procured, how they are configured and adapted to meet users' needs, as well as how and where users can access digital technologies. Communication, especially on the articulation of needs and the development of suitable solutions – has been difficult or absent altogether. There is also a clear need to enhance coherence across missions, promote scalability while allowing space for innovation at mission level.

Underlining the need for cultural change throughout peacekeeping, the process of embracing digital technologies is also taking place at different speeds in different parts of the UN peacekeeping family with awareness, understanding and use of digital technologies varying greatly. Substantive mission components with a few exceptions appear detached from discussions on the use and/or development of technology, reluctant to use digital tools, are unaware of their existence, or do not know where to look and who to ask in case a need is identified. As a result, how digital technologies can support mandate implementation remains underexplored and the potential of digital technologies remains unfulfilled throughout most of the substantive work of missions.

## 1.2 INNOVATION AND DIGITAL TRANSFORMATION AT HEADQUARTERS

**KEY RECOMMENDED ACTION:**
Create dedicated spaces for leadership to elevate, propagate and promote innovation in support of mandate implementation and safety and security by peacekeeping missions. For instance, these spaces could take the form of a USG-convened innovation and digital transformation oversight group which could consider external and internal approaches to innovation, and validate/endorse use as appropriate. A director-level steering group could address operational or tactical level bottlenecks and challenges and oversee effective and responsible implementation of initiatives. See proposal below.

***Rationale:*** The internal set up of the Secretariat should enable and facilitate the continuous introduction of new thinking and innovation.  A key consideration in this regard is **full leadership engagement** at all levels. Their active promotion and use of digital technology are key to bringing about the necessary cultural shift and tackling engrained patterns of behaviour which are contrary to the vision of a digital transformation, ranging from a lack of technology awareness and rigid adherence to traditional methods, to resistance to the use of data in decision making.

## 1.3 FORESIGHT ANALYSIS FOR DIGITAL TECHNOLOGY AND CONFLICT

**KEY RECOMMENDED ACTION:**
Create (multidisciplinary) capacity to monitor, analyse and advise on emerging technology issues as they affect peace operations, particularly where usage patterns present threats to missions or offer engagement opportunities on or over the horizon. Any capacity should be approached in an inclusive manner, drawing on the relevant skills, and linked to focal points in policy teams and other relevant offices in the peace and security pillar, the Executive Office of the Secretary-General (EOSG), as well as to mission analysis capacities.

***Rationale:*** Peacekeeping at present does not sufficiently or systematically capture a highly dynamic relationship between conflict actors and technology, and how these shape and impact the conflict environment. This includes recognising new threats, as well as strengthening awareness around existing and evolving ones, or identifying responses to implement peacekeeping mandates. There is currently no global-level approach to ensuring that peacekeeping routinely captures information on the use of technology, identifies overarching strategic trends and anticipates the impact of these trends on missions, to enable consideration in decision-making and planning.

### 1.4 DIGITAL TRANSFORMATION FUNDING MECHANISM

**KEY RECOMMENDED ACTION:**
Ensure dedicated and flexible funds to foster and facilitate innovative projects and support the digital transformation of UN Peacekeeping.

***Rationale:*** A critical obstacle to a future-oriented, data-driven, technology-enabled peacekeeping is the fact that organisational processes – whether on decision making, staffing, funding or procurement – are at odds with the pace of technological change and do not lend themselves to agile and technology-savvy peacekeeping. Dedicated flexible funding will provide fast and tailored funds to initiatives and projects that spur innovation and support the digital transformation of UN Peacekeeping.

## GOAL 2: MAXIMISING THE POTENTIAL OF CURRENT AND NEW TECHNOLOGY

*Enable the use of **existing digital technologies** to their **full potential** and incorporate these considerations when exploring and acquiring/**deploying new digital technologies** in order to empower missions and augment their capacity to carry out their mandates more efficiently and effectively.*

### 2.1 TRAINING AND CAPACITY BUILDING

**KEY RECOMMENDED ACTION:**
Enable a level playing field and develop a peacekeeping workforce equipped with the requisite digital skills, know-how and tools to be able to carry out their work effectively. Actions here range from strengthened technological awareness, data capture and management training for all uniformed and civilian personnel through improved pre-deployment and in-Mission training, to equipping Troop- and Police-contributing Country (T/PCC) units with the requisite digital tools and data to support situational awareness, as well as developing training related to existing guidance, such as for the protection of civilians or peacekeeping-intelligence, and to data-driven tools for identifying, analysing, and prioritising threats to civilians.

***Rationale:*** The SG's Data Strategy highlighted the need to strengthen skills, literacy and awareness on use of digital technologies, including data. Many initiatives from workforce planning to data literacy training are underway that will frame and facilitate similar efforts in peacekeeping, but capacity building and training of uniformed and non-uniformed personnel in missions and at Headquarters have specific requirements, due in part to the complex composition of peacekeeping missions.

While some training is provided in pre-deployment, induction or in-mission trainings, there is no systematic approach that differentiates which types of

This database manager helps to ensure together with the Joint Mission Analysis Centre team of MINUSCA that info is disseminated accurately and timely. Credit: MINUSCA

personnel require which type of capacity building and training and who should provide it. Training on different tools is often a one-time event and lacks the contextualisation and organisational commitment that would incentivise staff to apply them more consistently to benefit their daily work. Some peacekeeping digital technologies have been introduced in a piecemeal fashion, making it difficult to deliver comprehensive capacity building. It has also placed a burden on the absorption capacity of staff for tools and training. Fostering a cultural shift, building technological awareness and instilling a level of comfort with digital tools requires methods beyond training, such as platforms to facilitate knowledge sharing and learning across missions, that are not fully realised for peacekeeping.

Protecting peacekeepers against specific digitally-enabled threats, including IEDs or UAVs requires an integrated approach that brings together situational awareness, training and technology. Much of the technology used for the protection of convoys – advanced IED detection systems, ground-penetrating radar, electronic countermeasures and other alert systems – is normally provided as contingent-owned equipment (CoE). Many of the current T/PCCs would benefit from further enhancing their capacity in this area, as well as counter-IED training and adequate relevant equipment. This effort may include pre-deployment as well as in-mission training, and triangular partnerships and other forms of support. This remains an urgent ongoing need given continuous rotations.

## 2.2 TECHNOLOGICAL SOLUTIONS

**KEY RECOMMENDED ACTIONS:**

Buy, build or expand technological solutions to address long-standing challenges as needed based on data-driven analysis:

**Connect/consolidate ICT/data systems (interoperability)** for mission protection and mandate implementation, i.e. identify system integration opportunities and priorities, align taxonomies to maximise interoperability and data sharing among existing systems, and integrate information management systems, such as UNMAS or UN DSS, into situational awareness.

Promote **mobile, low bandwidth and offline applications,** for instance connecting local and community engagement to systems in real-time through mobile-access tools for both immediate consumption and further analysis of data, or ensuring convoys have reliable and secure communications with 'home base.' Find **scalable and sustainable secure network communications** (including costs, sharing, manageability, chain of custody, etc.).

Introduce **advanced analytics tools/system automation** to help render data capture and management more accurate, consistent and reliable, and to support analysis. This could be done through advanced text/audio/video capture and analysis, using artificial intelligence and machine learning, such as natural language processing, object and activity recognition algorithms, while ensuring risk assessments and/or validating findings prior to decision-making.

Deploy **additional technology for base, convoy and movement protection, medical care,** including expanding and updating the IED technology toolkit, enhancing integrated mission capabilities (e.g. Smart Camp) for threat detection, early warning and response, in accordance with the Current and Emerging Uniformed Capability Requirements for United Nations Peacekeeping (March 2021), casualty tracking, CASEVAC data collection and analysis, en-route and on-site telemedicine and addressing administrative challenges in deploying required technologies.

**Provide service to the 'last mile,'** i.e. identify/prioritise technology infrastructure challenges such as possible solutions to equitably distribute services to remote sites and mobile deployments and strengthen mechanisms to equitably distribute technologies across missions.

***Rationale:*** When it comes to **situational awareness, peacekeeping-intelligence and risk management of conduct and discipline,** there are technical difficulties in linking data systems that are not cohesive, interoperable or even suitable. **Fragmentation** is a central inhibiting factor: systems (databases) are rigid and do not link up, staff are unwilling and/or unable to share information, access is unclear and there is no consistency in how data is managed, stored or accessed. Unwillingness of sections to integrate data for comprehensive analysis is a key impediment and requires a reorientation towards a culture of differentiated sharing. Information collected is largely focused on activities rather than on impact. The Comprehensive Planning and Performance Assessment System (CPAS) has significantly improved **performance assessment.** Over time, it intends to provide missions with the ability to generate evidence of impact and link activities to, for instance, the absence of violence or the responsible use of resources but as of now needs to be further developed, including for decision-making in the Security Council. The use of CPAS for Security Council reporting, including factsheets, needs to be mainstreamed across missions. The ability to demonstrate impact is also essential for compelling storytelling by Strategic Communications and Public Information units, to raise awareness, build support, increase local outreach, dispel misperceptions and counter disinformation.

Digital technologies can help but are distributed unevenly across missions, field offices, camps or operating bases, that have varying levels of sophistication in their ICT infrastructure, and some gaps remain due to lack of funding or Member State support. A lack of technology to enable oversight and communication also carries a heightened risk of misconduct, while limiting a mission's ability to mitigate risks.

Some challenges in **base protection** such as a lack of sufficient perimeter surveillance technology can be alleviated through digital technologies. While some larger permanent compounds have a broad range of detection, monitoring/surveillance and disruption technologies, this is not the case for smaller, remote and/or temporary bases. Given a trend towards more mobile deployments, the need to better detect threats and disrupt attacks on temporary bases is likely to become more pressing. For **convoy and movement protection,** technology support is required to update convoys on developments in the threat environment en route and in near real-time, and provide them with tools for secure communications and offline data capture.

**Medical evacuation and care** in general and **CASEVAC** in particular are major challenges in mission. The deployment of a Casualty Tracking System will **minimize delays,** facilitate proactive and personalized reactive response at the different CASEVAC steps, and provide data for further tailored **quality improvement** initiatives. A CASEVAC data collection tool is necessary to be able to get a clear view of the injured in the field, identify gaps and needs among the whole CASEVAC system and assess the impact of the measures taken. A tool is already available in MINUSMA and should be extended to other missions after the inclusion of additional elements. Finally, **telemedicine** could help improve the quality and safety of care with limited costs and extend clinical capabilities (radiology, mental health, etc.). Systems are available allowing direct data transmission (video, multi-vital signs monitor) even during air CASEVAC.

## GOAL 3: UNDERSTANDING THREATS TO THE SAFETY AND SECURITY OF PEACEKEEPERS AND TO MANDATE IMPLEMENTATION

*Detect, analyse and address potential **threats against civilians, peacekeepers, political processes or missions** in a timely and integrated manner, identify opportunities to promote mandate implementation and build awareness and support.*

### 3.1 COMPREHENSIVE, TIMELY AND ACCURATE PICTURE OF THE SITUATION FOR BETTER INFORMED PLANNING AND DECISION-MAKING

**KEY RECOMMENDED ACTION:**
Strengthen mission capacity for data-driven analysis and reporting, including on the evolving role of digital technologies in the conflict environment and their impact on a peacekeeping mission.

***Rationale:*** Peacekeeping missions face a wide range of threats to their personnel, to their fixed assets, including camps, offices or other facilities, to their movements and activities, to their reputation, and to their technology infrastructure. In fact, the ability to live, work and move as safely as possible is a prerequisite for mandate implementation. Digital technologies are key to understanding the threat environment, including imminent attacks and longer-term trends. In light of the digital gender gap, a differentiated understanding of how these dynamics affect different parts of society and how they impact the ability of women and girls to participate in a peace process is essential.

For the protection of civilians and the safety and security of UN personnel, a pressing challenge is to collate different sources of information and process these in a timely manner. The quality of the data entered – for instance in SAGE – is highly dependent on the aptitude of the person feeding the system, so that data is often unreliable, inconsistent and can skew the narrative. In addition, the capacity and tools to analyse and inform decision making are limited, and missions are not accessing and integrating relevant additional – in particular, **external and recognised – data sources** to fully capture conflict dynamics.

When it comes to digitally-enabled weapons, it is incumbent upon peacekeeping to stay abreast of the latest IED or UAV developments and maintain partnerships with Member States, international organisations, the private sector and research communities to be able to identify and access cutting-edge technologies.

## 3.2 INTEGRATED APPROACH TO MISINFORMATION, DISINFORMATION AND HATE SPEECH

**KEY RECOMMENDED ACTION:**
Assemble a multidisciplinary, integrated capacity or mechanism at Headquarters, to work in close collaboration with mission-based focal points, to support the detection, analysis and response to potential disinformation and hate speech, including by providing guidance and advice on technology tools, such as application of the Rabat threshold test, media analysis or natural language processing, foster knowledge management across missions, and support contact and collaboration with technology providers as required. The work of this capacity or mechanism could be reflected in a deliberate workstream to enable internal coordination.

***Rationale:*** Misinformation, disinformation and hate speech are complex issues that impact missions in a variety of ways, ranging from being a direct threat to safety and security, provoking or facilitating widespread violence, undermining mandate implementation, including undermining political processes, peacebuilding efforts, and endangering past achievements, and affecting staff welfare. Faced with a growing challenge, missions and Headquarters have begun to test various tools for analysing social media and other parts of the information space. But while there has been some thinking around these issues, an overall strategic approach that recognises the multiple facets of mis/disinformation, is absent. Measures currently taken by missions to address mis/disinformation have been customised depending on operational needs and their respective communications landscapes. An integrated and multidisciplinary approach would help better equip and prepare missions to address these information threats.

## 3.3 MITIGATING MEASURES TO REDUCE THE LIKELIHOOD AND IMPACT OF CYBERATTACKS

**KEY RECOMMENDED ACTION:**
Establish continuous and pro-active cybersecurity monitoring and reinforce comprehensive and regularly scheduled cybersecurity assessments in missions to optimise threat detection and response, mitigation of identified vulnerabilities, and to ensure data governance and operational resilience plans are in place.

***Rationale:*** The assessment of cyberthreats is not routinely included in situational awareness or peacekeeping-intelligence, in part because the skills required to identify cyberthreats and implement protection measures are limited and unevenly distributed. Despite regular assessments, some missions still lack up-to-date data governance or operational resilience plans that identify critical data and systems, and countermeasures for managing breaches and threats. Wider use of digital technologies, not least the introduction of automated or machine-learning processes, entail new vulnerabilities that call for vigilance and close collaboration in managing cyberthreats.

## GOAL 4: ENSURING RESPONSIBLE USE

*Set parameters, monitor and oversee implementation of the **responsible use of digital technologies** for peacekeeping, in line with the SG's Roadmap for Digital Cooperation, the SG's Data Strategy and Data Governance Group and the United Nations standards of conduct and in collaboration with other efforts in this area.*

### 4.1 RESPONSIBLE USE GUIDANCE AND REDRESS MECHANISM

#### KEY RECOMMENDED ACTION

Building on guidance and tools that are being used in other parts of the system and adopting a do-no-harm approach, develop clear principles for the ethical use of digital technology, especially data, in peacekeeping, as well as guidelines for how these should be applied and regular reviews as well as a complaints mechanism. This should be done in close collaboration with related workstreams (e.g. SG Data Strategy, Human Rights Due Diligence Policy (HRDDP) for Technology, Data Protection and Privacy Policy) and with mission counterparts (e.g. chiefs of staff/information management officers).

***Rationale:*** Digital technologies in peacekeeping carry particular risks and vulnerabilities, given the need to consider host state sovereignty, data privacy of vulnerable populations and the high turn-over of peacekeepers. This necessitates a considered and deliberate approach to establish safeguards and practices that minimise exposure. Peacekeeping has the obligation to adopt a do-no-harm approach – and culture – and to strengthen responsible use, ethical considerations and accountability. The need to address these issues will only intensify with the introduction of more advanced, automated technologies and with the extensive capture, processing and analysis of data. It is thus essential that peacekeeping follows clear principles for the ethical use of digital technologies throughout their life cycles, assesses potential harm and unintended consequences, takes appropriate corrective actions if necessary, and ingrains this approach among staff.

# Implementing the vision for innovation and digital transformation of UN peacekeeping

**The digital transformation of UN peacekeeping in missions and at Headquarters requires dedicated attention and resources, broad consultation and coordination, and oversight.**

This section proposes one possible approach that could be adopted to drive innovation and the digital transformation process in peacekeeping. It is deliberately broad to allow for flexibility and agility to enable the governance structures to adjust, adapt and change in line with requirements over time.

The proposed approach is guided by three central considerations. First, that leadership engagement is critical to propel meaningful change, signal support for a culture of innovation and transformation, and eliminate barriers to innovation and seek accountability. Second, that the commitment and hands-on involvement of multiple partners across disciplines at different levels would enrich the digital transformation process. Third, that dedicated capacity would allow space for co-creation between technology users and developers/managers to flourish.

The approach proposed here would draw upon a mix of existing capacity and extrabudgetary resources. Extrabudgetary resources would augment human capital for the proposed multidisciplinary team, and fund activities in support of innovation and digital transformation in peacekeeping, including experimentation, testing, prototyping and piloting of technology tools, and the development of training and capacity-building resources.

The configuration of resources and organisational set-ups to enable innovation in missions would be driven by mission-specific considerations, including the existence of business analysis capacity, designated technology innovation roles, and the needs of each conflict environment. The proposed HQ-based multidisciplinary team below would provide advisory support to individual missions on the design and configuration of capacity for technology innovation, as well as supporting specific initiatives in missions.

The process unlocked through digital transformation in peacekeeping settings would have a positive impact on broader system-wide digital transformation and business process improvements. Successful innovations pioneered through the strategy could be brought to scale through existing ICT governance mechanisms.

The following represents a tentative proposal for a possible governance structure for the digital transformation of UN peacekeeping.

### INNOVATION AND DIGITAL TRANSFORMATION BOARD

An **Innovation and Digital Transformation Board** chaired at USG level could endorse and support technology innovation for scaling and referral to the UN Office of Information and Communications Technology (OICT), articulate expectations across peace and security pillar and seek top-level coherence, promote a culture of innovation in the pillar, including by supporting and rewarding innovation practices in the field and at headquarters, and consider technology innovations from external actors.

Meeting every six months, the Board would be composed of the USGs and ASGs of DPO, DOS, DMSPC, the Secretary-General’s Envoy on Technology, and the Chief Information Technology Officer, as well as the heads of four mission or their deputies, as designated. Missions to be rotated every two years.

A Community Liaison Assistant (CLA) working for MONUSCO meets with residents in Goma, North Kivu. CLAs play a pivotal role in protecting civilians by connecting communities to the UN, bridging communication gaps between uniformed components and the local population, establishing community alert networks, and discerning the threats present at the local level and the protection concerns of the population. Photo: Myriam Asmani

Other Secretariat principals, including the USGs of DPPA, the Office for Disarmament Affairs and the UN Counter-Terrorism Office could be invited periodically.

## DIRECTOR-LEVEL INNOVATION AND DIGITAL TRANSFORMATION TASK FORCE

Operational guidance to the digital transformation process could be provided by a Director-level Innovation and Digital Transformation Task Force. The Task Force could resolve any bottlenecks, delays and difficulties in the digital transformation process, as well as review and validate the approach taken to implement the strategy. The Task Force could meet every three months and be composed of Director-level representatives of the current interdepartmental peacekeeping technology working group that supported the development of this strategy.

## INNOVATION AND DIGITAL TRANSFORMATION TEAM

To meet the challenge at Headquarters, the creation of an **Innovation and Digital Transformation Team** is proposed. The objective is to establish a multidisciplinary centre of gravity for innovation and digital transformation that can promote a culture of innovation, draw together expertise from across the Secretariat (and possibly beyond) and oversee implementation of the strategy.

The Team would sit in the office of the Director for Shared Services, and in its day-to-day activities would work closely with the Information Management Unit based in the same office, as well as the DPPA Innovation Cell, field missions, and DOS, DMSPC, EOSG, the DPPA-DPO Shared Services and Regional Structure as well as other relevant UN entities working on innovation and digital transformation.

The Team would be matrixed and cross-functional, with dotted-line relationships to key Secretariat offices. It is proposed that the Team be staffed through a combination of extrabudgetary funds, internal secondments from relevant peacekeeping capacities, and through fellowships or similar arrangements with external partners.

Tasks could include:

- Act as a locus for the co-creation of innovative digital solutions for peacekeeping in the field and headquarters;
- Monitor and analyse trends in digital technology and conflict;
- Engage in rapid prototyping with internal and external entities, to bridge the gap between conceptual ideas and real, workable solutions (build/measure/learn);
- Train staff in the missions and at Headquarters on new technological trends and concepts; support the application of system-wide and development of peacekeeping-specific responsible use principles and methodologies, as required;
- Facilitate knowledge sharing across missions, including promoting existing/enhanced forums for innovation, ideation and technology development;
- Foster and develop partnerships on digital technology in peacekeeping, including with Member States, the technology sector, academic and civil society;
- Coordinate and drive the implementation of the strategy for the digital transformation of peacekeeping;
- Managing digital transformation funding.

# Annexes

## ANNEX I: KEY INITIATIVES USED AT HEADQUARTERS AND IN MISSIONS

The following provides a representative sample of key initiatives in the Summer of 2021 that reflect the dynamic and evolving environment in which the Strategy for the Digital Transformation of UN Peacekeeping will be implemented. The sample consists of concrete initiatives, as well as more generic descriptions of technologies already in use in peacekeeping. This is not an exhaustive list but shows the many types of initiatives with which the strategy will seek to find synergies.

Action for Peacekeeping: The A4P initiative was launched by the Secretary-General's in 2018, aiming to refocus peacekeeping with more targeted mandates, making operations stronger and safer, mobilizing support for political solutions and better equipping and training forces. The collective actions to strengthen peacekeeping are outlined in the Declaration of Shared Commitments endorsed by over 150 countries.

Action for Peacekeeping Plus: Launched by the Secretary-General as the implementation strategy for 2021-2023, A4P+ aims to accelerate progress on the implementation of the Declaration of Shared Commitments on UN Peacekeeping and to focus on crosscutting priorities, namely collective coherence behind a political strategy, strategic and operational integration, capabilities and mindsets, accountability to peacekeepers, accountability of peacekeepers, strategic communications, and cooperation with host countries.

Comprehensive Planning and Performance Assessment System: A UN tool to link the context of a country with peacekeeping planning, data, results and reporting to assess performance, inform future plans, and formulate recommendations.

Current and Emerging Uniformed Capability Requirements for United Nations Peacekeeping: A quarterly paper, which provides information on mid to long-term critical uniformed capability needs in peacekeeping missions, current gaps and other opportunities, such as training and capacity building, for Member States to contribute to UN operations by providing concrete offers to the Peacekeeping Capability Readiness System (PCRS).

Detailed Guidance on Implementation of the UN Strategy and Plan of Action for United Nations Field Presences: The Guidance provides detailed information on how to implement the 13 commitments set out in the Strategy and options for action that United Nations staff can take in field contexts, guided by the broad vision of prevention, and building on good practices from within the United Nations system as well as from Member States, civil society and other stakeholders.

Early Warning Tracking Mobile App: Released by the United Nations Operations and Crisis Centre (UNOCC) in late 2020, the app was developed to facilitate a rapid, coordinated, and multi-component response to early warnings received by the mission.  It is now live in MINUSMA, and will implemented in 2021 MONUSCO and UNISFA.

Field Support Group for COVID-19 Data Analytics: In response to the COVID-19 crisis, the global Field Support Group for COVID-19 Online Reporting System was launched in 2020. Regular data reporting on several topics from the UN missions into the FSGC Online Reporting System was enabled through the establishment of standard procedures, assignment of responsibilities and implementation of trainings. The data is managed in a central database and further used to produce reports and dashboards.

Geospatial Strategy for the United Nations: The strategy aims to design, foster and build synergies for activities and investments in geospatial information management in the United Nations Secretariat, as a strategic enabler for UN's work across pillars in development, peace and security, humanitarian issues and human rights.

Global Pulse: A Secretary-General's initiative on big data and artificial intelligence for development, humanitarian action, and peace with labs in operate in Finland, Indonesia, Uganda, and in New York at the UN Headquarters.

ICT Data Classification Technical Procedure: A mandatory procedure for all project teams to follow throughout the ICT project lifecycle to ensure that information and data managed in an ICT application are marked with proper business content categorization, retention schedule, sensitivity classification, personal identifiable information, scope of access, and whether containing vital information. The technical procedure allows information and data stored in ICT applications to be managed according to the Secretariat's information management policies and ensures that institutional memories are captured, protected, and accessible for the organization's daily operation as well as for the future generations.

Innovation Cell: In January 2020, the Department of Political and Peacebuilding Affairs launched the Innovation Cell, an interdisciplinary team dedicated to helping the Department and its field presences to understand and explore, pilot, and scale new technologies, tools, and practices in conflict prevention, mediation and peacebuilding.

Innovation Day (DMSPC): The participation in the weekly Innovation Day is open to all UN personnel with the aim to share new ideas, processes, behaviours, and concepts. They include internal briefings on innovation across the UN system, as well as briefings by external experts covering a wide variety of innovative and creative topics with links to actual projects, mandates, and internal contexts.

MINSIGHT application: The application aims to operationalise the SG's UN Data Strategy by utilising an innovative machine-learning approach to process, systematise, and visualise recommendations contained in reporting related to the work and performance of MINUSCA.

Misconduct Tracking System: A global database and confidential tracking system for all allegations of misconduct involving UN peacekeeping personnel.

#NewWork initiative: An UN staff-driven initiative that proactively aims to change the workplace culture through a platform on which best practices, skills and expertise can be shared and initiatives co-created.

Notification of Peacekeeper Casualties database system (NOTICAS): A web-based programme which enables electronic submission of casualty data for UN personnel from the missions to the Headquarters.

OICT's Emerging Technology Team: The Team investigates how technologies and their possible applications can facilitate the core work of the Secretariat.

OICT's Reboot Accelerator: The programme calls for innovative solutions to support the work and mandates of the UN and provides a space for the engagement of UN entities and external partners, including in the private sector and academia, fostering multi- multiple stakeholder collaboration and knowledge sharing.

Partnership for Technology in Peacekeeping: Established by the Department of Field Support in 2014, this initiative has the objective to bring greater involvement to peacekeeping through innovative approaches and technologies that have the potential to empower UN global operations.

Peacekeeping-Intelligence Policy: The policy framework, as laid out in the 2019 DPO Policy on Peacekeeping-Intelligence (DPO 2019.08), articulates a consistent and principled approach to peacekeeping-intelligence; ensures the most effective utilisation of available resources; and enacts mechanisms to enable an effective, integrated and secure whole-of-mission approach.

Performance Peacekeeping - Report of the Expert Panel on Technology and Innovation in UN Peacekeeping (2015): A report outlining recommendations of an independent expert panel on how technology and innovation can be leveraged to increase the effectiveness and efficiency of peacekeeping.

"Sage": Commissioned by the United Nations Operations and Crisis Centre (UNOCC), Sage is a web-based database system that allows UN military, police and civilians in UN peace operations to log incidents, events and activities to obtain dynamic dashboards visualizing hotspots.  It is currently operational in most PKOs and some SPMs.

Secretary-General's Data Strategy for Action by Everyone, Everywhere: Launched by the SG in 2020, the strategy outlines a long-term agenda for the UN's data-driven transformation promoting a vision that stresses the power of UN data assets and stimulates the UN System to embrace a more coherent and modern approach to data production and use.

Secretary-General's Strategy and Plan of Action on Hate Speech: The strategy launched by the SG in 2019 points out key objectives, principles and commitments recognising the threat that hate speech posed to the UN principles, values and programmes and aiming to give the UN the room and resources to address hate speech.

Secretary-General's Strategy on New Technologies: Launched by the SG in 2018, the goal of this internal strategy is to define how the United Nations system will support the use of new technologies like artificial intelligence, biotechnology, blockchain, and robotics to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights, and the norms and standards of international law.

Secretary-General's Roadmap for Digital Cooperation: Based on recommendations from the Secretary-General's High-level Panel for Digital Cooperation convened from 2018-2019, and further informed by a series of roundtable discussions, the report lays out a roadmap in which all stakeholders play a role in advancing a safer, more equitable digital world, one which will lead to a brighter and more prosperous future for all.

Smart Camp: The UN has launched a UN Smart Camp project, a group of projects coordinated around a more comprehensive "smarter" concept for UN camps, led by the Department of Operational Support. The project aims to expand the UN Smart Camp concept beyond a technology-centred approach to integrate it with relevant different business areas, workstreams and processes, to enhance the effectiveness and efficiency of support to as well as the use of camps towards mandate implementation in UN peace operations.

Smart IED Threat Mitigation Technology Roadmap: An interactive information exchange platform launched by UNMAS compiling and sharing the latest information on global IED threats and on the technology available to mitigate them.

Spatio-Temporal Incident Mapping Tool (MINUSMA): The tool has been developed in 2020 to better assess the impact of force operations on the protection of civilians by recording force activities, such as Temporary Operating Bases and patrols, plotting these activities on a map, and then superimposing incidents in which civilians were targeted.

Technology Solutions Collaboration Space: A platform built to help UN professionals to foster a collaboration culture and harness its power to equip them with suitable tools and best practices to address their challenges. It is a tool dedicated to "bridge the gap" between the field technology experts in missions and strategic decision-makers in Headquarters through information sharing and virtual teaming. The aim of the platform is to be interactive and a source of useful information for its community of experts regarding new technologies and novel approaches to established processes, to enhance mission capabilities and facilitate effective mandate implementation.

Umoja: A single, global solution that is enabling efficient and transparent management of the United Nation's financial, human and physical resources and improving programmatic delivery.

UN C4ISR Academy for Peace Operations (UNCAP, former UN Signals Academy): Established by the Department of Field Support in 2015 as an outcome of the Partnership for Technology in Peacekeeping and managed by the Office of Information and Communications Technology (OICT/OSD), this initiative has the objective of providing C4ISR[6] and camp security technology training to Peace Operations and enhance mandate implementation.

UN Global Pulse's Risks, Harms and Benefits Assessment Tool: A data privacy, ethics and data protection compliance mechanism designed to help identify and minimise the risks of harms and maximise the positive impacts of data innovation projects.

UN Innovation Network: An informal, collaborative community of UN innovators and external partners which share their expertise and experience to promote and advance innovation within the UN System.

UN Innovation Toolkit (DOS): Developed by the UN, for the UN, this digital platform includes twenty-one tools, step-by-step directions, worksheets, case studies, references as well as a 27-question assessment which provides a diagnosis on every user's strengths and areas for improvement.

UN Peace and Security Data Hub: A free public library of datasets on peace and security published by the United Nations.

UN Principles on Data Privacy and Data Protection: The principles set out a basic framework for the processing of personal data by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.

UNDSS Security Risk Management System: A system which captures real-time information entered by security officers and produces

[6] C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance.

rolling updates that could usefully contribute to peacekeeping situational awareness

Unite Aware: A platform that aggregates and processes trusted and secure data and presents that information to mission decision-makers via analysis, visualization, and reporting applications. The two main objectives of UA are to provide a comprehensive and integrated approach to situational awareness and support UN field missions to manage critical information management processes. The suite aims to create a cohesive solution which enables UN mission staff to access and view near real-time data from a variety of sources, displayed in a clear and intuitive format.

Unite Ideas: The platform engages and mobilizes data scientists, programmers, designers, students, and entrepreneurs worldwide to develop open source technology solutions to challenges posed by partners that are united in their goal to generate social good.

‘Verified’ initiative: A United Nations initiative that calls on people around the world to become “information volunteers” and share UN-verified, science-based content on the COVID-19 pandemic to keep their families and communities safe and connected.

## ANNEX II: OVERVIEW CONSULTATION AND VALIDATION PROCESS

| FORMAT | EVENTS |
|---|---|
| **Interdepartmental Working Group & Sub-groups**<br>(see membership in Annex III) | • Eight Working Group meetings<br>• Seven additional sub-working group meetings |
| **Baseline Survey** | • Almost 500 responses from Peacekeeping Missions and Headquarters staff (DOS, DPO, DMSPC, including OICT) |
| **Focus Groups** | • Trends in use of technology by conflict parties<br>• Measures to enhance safety and security, including: camp protection, situational awareness, peacekeeping-intelligence<br>• Conflict monitoring and analysis, including of disinformation and hate speech, political processes and protection of civilians and other online threats to mandate implementation.<br>• Training and capacity-building of civilian and uniformed personnel |
| **Bilateral consultations** | • Over 100 consultations within and beyond UN system |
| **Senior leadership briefings** | • Two briefings to USGs DPO, DOS and DMSPC<br>• Two briefings/consultations (each) with Directors DPO, DOS and DMSPC<br>• Two briefings/consultations with Chiefs of Staff/Directors of Mission Support (in peacekeeping missions) |
| **Roundtables** | • Policy challenges for UN data governance in peacekeeping<br>• Technical challenges for UN data governance in peacekeeping<br>• Use of data and digital technologies by non-UN partners<br>• Use of data and digital technologies by UN system partners |
| **Research Papers** | • Esberg, J. & Mikulaschek, C. (Aug 2021). *Digital technologies, peace and security: challenges and opportunities for United Nations Peace Operations.*<br>• Udupa, S. (Aug 2021). *Digital technology and extreme speech.*<br>• Druet, D. (Aug 2021). *Enhancing the use of digital technology for integrated situational awareness and peacekeeping-intelligence.*<br>• Pauwels, E. (Aug 2021). *Peacekeeping in an era of converging technological and security threats.* |
| **Consultations with Member States** | • Three informal briefings to Special Committee on Peacekeeping Operations (C34)<br>• Consultations with individual and groups of Member States |
| **Consultations with international/regional organisations** | • European Union (EU)<br>• North Atlantic Treaty Organisation (NATO)<br>• Organisation for Security and Cooperation in Europe (OSCE) |
| **Red Team** | • Four meetings to discuss and validate strategy drafts |
| **Draft document** | • Five rounds of consultations on successive iterations of draft strategy |

## ANNEX III: INTERDEPARTMENTAL WORKING GROUP

| DEPARTMENT | DIVISION/OFFICE/SECTION |
|---|---|
| **DPO** | Office of the Under-Secretary-General |
| **DPO** | Division of Policy, Evaluation, and Training |
| **DPO** | Office of Military Affairs |
| **DPO** | Office of Rule of Law and Security Institutions |
| **DPO** | Police Division |
| **DPO** | Office for Peacekeeping Strategic Partnership |
| **DPPA-DPO Regional & Shared Services** | Information Management Unit |
| **DPPA-DPO Regional & Shared Services** | Strategic Communication Section |
| **DPPA-DPO Regional & Shared Services** | Operations and Crisis Centre |
| **DPPA-DPO Regional & Shared Services** | Office of the Director for Coordination and Shared Services |
| **DPPA-DPO Regional & Shared Services** | OASG-Europe, Central America and the Americas |
| **DPPA-DPO Regional & Shared Services** | OASG-Africa |
| **DPPA-DPO Regional & Shared Services** | OASG-Middle East, Asia and the Pacific (invited) |
| **DPPA** | Policy and Mediation Division |
| **DOS** | Office of the Under-Secretary-General |
| **DOS** | Capacity Development and Operational Training Service |
| **DOS** | Office of Supply Chain Management |
| **DOS** | Division of Healthcare Management and Occupational Safety and Health |
| **DOS** | Division of Special Activities |
| **DMSPC** | Office of the Under-Secretary-General |
| **DMSPC** | Business Transformation and Accountability Division |
| **DMSPC** | Office of Human Resources |
| **DSS** | Division of Regional Operations |
| **OICT** | Operations Support Division |

| DEPARTMENT | DIVISION/OFFICE/SECTION |
|---|---|
| **OICT** | Policy, Strategy & Governance Division |
| **EOSG** | Strategic Planning and Monitoring Unit |
| **Office of the Envoy on Technology** | |
| **MINUSCA** | Office of Chief of Staff |
| **MINUSMA** | Office of Chief of Staff |
| **MINUSMA** | Field Technology Section |
| **MINUSMA** | Head of Office, Timbuktu |
| **MONUSCO** | Office of Chief of Staff |
| **UNISFA** | Office of Chief of Staff |
| **UNITAMS** | Office of Chief of Staff |
| **UNMISS** | Office of Chief of Staff |
| **UNTSO/UNSCO** | Field Technology Section |

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| A4P | Action for Peacekeeping |
| A4P+ | Action for Peacekeeping Plus |
| AI | Artificial intelligence |
| ASG | Assistant-Secretary-General |
| C34 | Special Committee on Peacekeeping Operations |
| CAR IOT | Central African Republic Integrated Operational Team |
| CITO | Chief Information Technology Officer |
| COS | Chief of Staff |
| CPAS | Comprehensive Planning and Performance Assessment System |
| DMSPC | Department of Management, Strategy, Policy and Compliance |
| DOS | Department of Operational Support |
| DPO | Department of Peace Operations |
| DPPA | Department of Peacebuilding and Political Affairs |
| DSS | United Nations Department for Safety and Security |
| EOSG | Executive Office of the Secretary-General |

| | |
|---|---|
| FSGC | Field Support Group for COVID-19 |
| FTS | Field Technology Section |
| GIS | Geographic Information System |
| HQ | Headquarters |
| HRDDP | Human Rights Due Diligence Policy |
| ICT | Information and Communications Technology |
| IED | Improvised Explosive Devices |
| ISR | Intelligence, Surveillance and Reconnaissance |
| MINUSCA | United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic |
| MINUSMA | United Nations Multidimensional Integrated Stabilization Mission in Mali |
| OASG | United Nations Office of the Assistant-Secretary-General |
| OCT | United Nations Counter-Terrorism Office |
| ODA | United Nations Office for Disarmament Affairs |
| OICT | United Nations Office of Information and Communications Technology |
| PKI | Peacekeeping-Intelligence |
| SG | Secretary-General |
| SGB | Secretary-General’s Bulletin |
| T/PCC | Troop- and Police-Contributing Country |
| UAV/S | Unmanned Aerial Vehicle or System |
| UCAV | Unmanned Combat Aerial Vehicle |
| UNIN | UN Innovation Network |
| UNMAS | United Nations Mine Action Service |
| USG | Under-Secretary-General |

17-09-2021